Wolfgang Marekfia

Strategisches GRC-Management

Ilmenauer Schriften zur
WIRTSCHAFTSINFORMATIK

Herausgegeben von
Prof. Dr. Volker Nissen,
Fachgebiet Wirtschaftsinformatik für Dienstleistungen
an der Technischen Universität Ilmenau.

Band 3

Strategisches GRC-Management

Anforderungen, Forschungsagenda und datenseitiges Modell

Wolfgang Marekfia

Universitätsverlag Ilmenau
2017

Impressum

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über http://dnb.d-nb.de abrufbar.

Diese Arbeit hat der Fakultät für Wirtschaftswissenschaften der Technischen Universität Ilmenau als Dissertation vorgelegen.

Tag der Einreichung:	22. Januar 2016
1. Gutachter:	Univ.-Prof. Dr. Volker Nissen (Technische Universität Ilmenau)
2. Gutachter:	Prof. Dr. Dr. h. c. Volker Herwig (FH Erfurt)
Tag der Verteidigung:	25. Mai 2016

Technische Universität Ilmenau/Universitätsbibliothek
Universitätsverlag Ilmenau
Postfach 10 05 65
98684 Ilmenau
http://www.tu-ilmenau.de/universitaetsverlag

Herstellung
readbox unipress
in der readbox publishing GmbH
Am Hawerkamp 31
48155 Münster
http://unipress.readbox.net

Druck und Bindung
CCC Druck und Medien GmbH, Münster

ISSN 2199-2096 (Druckausgabe)
ISBN 978-3-86360-151-5 (Druckausgabe)
URN urn:nbn:de:gbv:ilm1-2016000715

Titelfoto: photocase.com | Nortys

Inhaltsverzeichnis

Inhaltsverzeichnis **5**

Abbildungsverzeichnis **11**

Tabellenverzeichnis **12**

Abkürzungsverzeichnis **18**

1 Einleitung **23**

1.1 Ausgangssituation und Problemstellung *23*

1.2 Forschungsziel und Forschungsfragen *30*

1.3 Forschungsmethodische Positionierung *33*

1.4 Vorgehensweise *41*

2 Grundlagen zu Governance, Risiko- und Compliance-Management **45**

2.1 Vorüberlegungen *45*

2.2 Corporate Governance und IT-Governance *46*

2.3 Risikomanagement *51*

2.4 Compliance-Management *55*

2.5 Beziehungen und Integrationsaspekte von Governance, Risiko- und Compliance-Management *58*

2.5.1 Beziehungen und Integrationsaspekte von Compliance- und Risikomanagement 58

2.5.2 Beziehungen und Integrationsaspekte von Governance und Compliance-Management 60

2.5.3 Beziehungen und Integrationsaspekte von Governance und Risikomanagement 62

2.6 GRC und strategisches GRC-Management ... 63

2.7 GRC und Informationstechnologie ... 69

2.8 Erläuterung weiterer Begriffe ... 70

3 Anforderungen und Forschungsagenda für das strategische GRC-Management ... 76

3.1 Zielsetzung, Auswahl und Methodik des Literaturreviews ... 76

3.2 Verwandte Arbeiten ... 89

3.3 Relevante Theorien für das GRC-Management ... 94

3.3.1 Bedeutung und Identifikation der Theorien ... 94

3.3.2 Strategische Theorien ... 104

3.3.2.1 Darstellung der strategischen Theorien ... 104

3.3.2.2 Anwendung der strategischen Theorien in der GRC-Literatur ... 107

3.3.3 Ökonomische Theorien ... 109

3.3.3.1 Darstellung der ökonomischen Theorien ... 109

3.3.3.2 Anwendung der ökonomischen Theorien in der GRC-Literatur ... 113

3.3.4 Verhaltenswissenschaftliche Theorien ... 116

3.3.4.1 Darstellung der verhaltenswissenschaftlichen Theorien ... 116

3.3.4.2 Anwendung der verhaltenswissenschaftlichen Theorien in der GRC-Literatur ... 121

3.3.5 Zwischenfazit ... 124

3.4 Anforderungen für das strategische GRC-Management ... 125

3.4.1 Identifikation der Anforderungskategorien ... 125

3.4.2 Darstellung und theoretische Analyse der Anforderungskategorien ... 132

3.4.2.1 Strategische Ausrichtung ... 132

3.4.2.2 Integration ... 138

3.4.2.3 Geschäftsprozessorientierung ... 148

3.4.2.4 Management-Systeme ... 150

3.4.2.5 Automatisierung ... 152

3.4.2.6 Flexibilität 155
3.4.2.7 Menschliche Faktoren 159
3.4.3 Zwischenfazit 161

3.5 Forschungsstand und weiterer Forschungsbedarf 164
3.5.1 Strukturierung der Diskussion des Forschungsstandes .. 164
3.5.2 Untersuchung von GRC-bezogenen Management-Ansätzen hinsichtlich der Berücksichtigung der Anforderungen 170
3.5.2.1 Strategische Ausrichtung 170
3.5.2.2 Integration 173
3.5.2.3 Geschäftsprozessorientierung 177
3.5.2.4 Management-Systeme 178
3.5.2.5 Automatisierung 180
3.5.2.6 Flexibilität 182
3.5.2.7 Menschliche Faktoren 183
3.5.2.8 Zusammenfassung der Diskussion der Management-Ansätze 185
3.5.3 Forschungsstand: Strategische Ausrichtung 188
3.5.3.1 Forschungsziel: Beschreiben und Erklären 188
3.5.3.2 Forschungsziel: Gestalten 194
3.5.4 Forschungsstand: Integration 197
3.5.4.1 Forschungsziel: Beschreiben und Erklären 197
3.5.4.2 Forschungsziel: Gestalten 202
3.5.5 Forschungsstand: Geschäftsprozessorientierung 210
3.5.5.1 Forschungsziel: Beschreiben und Erklären 210
3.5.5.2 Forschungsziel: Gestalten 211
3.5.6 Forschungsstand: Management-Systeme 215
3.5.6.1 Forschungsziel: Beschreiben und Erklären 215
3.5.6.2 Forschungsziel: Gestalten 219
3.5.7 Forschungsstand: Automatisierung 220
3.5.7.1 Forschungsziel: Beschreiben und Erklären 220
3.5.7.2 Forschungsziel: Gestalten 223
3.5.8 Forschungsstand: Flexibilität 228
3.5.8.1 Forschungsziel: Beschreiben und Erklären 228
3.5.8.2 Forschungsziel: Gestalten 231

3.5.9 Forschungsstand: Menschliche Faktoren 233
3.5.9.1 Forschungsziel: Beschreiben und Erklären 233
3.5.9.2 Forschungsziel: Gestalten 236
3.5.10 Zwischenfazit 237

3.6 Zusammenfassung der Ergebnisse als Forschungsagenda 242
3.6.1 Vorgehensweise zur Entwicklung der Forschungsagenda 242
3.6.2 Zusammenfassung des weiteren Forschungsbedarfs 243
3.6.3 Möglichkeiten zur Bestimmung der Bedeutung und Bearbeitungsreihenfolge des weiteren Forschungsbedarfs 248
3.6.4 Elemente einer Forschungsagenda für das strategische GRC-Management 252

3.7 Grenzen des Literaturreviews 269

3.8 Zwischenfazit 271

4 Delphi-Studie zu Anforderungen und Forschungsbedarfen eines strategischen GRC-Managements 273

4.1 Zielsetzung, Auswahl und Methodik der Delphi-Studie 273

4.2 Planung der Delphi-Studie 278
4.2.1 Das Expertenpanel 278
4.2.2 Struktur und Vorgehensweise der Delphi-Studie 282
4.2.3 Pretest 285

4.3 Ergebnisse der Delphi-Studie 286
4.3.1 Vorüberlegungen zur Auswertung 286
4.3.2 Allgemeine Daten zum Expertenpanel 292
4.3.3 Ergebnisse der ersten Befragungsrunde 295
4.3.4 Ergebnisse der zweiten und dritten Befragungsrunde ... 297
4.3.4.1 Bedeutung der Anforderungen und Forschungsbedarfe 297
4.3.4.2 Konsens und Stabilität 305

4.4 Grenzen der Studie 311

4.5 Zwischenfazit *312*

5 Datenseitiges Modell für das strategische GRC-Management 315

5.1 Motivation und Ziele *315*

5.2 Methodik der Referenzmodellierung *317*
5.2.1 Grundlagen und Einordnung 317
5.2.2 Strukturierung des Forschungsprozesses 321
5.2.3 Identifikation adäquater Wissensquellen 322
5.2.4 Festlegung der Modellierungstechnik 325

5.3 Entwicklung des Modells *327*
5.3.1 Auswertung der existierenden Modelle in der GRC-Literatur 327
5.3.1.1 Identifikation existierender konzeptioneller Modelle im Kontext von GRC 327
5.3.1.2 Auswertung der relevanten Informationsobjekte 336
5.3.1.3 Auswertung der Beziehungen zwischen den Informationsobjekten 341
5.3.2 Abgleich der Modellobjekte mit den Anforderungen an das strategische GRC-Management 345
5.3.2.1 Vorüberlegungen 345
5.3.2.2 Strategische Ausrichtung 347
5.3.2.3 Integration 348
5.3.2.4 Geschäftsprozessorientierung 349
5.3.2.5 Management-Systeme 349
5.3.2.6 Automatisierung 350
5.3.2.7 Flexibilität 351
5.3.2.8 Menschliche Faktoren 352
5.3.3 Darstellung des Modells 352
5.3.4 Demonstration des Modells 356

5.4 Evaluierung *370*
5.4.1 Grundlagen und Vorgehensweise der Evaluierung 370
5.4.2 Übersicht der publizierten Fallbeispiele 372
5.4.3 Ergebnisse der Evaluierung 378

5.4.3.1 Allgemeine Beobachtungen ... 378
5.4.3.2 Adäquanz und Vollständigkeit der Informationsobjekte ... 379
5.4.3.3 Beziehungen der Informationsobjekte ... 388

5.5 Grenzen der Modellierung ... 389

5.6 Zwischenfazit ... 392

6 Schlussbetrachtungen ... 394

6.1 Zusammenfassung der Ergebnisse ... 394

6.2 Kritische Würdigung der Arbeit ... 397

6.3 Nutzen für Forschung und Praxis ... 400
6.3.1 Nutzen für die Forschung ... 400
6.3.2 Nutzen für die Praxis ... 404

6.4 Ausblick ... 406

Anhang ... 410

A Anhang zu Kapitel 3 Anforderungen und Forschungsagenda für das strategische GRC-Management ... 410

B Anhang zu Kapitel 4 Delphi-Studie zu Anforderungen und Forschungsbedarfen eines strategischen GRC-Managements ... 425

C Anhang zu Kapitel 5 Datenseitiges Modell für das strategische GRC-Management ... 437

Literaturverzeichnis ... 440

Abbildungsverzeichnis

Abb. 1: Strukturierung der Arbeit anhand der Kernelemente „Anforderungen und Forschungsagenda“ und „Datenseitiges Modell“ 44
Abb. 2: Modell eines unternehmensweiten Risikomanagements gemäß COSO (COSO 2004, S. 5) 54
Abb. 3: Zwiebelmodell für Regelwerke der Compliance nach Klotz und Dorn (2008, S. 11-14) bzw. Klotz (2009, S. 20-25) 56
Abb. 4: IT-Compliance-Managementprozess nach Rath und Sponholz (2009, S. 136) 58
Abb. 5: GRC-Dreieck (in Anlehnung an Klotz 2009, S. 8-11; Klotz und Dorn 2008, S. 6-10; Kranawetter 2009, S. 24; Puspasari et al. 2011, S. 312; Racz et al. 2010b; SAP 2009, S. 8; Schöler und Zink 2008, S. 17-18) 66
Abb. 6: Bedeutungsvarianten der IT im Kontext von GRC (in Anlehnung an Klotz und Dorn 2008, S. 9) 70
Abb. 7: Vorteile einer integrierten Erfüllung von GRC-Vorgaben 147
Abb. 8: Vorteile einer Integration der GRC-Teildisziplinen 147
Abb. 9: Datenseitiges Modell für das strategische GRC-Management 356

Tabellenverzeichnis

Tab. 1: Einige allgemeine Angaben zur ausgewerteten Literatur 87
Tab. 2: Publikationsorgane mit 10 oder mehr berücksichtigten Veröffentlichungen 88
Tab. 3: Überblick über Literaturreviews zu integrierten GRC-Konzepten 91
Tab. 4: Übersicht der Theorien aus der GRC-Literatur mit zwei oder mehr Anwendungen 100
Tab. 5: Übersicht der in der weiteren Analyse verwendeten Theorien 102
Tab. 6: Kategorien, Unterkategorien, Anzahl Kodierungen (Kod.) und relevante Theorien 129
Tab. 7: Analyse der Eigenschaften zu den GRC-Transaktionen 142
Tab. 8: Mögliche Koordinationsformen des GRC-Managements 144
Tab. 9: Anforderungen an das strategische GRC-Management 162
Tab. 10: Management-Ansätze für GRC aus der Literatur 168
Tab. 11: Bewertung der GRC-Management-Ansätze anhand der Anforderungen (1 von 2) 187
Tab. 12: Bewertung der GRC-Management-Ansätze anhand der Anforderungen (2 von 2) 188
Tab. 13: Forschungsstand nach Anforderungskategorie und Forschungsziel (1 von 2) 239
Tab. 14: Forschungsstand nach Anforderungskategorie und Forschungsziel (2 von 2) 240
Tab. 15: Forschungsbedarf zum strategischen GRC-Management (1 von 3) 245
Tab. 16: Forschungsbedarf zum strategischen GRC-Management (2 von 3) 246

Tab. 17: Forschungsbedarf zum strategischen GRC-Management (3 von 3) 247
Tab. 18: Erläuterung der Attribute der Forschungsagenda 252
Tab. 19: Forschungsagenda für das strategische GRC-Management (1 von 12) 257
Tab. 20: Forschungsagenda für das strategische GRC-Management (2 von 12) 258
Tab. 21: Forschungsagenda für das strategische GRC-Management (3 von 12) 259
Tab. 22: Forschungsagenda für das strategische GRC-Management (4 von 12) 260
Tab. 23: Forschungsagenda für das strategische GRC-Management (5 von 12) 261
Tab. 24: Forschungsagenda für das strategische GRC-Management (6 von 12) 262
Tab. 25: Forschungsagenda für das strategische GRC-Management (7 von 12) 263
Tab. 26: Forschungsagenda für das strategische GRC-Management (8 von 12) 264
Tab. 27: Forschungsagenda für das strategische GRC-Management (9 von 12) 265
Tab. 28: Forschungsagenda für das strategische GRC-Management (10 von 12) 266
Tab. 29: Forschungsagenda für das strategische GRC-Management (11 von 12) 267
Tab. 30: Forschungsagenda für das strategische GRC-Management (12 von 12) 268
Tab. 31: „Knowledge resource nomination worksheet“ für die vorliegende Delphi-Studie 280

Tab. 32: Übersicht zu möglichen Analysemethoden der deskriptiven Statistik für Delphi-Studien und deren Relevanz für die vorliegende Studie 288
Tab. 33: Übersicht zu möglichen Analysemethoden der schließenden Statistik für Delphi-Studien und deren Relevanz für die vorliegende Studie 290
Tab. 34: Teilnehmerzahlen der einzelnen Befragungsrunden 293
Tab. 35: Demografische Angaben zum Expertenpanel (basierend auf Runde 1) 294
Tab. 36: Befragungsergebnisse zu den Anforderungen für ein strategisches GRC-Management (1 von 2) 301
Tab. 37: Befragungsergebnisse zu den Anforderungen für ein strategisches GRC-Management (2 von 2) 302
Tab. 38: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (Rang 1 bis 10) [DandE = „Describe and Explain"] 304
Tab. 39: Verwendeter Forschungsprozess der Referenzmodellierung in Anlehnung an Becker et al. (2002, S. 36) und Thomas (2006, S. 244) 322
Tab. 40: Übersicht der ausgewählten Informations- und Referenzmodelle aus der GRC-Literatur (1 von 2) 331
Tab. 41: Übersicht der ausgewählten Informations- und Referenzmodelle aus der GRC-Literatur (2 von 2) 332
Tab. 42: Geordnete Übersicht zu den Modellelementen (1 von 4) 338
Tab. 43: Geordnete Übersicht zu den Modellelementen (2 von 4) 339
Tab. 44: Geordnete Übersicht zu den Modellelementen (3 von 4) 340
Tab. 45: Geordnete Übersicht zu den Modellelementen (4 von 4) 341
Tab. 46: Begründung der Beziehungen zwischen den Entitäten des Modells 343

Tab. 47: Herleitung von Informationsobjekten und Beziehungen aus den strategischen GRC-Anforderungen 346
Tab. 48: Beispiele zu den Informationsobjekten auf strategischer Ebene 362
Tab. 49: Beispiele zu den Informationsobjekten auf konzeptioneller Ebene 365
Tab. 50: Beispiele zu den Informationsobjekten auf operativer Ebene 368
Tab. 51: Übersicht der zur Evaluierung verwendeten Praxisbeispiele (1 von 2) 374
Tab. 52: Übersicht der zur Evaluierung verwendeten Praxisbeispiele (2 von 2) 375
Tab. 53: Charakteristika der Fallbeispiele (1 von 2) 376
Tab. 54: Charakteristika der Fallbeispiele (2 von 2) 377
Tab. 55: Zuordnung von wichtigen Begriffen aus den Fallbeispielen zu den Entitäten des Modells (1 von 2) 382
Tab. 56: Zuordnung von wichtigen Begriffen aus den Fallbeispielen zu den Entitäten des Modells (2 von 2) 383
Tab. 57: Weitere relevante Begriffe aus den Fallbeispielen, die nicht den Entitäten des entwickelten Modells zugeordnet werden konnten 387
Tab. 58: Auswertung der in der GRC-Literatur angewendeten Forschungsmethoden 410
Tab. 59: Überblick über Literaturreviews aus Teilbereichen von GRC (1 von 5) 412
Tab. 60: Überblick über Literaturreviews aus Teilbereichen von GRC (2 von 5) 413
Tab. 61: Überblick über Literaturreviews aus Teilbereichen von GRC (3 von 5) 414

Tab. 62: Überblick über Literaturreviews aus Teilbereichen von GRC (4 von 5) 415
Tab. 63: Überblick über Literaturreviews aus Teilbereichen von GRC (5 von 5) 416
Tab. 64: Literaturbelege zur Kodierung mit Zuordnung zu den Anforderungskategorien und Unterkategorien (1 von 5) 417
Tab. 65: Literaturbelege zur Kodierung mit Zuordnung zu den Anforderungskategorien und Unterkategorien (2 von 5) 418
Tab. 66: Literaturbelege zur Kodierung mit Zuordnung zu den Anforderungskategorien und Unterkategorien (3 von 5) 419
Tab. 67: Literaturbelege zur Kodierung mit Zuordnung zu den Anforderungskategorien und Unterkategorien (4 von 5) 420
Tab. 68: Literaturbelege zur Kodierung mit Zuordnung zu den Anforderungskategorien und Unterkategorien (5 von 5) 421
Tab. 69: Einteilung von gestaltungsorientierten Arbeiten nach Management-Methoden, Methoden zur Modellierung von GRC-Informationen und Automatisierungsmethoden 422
Tab. 70: Zuordnung der Veröffentlichungen zur Automatisierung der Compliance-Sicherung und Risikosteuerung zu den verschiedenen Automatisierungsansätzen 424
Tab. 71: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (vollständige Liste; 1 von 5) ... 425
Tab. 72: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (vollständige Liste; 2 von 5) ... 426
Tab. 73: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (vollständige Liste; 3 von 5) ... 427
Tab. 74: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (vollständige Liste; 4 von 5) ... 428
Tab. 75: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (vollständige Liste; 5 von 5) ... 429

Tab. 76: Bedeutung der Anforderungen und Forschungsbedarfe nach Anforderungskategorien 430
Tab. 77: Bedeutung der Forschungsbedarfe nach dem Forschungsansatz 430
Tab. 78: Weitere Auswertungen zu den Anforderungen (1 von 2) [ID=Identifier; M_{Diff} = Differenz der Mittelwerte; R = Runde, $Rang_{Diff}$ = Differenz der Ränge; CV = Variationskoeffizient, CV_{Diff} = Differenz der Variationskeoffizienten] 431
Tab. 79: Weitere Auswertungen zu den Anforderungen (2 von 2) [$Q_{0,25}$ = 0,25-Quantil (unteres Quartil); $Q_{0,75}$ = 0,75-Quantil (oberes Quartil); IQR = Interquartilsabstand; IQR_{Diff} = Differenz der Interquartilsabstände] 432
Tab. 80: Weitere Auswertungen zu den Forschungsbedarfen (1 von 2) [ID = Identifier; M_{Diff} = Differenz der Mittelwerte; R = Runde, $Rang_{Diff}$ = Differenz der Ränge; CV = Variantionskoeffizient, CV_{Diff} = Differenz der Variantionskeoffizienten] 433
Tab. 81: Weitere Auswertungen zu den Forschungsbedarfen (2 von 2) [$Q_{0,25}$ = 0,25-Quantil (unteres Quartil); $Q_{0,75}$ = 0,75-Quantil (oberes Quartil); IQR = Interquartilsabstand; IQR_{Diff} = Differenz der Interquartilsabstände] 435
Tab. 82: Zuordnung von weiteren Entitäten aus den bestehenden konzeptionellen Modellen zu den Informationsobjekten des Modells 437
Tab. 83: Definition der Informationsobjekte des Modells 438

Abkürzungsverzeichnis

4R	Return, Risk, Regulation und Reporting
ACIS	Australian Conference on Information Systems
ACM	Association for Computing Machinery
AIS	Association for Information Systems
AISeL	AIS Electronic Library
AMCIS	Americas Conference on Information Systems
AMG	Arzneimittelgesetz
ArchiMate	Enterprise Architecture at Work
ARIS	Architektur Integrierter Informationssysteme
BDSG	Bundesdatenschutzgesetz
BilMoG	Bilanzmodernisierungsgesetz
BPM	Business Process Management
BPMN	Business Process Modeling Notation
CAISE	Conference on Advanced Information Systems Engineering
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CV	Variationskoeffizient
DCGK	Deutscher Corporate Governance Kodex

DESRIST	International Conference on Design Science Research in Information Systems and Technology
DIN	Deutsche Institut für Normung
DandE	Describe and Explain (Beschreiben und Erklären)
DRS	Deutscher Rechnungslegungsstandard
DSR	Deutscher Standardisierungsrat
DT	Diffusionstheorie
ECIS	European Conference on Information Systems
EPK	Ereignisgesteuerte Prozesskette
ER	Entity Relationship
ERP	Enterprise Resource Planning
EU	Europäische Union
FDA	Food and Drug Administration
GAMP	Good Automated Manufacturing Practice
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GMP	Good Manufacturing Practice
GoM	Grundsätze ordnungsmäßiger Modellierung
GPM	Geschäftsprozessmanagement
GRC	Governance, Risk and Compliance
GRCIS	International Workshop on Governance, Risk and Compliance
GVK	Gemeinsamer Verbundkatalog
GDT	General Deterrence Theorie
GxP	Gute Arbeitspraxis
HGB	Handelsgesetzbuch
HICSS	Annual Hawaii International Conference on System Sciences

HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
ICDE	International Conference on Data Engineering
ICSL	Internal Controls Scripting Language
ICSOC	International Joint Conference on Service Oriented Computing
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
IEB	Integrated Enterprise Balancing
IEEE	Institute of Electrical and Electronics Engineers
IFRS	International Financial Reporting Standards
IIA	Institute of Internal Auditors
IKS	Internes Kontrollsystem
IT	Informationstechnologie
ITGI	IT Governance Institute
ITK	Informations- und Kommunikationstechnologie
IS	Information System
ISACA	Information Systems Audit and Control Association
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library
InT	Institutionalistische Theorie
IQR	Interquartilsabstand
KonTraG	Gesetzt zur Kontrolle und Transparenz im Unternehmensbereich
LNBIP	Lecture Notes in Business Information Processing
LNCS	Lecture Notes in Computer Science

LNI	Lecture Notes in Informatics
MBV	Market-based view
M	Mittelwert
MaRisk	Mindestanforderungen an das Risikomanagement
MEMO	Multi-Perspective Enterprise Modelling
MIS	Management Information System
MIT	Massachusetts Institute of Technology
MKWI	Multikonferenz Wirtschaftsinformatik
MobIS	Modellierung betrieblicher Informationssysteme
OCEG	Open Compliance and Ethics Group
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OCT	Organisational Control Theorie
PaaS	Platform as a Service
PACIS	Pacific Asia Conference on Information Systems
PCAOB	Public Company Accounting Oversight Board
PAT	Prinzipal-Agenten-Theorie
PS	Prüfungsstandard
PwC	PricewaterhouseCoopers
RFID	Radio-Frequency Identification
RBV	Resource-based view
SaaS	Software as a Service
SAS	Service Organization Auditing Standards
SHT	Stakeholdertheorie
SD	Standardabweichung
SteT	Stewardship-Theorie
SEC	Securities and Exchange Commission
SLA	Service Level Agreement

SOA	Serviceorientierte Architektur
SOM	Semantisches Objektmodell
SOX	Sarbanes-Oxley-Act
SOX Sec. 404	Sarbanes-Oxley-Act Section 404
TAM	Technology Acceptance Model
TSM	Theorie der Schutzmotivation
TÜH	Theorie des überlegten Handelns
TGV	Theorie des geplanten Verhaltens
TRE	Theorie der rationalen Entscheidung
TKT	Transaktionskostenökonomik/-theorie
TransPuG	Transparenz- und Publizitätsgesetz
UML	Unified Modeling Language
US-GAAP	United States Generally Accepted Accounting Principles

1 Einleitung

1.1 Ausgangssituation und Problemstellung

GRC als Abkürzung für „Governance, Risk and Compliance“ hat sich seit dem Jahr 2004, als der Begriff das erste Mal in einer Veröffentlichung von PricewaterhouseCoopers (PwC; PwC 2004) aufgebracht wurde, zu einem verbreiteten Schlagwort in Forschung und Unternehmenspraxis entwickelt. Bedeutende Software- und Beratungsunternehmen führen Angebote unter diesem Akronym. Unter GRC werden jedoch eine Vielzahl verschiedener Ansätze und Themen subsumiert. So versieht das Softwareunternehmen SAP Lösungen zur Vergabe und Kontrolle von Zugriffsrechten (SAP Access Control), zur Kontrolle von Geschäftsprozessen (Process Control), zum Außenhandel (Global Trade Services), zu Umwelt-, Gesundheits- und Arbeitsschutz bis hin zu einer Risikomanagement-Lösung (SAP Risk Management) mit dem Oberbegriff GRC (SAP 2015). In der Forschungsliteratur ist das Schlagwort zwar weniger verbreitet, jedoch lassen sich unter diesem Themengebiet ebenso eine Vielzahl von Ansätzen und Perspektiven einordnen. Diese reichen von Arbeiten zur Berücksichtigung von Risiken und Kontrollen in Geschäftsprozessmodellen (siehe bspw. Sadiq et al. 2007; Rieke und Winkelmann 2008), Automatisierungsansätzen für Kontrollen (siehe bspw. El Kharbili et al. 2008c; Sadiq et al. 2007; Sackmann 2008c; Sackmann und Kähmer 2008), Arbeiten zu Verhaltensaspekten hinsichtlich der Befolgung von Compliance-Vorgaben, insbesondere im Kontext der Informationssicherheit (siehe bspw. Boss et al. 2009; Herath und Rao 2009; Johnston und Warkentin 2010), bis hin zu Management-Ansätzen für GRC (siehe bspw. Menzies 2006; OCEG 2009; Racz et al. 2010b; Racz et al. 2010c; Racz et al. 2011b, Vicente und da Silva 2011a; Vicente und da Silva 2011b).

Die Vielzahl an möglichen Ansätzen und Werkzeugen spiegelt sich in der Unternehmenspraxis oft in isolierten Initiativen wider (Böhm 2008, S. 22; Gericke et al. 2009a, S. 1; Marinos et al. 2009, S. 367; Menzies 2006, S. 63-64; Oh et al. 2007, S. 1; Racz et al. 2010a, S. 1; van der Veen et al. 2011, S. 265). Solche siloartigen und nicht integrierten Ansätze zeigen jedoch methodische Schwächen. Einerseits kann Governance nur dann die Aufgabe der Unterstützung strategischer Entscheidungen erfüllen, wenn hierfür aus dem Risiko- und Compliance-Management geeignete Informationen zur Verfügung stehen. Sind relevante Informationen für die strategische Entscheidungsebene nur siloartig vorhanden und können daher nur ausschnittsweise weitergegeben werden, kann dies im schlechtesten Fall zu fehlenden Informationen und falschen strategischen Entscheidungen führen.[1] Außerdem können mögliche Überschneidungen und Abhängigkeiten kaum berücksichtigt werden, was die Nutzung von Synergien verhindert. Da ein Gesamtüberblick aller Aktivitäten sowie des Compliance-Status und der Risikosituation wohl nur in den seltensten Fällen verfügbar ist, entsteht die Gefahr von Doppelarbeiten, aber auch von Lücken.

Die einzelnen Themengebiete Governance, Risiko- und Compliance-Management sind nicht neu, sondern in der Literatur seit Jahren thematisiert und in der Praxis mindestens genauso lang praktiziert. Interessanterweise ist ihre Bedeutung sowohl im unternehmensweiten („corporate“) Kontext als auch in der Informationstechnologie (IT) in den letzten Jahren nochmals gestiegen. Als Auslöser hierfür nennt Racz (Racz 2011, S. 16-20) Entwicklungen in allen Bereichen von GRC. Hierzu

[1] Siehe bspw. die Ausführungen von Oh et al. (2007) zu Nachteilen von siloartigen Ansätzen im Kontext des Risikomanagements.

gehören Governance-Skandale, wie der von Enron und eine verschärfte Risikosituation, bedingt durch Instabilität der internationalen Märkte, Globalisierung, Umweltrisiken sowie politische Risiken und Terrorismus. Außerdem werden von Racz (Racz 2011, S. 18-20) „unzählige" Regulierungen genannt. Hierzu gehören der Sarbanes-Oxley-Act (SOX) von 2002 und ähnliche Initiativen, wie in Deutschland das Bilanzmodernisierungsgesetz (BilMoG) sowie industriebspezifische Regulierungen, wie im Finanzdienstleistungsbereich „Basel II", „Basel III" und die „Mindestanforderungen an das Risikomanagement" (MaRisk). Weitere Regulierungen werden mit der „EU Data Protection Directive" (Directive 95/46/EC), dem Bundesdatenschutzgesetzt und dem amerikanischen Health Insurance Portability and Accountability Act (HIPAA) im Bereich des Datenschutzes sowie mit Vorgaben zur Finanzberichtserstattung, wie dem International Financial Reporting Standards (IFRS), dem United States Generally Accepted Accounting Principles (US-GAAP) sowie dem Handelsgesetzbuch (HGB) einschließlich dem Gesetzt zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) genannt. Auf die IT wirken diese Regulierungen mittelbar durch ihre Rolle bei der Unterstützung der jeweiligen Geschäftsprozesse. Zum anderen lassen sich aus diesen Regulierungen auch Vorgaben für die Entwicklung und den Betrieb von Informationstechnologie ableiten. IT-Abteilungen sind somit ebenfalls betroffen, wobei auf dieser Ebene ebenfalls vielfältige Standards und Best Practices wie die Control Objectives for Information and Related Technology (COBIT) und die IT Infrastructure Library (ITIL) sowie bspw. die Standards ISO 38500 oder ISO 27001/2 und industriespezifische Rahmenwerke wie die Good Automated Manufacturing Practice (GAMP) für die Pharmaindustrie existieren. Insbesondere für international agierende Konzerne ergibt sich hieraus die Komplexität mehrere Vorgaben zugleich erfüllen

zu müssen. Eine global agierende IT-Abteilung muss hierbei bspw. alle Vorgaben der jeweiligen Landesgesellschaften erfüllen.

Die ursprünglich abgegrenzten Konzepte für die Teilaufgaben von GRC weiten sich aufgrund dieser aktuellen Herausforderungen aus und konvergieren. Ein Beleg hierfür ist der weitgefasste Compliance-Begriff, der nicht nur auf Gesetze abzielt, sondern interne und externe sowohl verpflichtende als auch freiwillige Vorgaben, also auch Standards und Best Practices sowie Verträge und interne Richtlinien beinhaltet (Johannsen und Goeken 2006, S. 10). Das Risikomanagement wurde zudem, z.B. im Rahmen der Umsetzung eines internen Kontrollsystems, stärker formalisiert, um regulatorischen Ansprüchen zu genügen. Die jeweils gewählten Perspektiven in den GRC-Teilbereichen bleiben jedoch noch recht verschieden. Ein hohes Integrationspotential zwischen den GRC-Teilaufgaben lässt sich konstatieren, da eine Vielzahl von Berührungspunkten existieren (Teubner und Feller 2008, S. 406-407), wobei sich die Konzepte auf verschiedene Hierarchieebenen konzentrieren. Während die Corporate Governance die Unternehmensspitze tangiert und Risikomanagement vorwiegend als Managementaufgabe verstanden wird, betrifft die Compliance alle Mitarbeiter bei der Ausführung der operativen Tätigkeiten (Menzies 2006, S. 334-336).

Aktuelle Studien zur Situation von GRC in der Praxis zeigen ein signifikantes voranschreiten der Integration in den letzten Jahren (OCEG 2015, S. 13), womit neben den Zielen der Verbesserung von GRC und Kosteneinsparungen auch die Hoffnung von Performanceverbesserungen der Kernprozesse verbunden ist (OCEG 2012; OCEG 2015). Insbesondere in hochregulierten Branchen wie der Pharmaindustrie und der Finanzdienstleistungsbranche ist GRC mit erheblichen Kosten verbunden. Peek und Rhode (2010, S. 3) kommen in einer Studie unter großen amerikanischen Finanzdienstleistungsunternehmen hinsichtlich

der Kosten von Compliance zu dem Ergebnis, dass die durchschnittlichen Compliance-Kosten in den Jahren 2002 bis 2006 um 159 Prozent gestiegen sind. In absoluten Zahlen beliefen sich die geschätzten Kosten für das Compliance-Management in den befragten Unternehmen in einer Spanne von 200 bis 400 Millionen US-Dollar pro Jahr. Hierbei ist anzumerken, dass nur direkte Kosten des Compliance-Managements wie Personalkosten, IT-Kosten und Beratungskosten betrachtet wurden. Es ist zu bedenken, dass GRC nicht lediglich die einmalige Umsetzung einer bestimmten regulatorischen Vorgabe bedeutet. Vielmehr müssen erhebliche Anstrengungen unternommen werden, um einen regelkonformen Zustand dauerhaft zu erhalten. Neben diesen direkten Kosten zur Etablierung und Aufrechterhaltung des GRC-Systems existieren zudem weitere Kosten, welche im Rahmen der Ausführung der Geschäftsprozesse in den regulierten Bereichen entstehen. So ist mit der Normerfüllung in der Regel einer Formalisierung der betrieblichen Abläufe durch Arbeitsanweisungen und entsprechende Dokumentation verbunden. Außerdem können Flexibilitätseinbußen entstehen. Ein einfaches Beispiel hierfür sind durch Regulierungen wie den SOX verpflichtend gewordene Softwaretests in der IT, um nachzuweisen, dass technische Änderungen die Funktionsfähigkeit der internen Kontrollen zur Finanzberichterstattung nicht beeinträchtigen. Hierdurch kann zwar das Risiko von softwareinduzierten Fehlern reduziert und somit die Qualität der Software verbessert werden, jedoch wird, neben den für die Tests anfallenden Kosten, gegebenenfalls auch die Reaktionsgeschwindigkeit der IT auf geänderte Benutzeranforderungen vermindert.

GRC wird als Folge dieser Entwicklungen derzeit als Bürde für das Geschäft und als Kostenverursacher wahrgenommen. Zwischen regulatorischen Erfordernissen und der strategischen Zielerreichung wird somit ein Zielkonflikt („trade-off“) vermutet (Böhm et al. 2009, S. 7).

Gleichzeitig wird das ökonomische Umfeld für Unternehmen zunehmend schwieriger und ist geprägt von zunehmender Internationalisierung, kürzer werdenden Produktlebenszyklen und schnelleren technologischen Entwicklungen (Schmelzer und Sesselmann 2013, S. 1-2). Im Kontext der Informationstechnologie ist die Erzielung eines Wertbeitrags daher ein wichtiger Bestandteil der IT-Governance (Johannsen und Goeken 2006). In diesem Spannungsfeld aus regulatorischem und wirtschaftlichem Druck gilt es, auch die Chancen von GRC zu erkennen und zu nutzen. Im Rahmen dieser Arbeit wird der Standpunkt vertreten, dass GRC nicht lediglich als Kostentreiber, sondern als strategische Chance begriffen werden sollte. Diese Chance besteht unter anderem darin, die durch GRC entstehenden Nutzenpotentiale, bspw. hinsichtlich der Verbesserung von Geschäftsprozessen, bestmöglich zu Nutzen.

In der Literatur existieren bereits einige Arbeiten, die den Aspekt der Integration der GRC-Teildisziplinen aufgreifen (siehe bspw. Krey 2010; Krey et al. 2011; Krey 2012; Krey et al. 2012; Menzies 2006; OCEG 2009; Racz et al. 2010b; Racz et al. 2010c; Racz et al. 2011b; Vicente und da Silva 2011a; Vicente und da Silva 2011b). Gegenwärtige Ansätze wie das GRC Capability Model der Open Compliance and Ethics Group (OCEG 2009) oder von Racz et al. (2010b; 2010c; 2011b) stellen den Managementprozess von GRC ins Zentrum ihrer Betrachtungen. Das GRC Capability Model stellt detailliert mögliche GRC-Aktivitäten dar, die Integration von GRC wird jedoch nicht explizit herausgestellt. Es bleibt ebenso unklar, wie der Ansatz in bestehende Rahmenwerke integriert werden kann. Letztlich werden Governance-Aspekte nur eingeschränkt einbezogen (siehe auch Kritik von Racz et al. 2010c, S. 2). Auch bleiben die Begriffe teilweise unklar bzw. nicht verwendete aber geläufige Begriffe können nicht zugeordnet werden.

Ebenso wirkt der Ansatz in sich unvollständig, da nicht eindeutig dargestellt wird, welche Anforderungen ein solcher Ansatz zu erfüllen hat und welche Ziele damit verwirklicht werden können. Racz et al. (2010b) entwickeln aufbauend auf einer eigenen Definition für GRC zum einen ein sogenanntes Rahmenwerk für die GRC-Forschung, wobei das bekannte GRC-Dreieck um weitere Aspekte der Definition ergänzt wird.[2] Außerdem entwickeln Racz et al. (2010c; 2011b) ein Prozessmodell für GRC im Kontext der Informationstechnologie („IT-GRC"). Es wird hierbei deutlich, dass in den einzelnen GRC-Teilbereichen eine ähnliche methodische Vorgehensweise angewendet werden kann, konkrete Überschneidungen und Interdependenzen werden jedoch nicht herausgestellt. Vicente und da Silva (2011a; 2011b) versuchen, im Gegensatz zu den auf den Managementprozess von GRC ausgerichteten Ansätzen, ein konzeptionelles Modell für ein integriertes Management von GRC zu entwickeln (Vicente und da Silva 2011b) und ergänzen dieses im Rahmen der Entwicklung eines „Business Viewpoint" um den Managementprozess (Vicente und da Silva 2011a), wobei auf das von Racz et al. (2010c; 2011b) entwickelte Prozessmodell für IT-GRC zurückrückgegriffen wird. Das konzeptionelle Modell wird im Wesentlichen anhand der Definitionen von Governance, Risiko- und Compliance-Management entwickelt. Insbesondere die Beziehungen der Modellelemente und somit die eigentlich thematisierten Integrationsaspekte von GRC erscheinen wenig begründet.[3] Die zuvor dargestellten Ansätze weisen zudem die Problematik auf, dass der Integrationsaspekt betont wird, jedoch weitere Anforderungen vernachlässigt oder nicht explizit

[2] Siehe Abschnitt 2.6.

[3] Für eine detaillierte Diskussion des Modells von Vicente und da Silva sei auf den Abschnitt 5.3.1.1 verwiesen.

dargestellt werden. Aus einer ganzheitlichen Perspektive betrachtet kann, und dies wird im weiteren Verlauf der Arbeit detailliert dargestellt, das GRC-Management jedoch nicht auf diesen Aspekt reduziert werden, sondern es ist zu vermuten, dass vielfältige Anforderungen an ein GRC-Management zu stellen sind. Durch die fehlende Explikation der Anforderungen und Ziele des GRC-Managements bleibt die Eingrenzung des Themengebiets außerdem insgesamt recht vage.

1.2 Forschungsziel und Forschungsfragen

Stölzle (2002, S. 519) bezeichnet den Gedanken der Leitidee als hilfreich, die eine erste Vorstellung über das zu bearbeitende Problemfeld vermitteln soll. Aufbauend auf dem zuvor dargestellten Spannungsfeld, liegt dieser Forschungsarbeit die Leitidee eines integrierten und strategisch ausgerichteten GRC-Managements zu Grunde, welches in Abgrenzung zu bestehenden Ansätzen als „strategisches GRC-Managements“ bezeichnet werden soll. Neben den beiden Aspekten der Integration und strategischen Ausrichtung wird hiermit auch der Management-Aspekt betont, womit eine sinnvolle Eingrenzung des Gegenstandsbereichs erfolgen soll. In Abgrenzung zur operativen Erfüllung verschiedener Vorgaben oder der Durchführung der risikosteuernden Maßnahmen, zielt das Management von GRC auf eine umfassende Planung und Steuerung des GRC-Status, eine Integration der Teilaspekte, Ausrichtung an den strategischen Zielen und kontinuierliche Verbesserung ab.

Obwohl Corporate Governance, Risiko- und Compliance-Management schon seit einigen Jahren als eigenständige Konzepte existieren, steht die Forschung zu integrierten GRC-Management-Ansätzen noch am Anfang und hat durch die neueren Entwicklungen an Komplexität und Aktualität gewonnen. Aus Sicht der Unternehmenspraxis ergibt sich

hierdurch die Notwendigkeit nach einem GRC-Management-Ansatz, der in der Lage ist, den bestehenden Herausforderungen zu begegnen sowie die bestehenden Management-Systeme einzuordnen und weiterzuentwickeln. Ein solcher GRC-Management-Ansatz liegt forschungsseitig bislang nicht vor. Neben den einleitend angeführten ersten Ansätzen, die eine Integration berücksichtigen, wird GRC in der Literatur überwiegend nicht als integrierter Ansatz betrachtet, und der Großteil der Literatur erfasst derzeit Einzelfragen aus den GRC-Teildisziplinen. Hierbei existieren sehr unterschiedliche Perspektiven auf das Themengebiet, und es werden unterschiedliche Ziele verfolgt, wobei unbeantwortet bleibt, wie die vereinzelten Vorschläge in einen umfassenden Ansatz zu integrieren sind. Obwohl es legitim ist sich innerhalb eines Forschungsvorhabens auf einzelne Aspekte eines Themengebietes zu konzentrieren, sollte eine solche Einschränkung idealerweise auf der Grundlage eines umfassenden Verständnisses des Themengebiets erfolgen. Hiermit ließen sich die Arbeiten einordnen, und es kann insbesondere beantwortet werden, welche Anforderungen damit unterstützt werden sollen. Die genannten Forschungsarbeiten, die integrative GRC-Ansätze betrachten, lassen zwar vermuten, dass der Integrationsaspekt von besonderer Bedeutung ist, jedoch kann das Themengebiet bei weitem nicht auf diesen beschränkt werden. Es ist derzeit nicht klar, welchen Anforderungen ein GRC-Management-Ansatz genügen muss. Neben der Automatisierung von Kontrollen oder der informationstechnischen Unterstützung des GRC-Managements sind hierbei auch organisatorische Aspekte zu berücksichtigen. Eine Kombination von informationstechnischen und organisatorischen Konzepten gewinnt auch an Bedeutung, da die Literatur nahelegt, dass der Wertbeitrag von IT langfristig signifikant steigt, wenn ihr Einsatz durch geeignete Organisationskonzepte komplementiert wird (Tallon et al. 2000).

Aufgrund des Forschungsstandes kann die Entwicklung eines Ansatzes für ein strategisches GRC-Management lediglich als Fernziel der GRC-Forschung formuliert werden. Der initialen Idee eines integrierten und strategisch ausgerichteten GRC-Managements folgend, ist es daher das Forschungsziel der vorliegenden Arbeit, ein allgemeines Verständnis für ein strategisches GRC-Management zu legen. Ein solches Verständnis liefert zum einen wichtige Hinweise zur Etablierung, Bewertung und Weiterentwicklung von GRC-Management-Ansätzen in der Praxis. Darüber hinaus soll dieses Verständnis jedoch insbesondere auch weitere Forschungsanstrengungen leiten. Wie noch weiter zu zeigen sein wird, sind daher die folgenden Forschungsfragen, welche die Arbeit leiten sollen, zur Erreichung dieses Forschungsziels relevant.

1. Welche Anforderungen sind an einen strategischen GRC-Management-Ansatz zu stellen?
2. Welcher Forschungsstand existiert und welcher weitere Forschungsbedarf ist evident?
3. Wie kann der Forschungsbedarf strukturiert werden?
4. Welche Informationen sind für GRC relevant und welche Beziehungen existieren zwischen diesen Informationen?

Die Beantwortung der Forschungsfrage hinsichtlich der Anforderungen für das strategische GRC-Management bildet den Ausgangspunkt des hier dargestellten Forschungsvorhabens und stellt gleichzeitig eine zentrale Vorarbeit für die Beantwortung der weiteren Forschungsfragen dar. Die Anforderungen werden zur Strukturierung der GRC-Forschung herangezogen und liefern gleichzeitig eine grobe Definition des Gegenstandsbereichs des strategischen GRC-Managements. Die Diskussion des Forschungsstandes sowie die Herleitung des weiteren Forschungsbedarfs werden anhand der Anforderungen systematisiert. Da bislang

nur wenige Arbeiten zum integrierten Management existieren, sollten im Rahmen der Aufarbeitung des Forschungsstandes im Sinne kumulativer Forschung auch Arbeiten aus den Teilbereichen von GRC einbezogen werden. Der herzuleitende Forschungsbedarf soll insbesondere das genannte Fernziel der GRC-Forschung, also die Entwicklung eines Ansatzes für das strategische GRC-Management, unterstützen. Dieser Forschungsarbeit liegt weiterhin der Gedanke zu Grunde, dass ein Verständnis der für GRC-relevanten Informationen sowie deren Beziehungen von herausragender Bedeutung ist. Hiermit wird die Grundlage für ein einheitliches Begriffsverständnis gelegt, eine detailliertere Definition des Gegenstandsbereiches eines strategischen GRC-Managements gegeben und wichtige Aspekte hinsichtlich der bedeutsamen Elemente für eine strategische Ausrichtung und Integration des GRC-Managements geklärt. Auch zur Beantwortung dieser Forschungsfrage werden die zuvor hergeleiteten Anforderungen für das strategische GRC-Management herangezogen. Sie dienen in diesem Kontext als eine der Wissensquellen zur Entwicklung der relevanten Informationen sowie deren Beziehungen. Die Forschungsfragen beziehen sich somit auf die Kernelemente, die zur Grundlegung eines allgemeinen Verständnisses für das strategische GRC-Management notwendig sind und weisen gleichzeitig eine logische Beziehung zueinander auf.

1.3 Forschungsmethodische Positionierung

Dieser Abschnitt stellt forschungsmethodische Grundlagen dar, die für das hier dargestellt Forschungsvorhaben relevant sind. Zum anderen soll der Abschnitt eine Einordnung der Forschungsarbeit in den Gegenstandsbereich der Wirtschaftsinformatik und Managementforschung ermöglichen.

Gegenstandbereich der Wirtschaftsinformatik sind Informations- und Kommunikationssysteme in Wirtschaft und Verwaltung (Heinrich et al. 2007, S. 14; Mertens et al. 2012, S. 1; Österle et al. 2010, S. 3; o.V. 2013, S. 382). Als Aufgabe der Wirtschaftsinformatik kann die „Entwicklung und Anwendung von Theorien, Konzepten, Modellen, Methoden und Werkzeugen für die Analyse, Gestaltung und Nutzung von Informationssystemen" (o.V. 2013, S. 382) bezeichnet werden, wobei der Begriff Informationssystem gleichbedeutend zur Bezeichnung Informations- und Kommunikationssystem verwendet wird. Bestandteile von Informationssystemen sind Aufgaben, Menschen und die Informationstechnik (Heinrich et al. 2007, S. 16). Informationssysteme werden daher auch als sozio-technische Systeme bezeichnet (Österle et al. 2010, S. 3). Mertens (1995, S. 48) bezeichnet mit „sinnhafte[r] Vollautomatisierung" das langfristige Ziel der Wirtschaftsinformatik. Die Wirtschaftsinformatik ist eine wirtschafts- und sozialwissenschaftliche Disziplin, die eine ingenieurswissenschaftliche Durchdringung aufweist (Heinrich et al. 2007, S. 13; Mertens et al. 2012, S. 7). Sie beschäftigt sich mit Objekten der Wirklichkeit und kann somit als Realwissenschaft bezeichnet werden. Außerdem weist die Wirtschaftsinformatik formalwissenschaftliche Einflüsse auf (Heinrich et al. 2007, S. 50). Die Wirtschaftsinformatik greift auf Ansätze der Wirtschaftswissenschaft (Betriebswirtschaftslehre und gelegentlich Volkswirtschaftslehre) und der Informatik zurück.

Die Beziehung zur Betriebswirtschaftslehre ist für die Thematik dieser Arbeit von besonderer Bedeutung. Die Betriebswirtschaftslehre will als anwendungsorientierte Wissenschaft Handlungsempfehlungen für das Wirtschaften in Betrieben erteilen (Wöhe und Döring 2013, S. 27). Betriebe, die somit der Gegenstandsbereich der Betriebswirtschaftslehre sind, werden als „planvoll organisierte Wirtschaftseinheit in der Pro-

duktionsfaktoren kombiniert werden, um Güter und Dienstleistungen herzustellen und abzusetzen“ (Wöhe und Döring 2013, S. 27) verstanden. Weiterhin ist die vorliegende Arbeit im Kontext der Managementforschung zu verorten, die einen Teilbereich der Betriebswirtschaftslehre darstellt. Management ist das Erkenntnisobjekt der Managementforschung (Staehle und Conrad 1999, S. 34 und S. 95-100).[4] Ein strategischer GRC-Management-Ansatz sollte sowohl die Organisationsstruktur einschließlich der Rollen und Verantwortlichkeiten, die Managementprozesse sowie die notwendigen Methoden und Werkzeuge für das GRC-Management beinhalten. Informationssysteme sind somit ein wesentlicher Bestandteil eines solchen Ansatzes. Es kann argumentiert werden, dass Informationssysteme einen signifikanten Einfluss auf ihre organisatorische Umgebung haben. Dies erfordert eine integrierte Betrachtung von Fragestellungen des Managements bzw. der Organisationsgestaltung sowie der Informationstechnik (Picot und Baumann 2009).

In der Wirtschaftsinformatik ist das methodologische Selbstverständnis in zwei Richtungen ausgeprägt (Wilde und Hess 2007). Zum einen existieren Methoden der Informationssystemgestaltung (Entwicklungsmethoden) und zum anderen Methoden der Erkenntnisgewinnung (Forschungsmethoden). Die Forschungsmethoden können hierbei im Lichte zweier erkenntnistheoretischer Paradigmen, dem gestaltungsorientierten oder konstruktionswissenschaftlichen Paradigma („Design Science“) und dem behavioristischen oder verhaltenswissenschaftlichen Paradigma („Behavioral Science“), betrachtet werden. Ziel der gestal-

[4] Zur Definition des Begriffs Management sowie der im Folgenden angesprochenen Bestandteile eines Management-Ansatzes siehe Abschnitt 2.8.

tungsorientierten Forschung ist die Entwicklung und Evaluierung von Artefakten für bislang ungelöste Problemstellungen (siehe bspw. March und Smith 1995). Als Artefakte können in Anlehnung an Hevner (begriffliche) Konstrukte, Modelle, Methoden und Instanzen unterschieden werden (Hevner et al. 2004, S. 78-79). Diese Artefakte weisen eine enge Verbindung zueinander auf. Konstrukte bieten die Sprache in welcher das Problem und der Lösungsraum beschrieben werden können. Modelle verwenden Konstrukte um Phänomene der realen Welt abzubilden. Sie helfen somit bei dem Verständnis der Probleme und möglichen Lösungen und unterstützen somit Designentscheidungen. Methoden definieren Prozesse zur Problemlösung. Letztlich bieten Instanzen in einem konkreten Anwendungsfeld die Möglichkeit der Evaluierung von Konstrukten, Modellen und Methoden. Ein wesentliches Beispiel für Instanzen in der Wirtschaftsinformatik sind Software-Prototypen. Das verhaltenswissenschaftliche Forschungsparadigma verfolgt eine reaktive Forschungsstrategie und untersucht existierende Informationssysteme hinsichtlich ihrer Auswirkungen auf Anwender, Unternehmen oder Märkte (Wilde und Hess 2007, S. 281).

Diese paradigmenorientierte Betrachtung der Forschungsmethoden auf Makroebene kann durch eine methodologische Betrachtung auf Mikroebene ergänzt werden. Hierbei werden einzelne Forschungsmethoden wie Fallstudien, Referenzmodellierung und argumentativ-deduktive Analyse betrachtet (Wilde und Hess 2007, S. 280-283). Diese Forschungsmethoden lassen sich nach den Dimensionen Formalisierungsgrad (quantitativ / qualitativ) und Paradigma (verhaltenswissenschaftlich / konstruktiv) ordnen (Wilde und Hess 2006, S. 10-14). In der angloamerikanischen Forschung existiert mit „Information Systems“ eine Disziplin, die hohe Gemeinsamkeiten mit der Wirtschaftsinformatik aufweist und daher als Schwesterdisziplin bezeichnet wird. Unter-

schiedlich ist insbesondere die forschungsmethodische Ausrichtung, die im Gegensatz zur Wirtschaftsinformatik verhaltenswissenschaftlich geprägt ist (siehe für eine Gegenüberstellung der Forschungsdisziplinen Herzwurm und Stelzer (2008)).

Organisationen können ebenfalls als Artefakte verstanden werden, und es ist somit auch ein gestaltungsorientierter Ansatz im Kontext der Management- bzw. Organisationsforschung anwendbar (van Aken und Romme 2009, S. 6).[5] Van Aken und Romme (2009, S. 8-10) weisen im Kontext gestaltungsorientierter Managementforschung explizit auf die Notwendigkeit der Synthese von Wissen aufbauend auf einem systematischen Review hin. Dies ist in Zusammenhang mit dem Konzept der evidenzbasierten Forschung zu sehen, das aus der Medizin bekannt ist, und im Rahmen des „Evidence-based Managements" auch Einzug in die Managementforschung nimmt.[6] Evidenzbasierte Forschung wird charakterisiert als eine „Erkenntnismethode, die klar definierte Kriterien für die Bewertung von wissenschaftlichen Studien sowie deren Synthese aufstellt" (Bayerl et al. 2009, S. 120).[7] Obwohl hierbei vornehmlich auf Metaanalysen von empirischen Arbeiten verwiesen wird, ist jedoch an anderer Stelle auch auf die Bedeutung strukturierter Literaturanalysen zur Synthese von Wissen hingewiesen worden (siehe bspw. Fettke (Fettke 2006a, S. 257-258)).

Diese Arbeit folgt dem Design-Science-Forschungsansatz (siehe für die Wirtschaftsinformatik bspw. Hevner et al. 2004; Hevner und Chatterjee

---

[5] Weitere Arbeiten zu Design Science im Kontext der Management- und Organisationsforschung existieren von Romme (2003), van Aken (2004), Huff et al. (2006) und Bate (2007).

[6] Siehe für Arbeiten im Kontext der Wirtschaftsinformatik bspw. Goeken und Patas (2010).

[7] Zur Begriffsabgrenzung siehe bspw. Goeken und Patas (2010, S. 174-175).

2010; March und Smith 1995; Österle et al. 2010), welches der vorherrschende Ansatz in der deutschsprachigen Wirtschaftsinformatik ist (Österle et al. 2010). Hevner et al. (2004, S. 80) stellen in ihrem vielbeachteten Beitrag ein Framework für die Information Systems-Forschung vor, das eine Kombination von behavioristischer und konstruktionsorientierter Forschung, hier bezeichnet als Design Science, darstellen soll. Auf der einen Seite dieses Rahmenkonzepts steht die Umwelt, die durch die Menschen, die Organisation und die Technologie konkretisiert wird. Aus der Umwelt ergeben sich die Geschäftsanforderungen, welche die Relevanz der Forschung bestimmen. Auf der anderen Seite steht die Wissensbasis, die aus Theorien und Artefakten ebenso wie aus Forschungsmethoden besteht. Die Anwendung der Wissensbasis hat wesentlichen Einfluss auf die Rigorosität der Forschung. Information Systems-Forschung erfolgt demnach in zwei komplementierenden Phasen. Die behavioristische Forschung entwickelt und begründet Theorien, die Phänomene mit Bezug zu Informationssystemen erklären und vorhersagen. Diese Theorien werden durch gestaltungsorientierte Forschung aufgegriffen um Artefakte zu entwickeln und zu evaluieren. Artefakte können wiederum Schwächen in Theorien aufdecken und eine Veränderung oder Verfeinerung dieser erforderlich machen.[8]

[8] Obwohl Hevner et al. das Ziel ihres Forschungsbeitrags mit „to describe the performance of design-science research in Information Systems via a concise conceptual framework and clear guidelines for understanding, executing, and evaluating the research" (Hevner et al. 2004, S. 75) angeben, kombiniert das Rahmenwerk behavioristische und gestaltungsorientierte Forschung („Figure 2 presents our conceptual framework for understanding, executing, and evaluating IS research combining behavioral-science and design-science paradigms. We use this framework to position and compare these paradigms." (Hevner et al. 2004, S. 79).

Des Weiteren entwickeln Hevner et al. in diesem Beitrag (Hevner et al. 2004, S. 11-25) Richtlinien für die gestaltungsorientierte Forschung, die im Rahmen der vorliegenden Arbeit berücksichtigt wurden. Der Design-Science-Forschungsansatz ist ein Problemlösungsprozess und beinhaltet die Konstruktion von wissenschaftlichen Artefakten (1) bspw. in Form eines Modells oder einer Methode. Weiterhin muss ein relevantes Problem (2) bearbeitet und einer (technologie-basierten) Lösung zugeführt werden. Darüber hinaus muss die Arbeit einen innovativen Beitrag (3) leisten und eine Evaluation (4) des entwickelten wissenschaftlichen Artefakts stattfinden. Weiterhin muss das wissenschaftliche Artefakt genau spezifiziert und konsistent sein. Dies bedeutet, dass Forschungsmethoden zur Konstruktion und Evaluation des Artefakts eingesetzt werden müssen (Research Rigor (5)). Der Prozess in dem das Artefakt entwickelt wurde, bzw. das Artefakt selbst, repräsentiert oder ermöglicht einen Suchprozess, in welchem ein Problemraum konstruiert und ein Mechanismus zur Lösungsfindung bereitgestellt wird (Design als Suchprozess (6)). Letztlich muss eine effektive Kommunikation (7) der Forschungsergebnisse stattfinden.

Für den Prozess gestaltungsorientierter Forschung gibt es verschiedene Vorschläge, die teilweise unterschiedliche Aspekte betonen. Das Memorandum gestaltungsorientierter Forschung (Österle et al. 2010, S. 4-5) schlägt einen vierstufigen Forschungsprozess vor, der aus den Phasen Analyse, Entwurf, Evaluation und Diffusion besteht. In der Phase Analyse wird das Forschungsproblem einschließlich der relevanten Einflussfaktoren identifiziert und somit das Forschungsziel sowie die Forschungsmethode festgelegt. Anschließend wird das Artefakt unter Anwendung der festgelegten Forschungsmethode(n) entwickelt und evaluiert. Abschließend findet die Diffusion der Forschungsergebnisse in den relevanten Zielgruppen statt, was insbesondere eine Publikation

der Forschungsergebnisse beinhaltet. Peffers et al. (2006, S. 2007) schlagen zur Produktion und Präsentation von Design-Science-Research einen sechsstufigen Prozess vor. Der Prozess besteht aus den sechs Phasen „Problem Identification & Motivation", „Objectives of a solution", „Design & Development", „Demonstration", „Evaluation" und „Communication", wobei verschiedene Rückkopplungen zwischen den Phasen relevant sind. Außerdem werden mögliche Einstiegspunkte zur Forschung identifiziert. Es sollen Ziele für die Forschung definiert werden, deren Erreichung im Rahmen der Evaluation kontrolliert werden. Die Kommunikation der Forschungsergebnisse und das damit verbundene Feedback stellt eine zweite Möglichkeit zur Verbesserung der zu entwickelten Methodik dar. Hierdurch erhält der Forschungsprozess einen iterativen Charakter. Neben der Hervorhebung der Bedeutung einer Definition der Forschungsziele, welche die Grundlage der Evaluation darstellen, betont der Prozess von Peffers et al. somit insbesondere die Demonstration der Artefakte. Diese weist explizit auf die Bedeutung der praktischen Anwendung des Artefakts hin, die jedoch z.B. im Rahmen der Durchführung einer Fallstudie ebenfalls der Evaluation dient.

Neben den zuvor dargestellten Grundlagen gestaltungsorientierter Forschung ist die Unterscheidung qualitativer und quantitativer Forschungsansätze, die aus der empirischen Sozialforschung stammt, relevant (Flick et al. 2008, S. 24; Tracy 2010). Während qualitative Forschung überwiegend im Entdeckungszusammenhang (explorative Forschung) angewendet wird, stehen quantitative Methoden überwiegend im Begründungszusammenhang. Qualitative Methoden erzeugen überwiegend qualitatives Datenmaterial (bspw. Interviews mit offenen Fragen) und wenden interpretative Auswertungsmethoden an. Hingegen werden Methoden, die überwiegend quantitative Daten erzeugen (bspw.

Fragebögen mit Skalen), der quantitativen Forschung zugeordnet. Die Forschung zu strategischen GRC-Management-Ansätzen befindet sich noch in einer frühen Phase. Daher ist dieses Forschungsvorhaben explorativer Natur und bezieht sich somit nicht auf das Testen von Hypothesen.

Die gewählte Forschungsstrategie kombiniert weiterhin verschiedene Datenquellen und Forschungsmethoden im Sinne einer Triangulation (siehe bspw. Flick et al. 2008, S. 309; Brühl und Buch 2006, S. 3). Für die Information Systems-Forschung bringt Mingers (2001, S. 243-244) zwei Hauptargumente für die Kombination von Forschungsmethoden vor. (1) Die Komplexität der Welt lässt sich nicht mit einer einzigen Forschungsmethode erfassen. Unterschiedliche Aspekte eines Phänomens können nur durch mehrere Forschungsmethoden umfassend analysiert werden. (2) Ein Forschungsvorhaben stellt einen Prozess mit mehreren Phasen dar. In den einzelnen Phasen ist der Forscher mit unterschiedlichen Herausforderungen konfrontiert, denen er nur durch den Einsatz mehrerer Forschungsmethoden adäquat begegnen kann.

1.4 Vorgehensweise

Die Vorgehensweise der Arbeit gliedert sich grob in Anlehnung an den zuvor erläuterten Forschungsprozess zur gestaltungsorientierten Forschung (Peffers et al. 2006; Peffers et al. 2007; Österle et al. 2010). Zur Beantwortung der dargestellten Forschungsfragen werden zwei Kernbereiche gebildet, und es ist eine zweimalige Durchführung des allgemeinen Forschungsprozesses notwendig. Konkret werden für die beiden Kernbereiche dieser Arbeit „Anforderungen und Forschungsagenda“ sowie „Datenseitiges Modell“ separate Forschungsprozesse durchgeführt. Die Anforderungen und Forschungsagenda sowie das datenseitige Modell eines strategischen GRC-Managements bilden somit die

Artefakte, die im Rahmen dieser Arbeit entworfen werden sollen. Insbesondere die Anforderungen und das datenseitige Modell stellen allgemeine Aussagen dar, die zur Lösung von konkreten Problemen in der Praxis, nämlich der (Weiter-)Entwicklung von GRC-Management-Ansätzen, verwendet werden können. Die Forschungsagenda wird ebenfalls als ein Artefakt gesehen, und es wird angenommen, dass ein gestaltungsorientierter Forschungsprozess zu ihrer Entwicklung sinnvoll angewendet werden kann. Insbesondere die Kernaufgaben gestaltungsorientierter Forschung, namentlich der Entwurf und die Evaluierung, erscheinen sinnvoll. Die Forschungsagenda soll Hinweise zur Weiterentwicklung des Forschungsfeldes strategisches GRC-Management geben. Die Festlegung der Forschungsziele und konkreten Forschungsmethoden zu den Bereichen erfolgt in den jeweiligen Kapiteln. Es ist zudem anzumerken, dass eine Demonstration als Teil der Entwicklung der Artefakte angesehen wird und lediglich für das datenseitige Modell stattfindet. Für die Forschungsagenda kann im eigentlichen Sinne keine Demonstration durch Anwendung stattfinden. Sie dient Forschern als Informationsquelle. Stattdessen wird dargestellt, wie die Forschungsagenda Forscher bei eigenen Forschungsvorhaben unterstützen kann.[9]

Es ist darauf hinzuweisen, dass durchaus Beziehungen zwischen diesen Forschungsprozessen bestehen. So baut der Forschungsprozess, der auf die Entwicklung eines datenseitigen Modells abzielt, auf den Ergebnissen des Forschungsprozesses zum Kernbereich „Anforderungen und Forschungsagenda“ auf. Insbesondere werden die durchgeführte Literatursuche sowie die entwickelten Anforderungen aufgegriffen. Abb. 1

[9] Siehe Abschnitt 3.6.4.

stellt die gewählte Vorgehensweise grafisch dar und unterscheidet neben den Kernbereichen, die Kernaktivitäten gestaltungsorientierter Forschung „Konstruktion“ und „Evaluierung“. Des Weiteren werden ausgewählte wichtige Aspekte der einzelnen Forschungsschritte stichwortartig dargestellt, um einen Überblick über die Forschungsarbeit zu gewähren.

Aufbauend auf dieser Strukturierung ist die Arbeit im Anschluss an dieses einleitende Kapitel wie folgt gegliedert. Kapitel 2 erörtert insbesondere die Grundlagen zu Governance, Risiko- und Compliance-Management sowie zu den Begriffen GRC und strategisches GRC-Management. Im anschließenden Kapitel 3 werden die Anforderungen hergeleitet, der Forschungsstand zum strategischen GRC-Management diskutiert sowie die Forschungsagenda entwickelt. In Kapitel 4 wird die Delphi-Studie zum strategischen GRC-Management dargestellt. Diese beinhaltet neben der Evaluierung der Forschungsergebnisse zu den Anforderungen und der Forschungsagenda insbesondere auch eine Priorisierung der Anforderungen und des Forschungsbedarfs. Das Kapitel 5 stellt die Entwicklung und Evaluierung des datenseitigen Modells für das strategische GRC-Management dar. Abschließend werden in Kapitel 6 die Ergebnisse zusammengefasst, kritisch gewürdigt, der Nutzen für Forschung und Praxis dargestellt sowie ein Ausblick gegeben.

Im Zuge der Erstellung dieser Arbeit sind verschiedene Publikationen (Marekfia und Nissen 2009; Marekfia und Nissen 2012; Marekfia und Nissen 2013; Marekfia und Nissen 2014; Nissen und Marekfia 2013; Nissen und Marekfia 2014) entstanden, die durch entsprechende Begutachtungsprozesse die Möglichkeit beinhalteten, die vorläufigen Forschungsergebnisse stetig weiterzuentwickeln. Diese Veröffentlichungen thematisieren jeweils Ausschnitte der vorliegenden Forschungsarbeit.

Für das einleitende Kapitel sowie das Kapitel zu den Grundlagen von Governance, Risiko- und Compliance-Management wurde auf die relevanten Abschnitte aller genannten Publikationen zurückgegriffen. Soweit eines der weiteren Kapitel (Kapitel 3 bis 6) auf den in einer Veröffentlichung dargestellten Forschungsergebnissen aufbaut, weist eine Fußnote zu Beginn des jeweiligen Kapitels darauf hin.

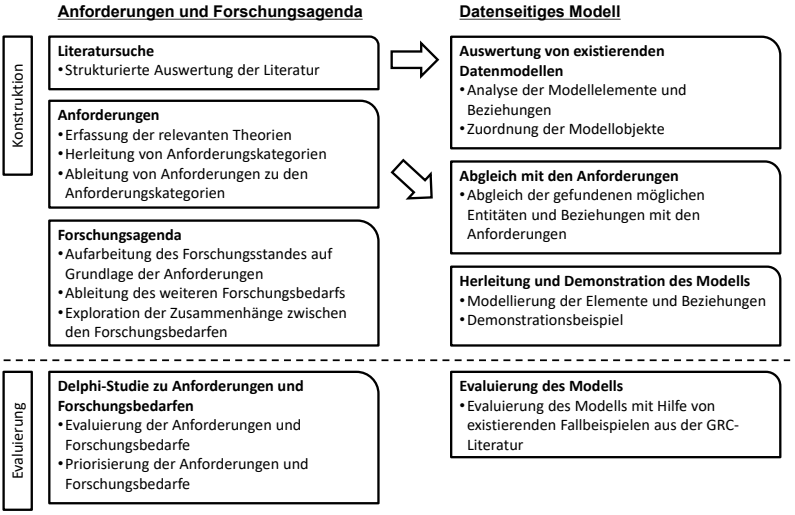

Abb. 1: Strukturierung der Arbeit anhand der Kernelemente „Anforderungen und Forschungsagenda“ und „Datenseitiges Modell“

2 Grundlagen zu Governance, Risiko- und Compliance-Management

2.1 Vorüberlegungen

In einer frühen Phase des Forschungsprozesses müssen die Schlüsselbegriffe definiert werden, und es sollten jene Forschungsbereiche identifiziert werden, die relevant für das verfolgte Forschungsziel sind (Torraco 2005, S. 359; vom Brocke et al. 2009, S. 9; Zorn und Campbell 2006, S. 175). Im diesen Kapitel sollen die für die weitere Arbeit relevanten Grundlagen gelegt, Begriffe definiert und in die jeweiligen Zusammenhänge eingeordnet werden. Hierbei konzentriert sich die Darstellung auf die Definition und Grundlegung der Konzepte Governance, Risiko- und Compliance-Management und deren Zusammenhänge. Hieraus wird der Begriff GRC hergeleitet. Des Weiteren werden Überlegungen zu eventuellen Unterschieden und Gemeinsamkeiten von unternehmensweiten und IT-bezogene Ansätzen angestellt. Außerdem findet eine Einführung in den Begriff des strategischen GRC-Managements statt, wobei auch dargelegt wird, welche grundlegenden Ideen diese Arbeit leiten. Abschließend sollen in diesem Kapitel weitere relevante Begriffe erläutert werden. Die Darstellungen in diesem Kapitel stellen somit auch eine erste Eingrenzung des Themengebiets dar. Diese Grundlegung der relevanten Konzepte ist eine wichtige Vorarbeit für alle weiteren Forschungsschritte insbesondere auch für den im Anschluss dargestellten Literaturreview. Es ist darauf hinzuweisen, dass die Betrachtung integrierter GRC-Ansätze auf strategischer Ebene noch in einem frühen Forschungsstadium ist. Ein Teil der relevanten Grundlagen für das strategische GRC-Management, wie bspw. die relevanten Theorien, werden daher erst im Rahmen des Literaturreviews hergeleitet.

Zur Darstellung der Grundlagen von GRC wird der Empfehlung von Baker (2000, S. 222) folgend im Wesentlichen auf Lehr- und Handbücher zurückgegriffen, da diese Übersichtsdarstellungen zu den GRC-Teildisziplinen enthalten. Die Analyse der Beziehungen und Integrationsaspekte der GRC-Teildisziplinen findet auf Basis der Publikationen statt, die im Rahmen des in Kapitel 3 durchgeführten Literaturreviews identifiziert wurden, und stellt somit teilweise einen Vorgriff auf die im weiteren Forschungsprozess erzielten Forschungsergebnisse dar. Anzumerken ist, dass eine detaillierte Analyse der Integration innerhalb der Entwicklung der Anforderungen stattfindet. Die Klärung der grundlegenden Zusammenhänge ist jedoch zur Motivation und zum Verständnis der weiteren Forschungsschritte von herausragender Bedeutung.

2.2 Corporate Governance und IT-Governance

Der Begriff Corporate Governance kann in einer engen Abgrenzung aus der Sicht des Shareholder-Ansatzes und in einer weiten Abgrenzung aus der Sicht des Stakeholder-Ansatzes erklärt werden (Witt 2003, S. 61-116; Mallin 2007, S. 159-265). Die Sicht des Shareholder-Ansatzes stellt im Wesentlichen das anglo-amerikanische Verständnis, das sich im SOX wiederspiegelt, dar. Die Sicht des Stakeholder-Ansatzes findet sich hingegen im Deutschen Corporate Governance Kodex (DCGK) (Regierungskommission DCGK 2010). Corporate Governance beinhaltet aus Sicht des Stakeholder-Ansatzes die Führung, Kontrolle und Steuerung von Unternehmen mit dem Ziel, einen Interessensausgleich zwischen allen Stakeholdern herzustellen (Witt 2003, S. 1-6). Corporate Governance liefert somit den strukturellen Rahmen für die Strategiefestlegung und die Mittel zu deren Umsetzung einschließlich der Erfolgskontrolle (OECD 2004, S. 11). Governance wird von Aufgaben

des Managements abgegrenzt (Bird 2001, S. 300). So wird unter anderem festgestellt, dass während Management täglich mit der Führung und der Umsetzung der Strategie beschäftigt ist, Governance lediglich die übergreifenden Unternehmensrichtlinien festlegt. Governance ist weiterhin die Autorität, die das Management beauftragt. Corporate Governance legt insbesondere die Grundsätze einer verantwortungsvollen Unternehmensführung sowie deren Kontrolle fest (Regierungskommission DCGK 2010).

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD 2004) formuliert insgesamt sechs Grundsätze der Corporate Governance, welche die Bereiche „Sicherung der Grundlagen eines effektiven Corporate-Governance-Rahmens", „Aktionärsrechte und Schlüsselfunktionen der Kapitaleigner", „Gleichbehandlung der Aktionäre", „Rolle der verschiedenen Unternehmensbeteiligten (Stakeholder) bei der Corporate Governance", „Offenlegung und Transparenz" sowie „Pflichten des Aufsichtsorgans (Board)" betreffen. Für Deutschland stellt der Deutsche Corporate Governance Kodex (Regierungskommission DCGK 2010) Empfehlungen und Anregungen für eine verantwortungsvolle Unternehmensführung zur Verfügung, die sich auf börsennotierte Gesellschaften beziehen. Von Empfehlungen, die innerhalb des Kodex mit dem Wort „soll" gekennzeichnet sind, können Unternehmen zwar abweichen, müssen diese Abweichung jedoch jährlich offenlegen („comply or explain"). Für Aktiengesellschaften nach deutschem Recht ist ein sogenanntes duales Führungssystem, das eine Trennung zwischen Vorstand und Aufsichtsrat beinhaltet, vorgeschrieben. Der Kodex befasst sich mit der Ausgestaltung von Aufsichtsrat, Hauptversammlung und Vorstand sowie dem Zusammenwirken zwischen Vorstand und Aufsichtsrat. Des Weiteren werden Empfehlungen

und Anregungen hinsichtlich der Transparenz, Rechnungslegung und Abschlussprüfung gemacht.

Der Term IT-Governance findet seit Beginn der 1990er Jahre Verbreitung (siehe z.B. Loh und Venkatraman 1992; Henderson und Venkatraman 1993) und wird im Allgemeinen als eine Teilmenge der Corporate Governance verstanden (Weill und Ross 2004, S. 4-10; van Grembergen et al. 2004, S. 4-7). Die Definition von IT-Governance wird in der Literatur kontrovers diskutiert, wobei entweder die Struktur oder der Prozess betont wird (Dahlberg und Kivijärvi 2006, S. 2-5; Grant et al. 2007, S. 2-3; Webb et al. 2006). Weil und Ross betonen die Struktur und definieren IT-Governance als „specifying the decision rights and accountability framework to encourage desirable behavior in using IT" (Weill und Ross 2004, S. 2). Eine bedeutende Arbeit, die bei der Definition von IT-Governance den Prozessaspekt betont, stammt von Van Grembergen et al. (2004). Dieser definiert IT-Governance als „the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT" (van Grembergen et al. 2004, S. 5). Das IT Governance Institute bringt diese Sichten in ihrer Definition zusammen und versteht unter IT-Governance „the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives" (ITGI 2007, S. 5). Die Definition von Van Grembergen et al. (2004, S. 5) befasst sich neben der Bedeutung der IT-Governance auf den unterschiedlichen Hierarchieebenen (Board, Executive Management, IT Management) im Wesentlichen mit der Ausrichtung der IT(-Ziele) an den Geschäftszielen, was als Business/IT-Alignment bezeichnet wird. Es kann des Weiteren als mittler-

weile akzeptiert angesehen werden, dass IT-Governance durch das Zusammenspiel von Strukturen, Prozessen und sogenannten relationalen Mechanismen, im Englischen als „relational mechanisms“ bezeichnet, implementiert werden kann (van Grembergen et al. 2004, S. 20). Teilweise werden die Sicherstellung des Wertbeitrags durch IT sowie die Sicherstellung der Compliance als Kernaufgaben von IT-Governance angesehen (ISO 2008; Raghupathi 2007; S. 94). Es werden jedoch auch weitere Aufgaben, wie Erfolgsmessung, Ressourcenmanagement und Risikomanagement (Grant et al. 2007, S. 5; Johannsen und Goeken 2006, S. 14; ITGI 2007, S. 6; van Grembergen et al. 2004, S. 7), der IT-Governance zugeordnet.

Auch im IT-Kontext wird auf die Unterscheidung von IT-Governance und IT-Management hingewiesen (van Grembergen et al. 2004, S. 5; Weill und Ross 2004, S. 8). Letzteres bezieht sich im Gegensatz zur IT-Governance auf die effektive und effiziente Bereitstellung der IT-Dienstleistungen und -Produkte sowie auf den operativen IT-Betrieb. Weil und Ross (2004, S. 8) führen aus, dass sich Governance darauf bezieht festzulegen, wer Entscheidungen trifft, während Management das Treffen und Umsetzen der Entscheidungen beinhaltet. Allgemein kann zudem festgestellt werden, dass strukturelle Fragen, wie die hinsichtlich zentraler oder dezentraler IT (Sambamurthy und Zmud 1999, S. 261) zuerst in der Literatur untersucht wurden. Im Anschluss wurde um der Komplexität von IT-Governance gerecht zu werden auch eine prozessorientierte Sichtweise auf die IT-Governance eingenommen (siehe bspw. Peterson 2000; Peterson et al. 2002).[10] Nach wirksam werden des SOX wurde IT-Governance stärker im Kontext der Corporate

[10] Zur Darstellung der Entwicklung der IT-Governance siehe bspw. Grant et al. (2007).

Governance verortet und die Kontrollprozesse fokussiert (Jacobson 2009, S. 3; Raghupathi 2007, S. 94). Eine wichtige Arbeit in diesem Kontext ist COBIT (ITGI 2007) vom IT Governance Institute (ITGI), die daher nachfolgend kurz erläutert werden sollen.

COBIT (ITGI 2007) ist ein Rahmenwerk für IT-Governance, das generelle Kontrollziele (engl. control objectives) für die IT-Prozesse zur Verfügung stellt.[11] Es wird daher auch für IT-Prüfungen von Revisoren und externen Auditoren verwendet. COBIT bezieht IT-Governance auf die „focus areas", „strategic alignment", „value delivery", „resource management", „risk management" und „performance measurement" (ITGI 2007, S. 6). Das Rahmenwerk beschreibt in der Version 4.1 weiterhin insgesamt 34 Prozesse für die IT, welche in die vier Domänen

- Planung und Organisation (engl. „Plan and Organise")
- Beschaffung und Implementierung (engl. „Acquire and Implement"),
- Betrieb und Unterstützung (engl. „Deliver and Support") sowie
- Überwachung und Bewertung (engl. „Monitor and Evaluate")

eingeteilt werden. COBIT definiert weiterhin für jeden IT-Prozess Kontrollziele, wobei jeweils ein übergeordnetes Kontrollziel und mehrere Detailziele vorgeschlagen werden. Kontrollen werden definiert als Richtlinien, Prozeduren, Praktiken und organisatorische Strukturen, die

[11] Im Rahmen dieser Arbeit wird konsistent die Version 4.1 von COBIT verwendet. Dies ist insbesondere in der weiten Verbreitung, hohen Bedeutung und großen Rezeption dieser Version sowie der ausführlichen Dokumentation der IT-Prozesse begründet. Die Version 5.0 von COBIT wurde 2012 freigegeben und ist als eine Weiterentwicklung der Version 4.1 zu verstehen. COBIT 5.0 verwendet insbesondere die Mehrzahl der IT-Prozesse aus der Version 4.1 (siehe http://www.isaca.org/COBIT/Documents/Compare-with-4.1.pdf, Abruf am 2015-10-02).

sicherstellen, dass Geschäftsziele erreicht und unerwünschte Ereignisse vermieden werden (ITGI 2007, S. 13). COBIT ermöglich darüber hinaus eine Messung des Reifegrads der IT-Prozesse.

Ein weiterer Standard zur IT-Governance stammt von der International Organization for Standardization (ISO). Der ISO-Standard 38500 (ISO 2008) definiert „Corporate Governance of Information Technology" als „[t]he system by which the current and future use of IT is directed and controlled." (ISO 2008, S. 3). Dem Standard entsprechend verfolgt IT-Governance sowohl „Conformance", womit Compliance gemeint ist, als auch „Performance", womit auf den Wertbeitrag der IT abgezielt wird. Das Rahmenwerk führt mit „Responsibility", „Strategy", „Acquisition", „Performance", „Conformance" und „Human Behaviour" insgesamt sechs Prinzipien ein. Diese werden für die Konkretisierung der drei Hauptaufgaben der IT-Governance, nämlich „Direct", „Evaluate" und „Monitor" herangezogen. Gegenstandsbereich der IT-Governance sind IT-Projekte und der IT-Betrieb. „Direct" ordnet die Verantwortlichkeiten zu und ist für die Erstellung von Plänen und Richtlinien zuständig. „Evaluate" beschreibt die Untersuchung des gegenwärtigen und zukünftigen IT-Einsatzes und ist somit Teil des Strategieprozesses. „Monitor" überwacht die Zielerreichung hinsichtlich Conformance und Performance.

2.3 Risikomanagement

Der Begriff Risiko wird kontrovers diskutiert, kann jedoch in Abgrenzung zu Chance als negative Abweichung eines tatsächlichen von einem erwarteten Ereignis definiert werden (bspw. KonTraG). Im Rahmen der Risikoaggregation kann es aufgrund von Kompensationseffekten sinnvoll sein, positive und negative Abweichungen zu betrachten (Gleißner 2011, S. 8-9; Strohmeier 2007, S. 34).

Das Committee of Sponsoring Organizations of the Treadway Commission (COSO) definiert Risikomanagement als ein Prozess um die das Unternehmen beeinflussenden Ereignisse zu erkennen, und hinreichende Sicherheit in Bezug auf die Erreichung der Ziele des Unternehmens zu gewährleisten (COSO 2004, S. 2). Im Risikomanagement können, wie vom Deutschen Standardisierungsrat (DSR) beispielhaft dargestellt (siehe DSR 5 zur Risikoberichterstattung), verschiedene Risikokategorien unterschieden werden (Kajüter 2001; Paetzmann 2008, S. 89-91). Diese sind Umfeld- und Branchenrisiken, unternehmensstrategische und leistungswirtschaftliche Risiken, Personalrisiken, informationstechnische und finanzwirtschaftliche Risiken sowie sonstige Risiken. Gemäß dieser Systematik bilden informationstechnische Risiken eine eigene Kategorie. Andere Autoren (siehe bspw. Prokein 2008, S. 9-11) subsumieren die IT-Risiken unter die operativen Risiken. Operative bzw. informationstechnische Risiken können nach ihrer Ursache in die Kategorien Prozesse und Organisation, Mitarbeiter, Infrastruktur und externe Ereignisse unterteilt werden (siehe Deutsche Bundesbank (2001, S. 28) und Gefährdungskataloge gemäß IT-Grundschutz).

Nachfolgend soll zur Veranschaulichung eines geschäftsprozessorientierten Risikomanagement-Ansatzes auf das Modell der COSO (2004) eingegangen werden, das im Kontext des SOX an Bedeutung gewonnen hat und von der Securities and Exchange Commission (SEC), der amerikanischen Börsenaufsichtsbehörde, zur Anwendung empfohlen wird (Johannsen und Goeken 2006) und somit auch für das Compliance-Management relevant ist. COSO stellt den eigenen Ansatz für ein unternehmensweites Risikomanagement als dreidimensionales Modell („Würfel“) dar, der aus Zielkategorien, Komponenten und Organisationseinheiten besteht. Die vier Zielkategorien sind strategisch, betrieb-

lich, Berichterstattung und Regeleinhaltung. Risikomanagement soll das Unternehmen bei der Zielerreichung unterstützen. Die dargestellten Zielkategorien sollen die Ausrichtung des Risikomanagements auf unterschiedliche Aspekte ermöglichen. Unter den strategischen Zielen werden die übergeordneten Ziele einer Organisation verstanden. Betriebliche Ziele betreffen den wirksamen und wirtschaftlichen Ressourceneinsatz. Die weiteren Ziele betreffen der Kategorisierung folgend die Zuverlässigkeit der Berichtserstattung und Einhaltung von relevanten Vorschriften. Aufgabe des unternehmensweiten Risikomanagements ist es, hinreichende Sicherheit zur Erreichung dieser Ziele zu gewährleisten. Als Organisationseinheiten werden Niederlassung, Geschäftseinheit, Geschäftsbereich und Gesamtorganisation unterschieden. Durch die Einbeziehung der Organisationseinheiten in das Modell soll es möglich werden, dass sich Risikomanagement im Sinne eines unternehmensweiten Ansatzes auf die Gesamtorganisation oder lediglich auf eine der Unterkategorien bezieht. Die Komponenten sind internes Umfeld, Zielfestlegung, Ereignisidentifikation, Risikobeurteilung, Risikosteuerung, Kontrollaktivitäten, Information und Kommunikation sowie Überwachung. Die Komponenten beschreiben somit den Prozess des Risikomanagements, wobei diese wechselseitig zueinander in Beziehung stehen. Sie werden weiterhin als Kriterien zur Beurteilung der Funktionsfähigkeit des Risikomanagements herangezogen. Interne Kontrollen werden als ein wesentlicher Bestandteil des Risikomanagements angesehen und sind daher in das Framework integriert. Es wird letztlich hinsichtlich der Rollen und Verantwortlichkeiten des Risikomanagements festgestellt, dass jede Person eines Unternehmens einen Teil der Verantwortung für das unternehmensweite Risikomanagement trägt. Dem Vorstand kommt jedoch besondere Bedeutung zu.

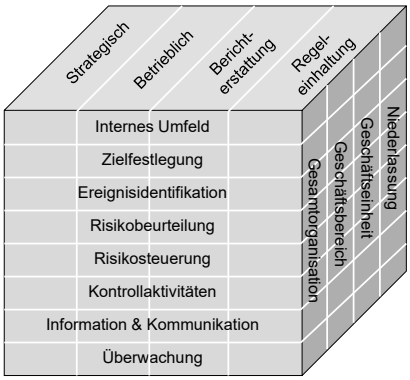

Abb. 2: Modell eines unternehmensweiten Risikomanagements gemäß COSO (COSO 2004, S. 5)

Die Komponenten des Risikomanagement-Rahmenwerkes der COSO weisen eine hohe Ähnlichkeit zu anderen Darstellungen des Risikomanagementprozesses in der Literatur auf. Obwohl die Verwendung der Bezeichnungen für die einzelnen Phasen teilweise unterschiedlich ist, werden im Wesentlichen die Phasen Risikoidentifikation, Risikobewertung, Risikobewältigung und Risikoüberwachung unterschieden (siehe bspw. Gleißner 2011, S. 41-47; Romeike und Brühwiler 2010, S. 95; Strohmeier 2007, S. 6).[12]

[12] Der Risikomanagement-Standard ISO 31000 der International Organization of Standardization (ISO) wird im Rahmen dieser Arbeit nicht betrachtet. Dies liegt darin begründet, dass es sich bei dem Standard um einen sehr allgemeinen und generischen Ansatz handelt (Romeike und Brühwiler 2010, S. 87). Zudem wurde zwischenzeitlich der nationale Entwurf dieses Standards durch das Deutsche Institut für Normung (DIN) zurückgezogen, was bedeutet, dass keine nationale Umsetzung des Standards in Deutschland stattgefunden hat.

2.4 Compliance-Management

Die Definition des Begriffs Compliance wird in ein enges und ein weites Verständnis unterteilt. Gemäß der engen Auffassung bedeutet Compliance die Einhaltung von gesetzlichen Anforderungen (Hauschka 2007, S. 2; Klotz 2007). Das weite Begriffsverständnis erstreckt sich auf die Einhaltung von internen und externen sowohl verpflichtenden als auch freiwilligen Vorgaben. Zu diesen Vorgaben gehören z.B. Gesetze, Standards und Best Practices sowie Verträge und Richtlinien (Tarantino 2007, S. 21-22; Pupke 2008, S. 9-24; Johannsen und Goeken 2006, S. 10). Compliance-Management ist dem weiten Begriffsverständnis folgend ein System, das die Einhaltung von internen und externen sowohl verpflichtenden als auch freiwilligen Vorgaben sicherstellt. Compliance bedeutet ins Deutsche übersetzt in etwa Einhaltung, Befolgung oder Übereinstimmung. Die Einhaltung von Gesetzen ist in Rechtsstaaten eine selbstverständliche Pflicht. Compliance geht, wie dargestellt, hierüber hinaus und verlangt, die Errichtung eines Systems, das die Einhaltung von gesetzlichen und weiteren Vorgaben sicherstellt (Hauschka 2007, S. 3). Der Compliance-Begriff sollte jedoch nicht auf die Sicherstellung der Erreichung jeder Art von geschäftlichen Zielen (Grundei und Talaulicar 2009, S. 73) bzw. auf die Vermeidung jeder Art von fehlerhaften Entscheidungen (Hauschka 2007, S. 4) ausgeweitet werden.

Von Klotz und Dorn (2008, S. 11-14) bzw. Klotz (2009, S. 20-25) wird ein Klassifikationsschema für die relevanten Regelwerke der IT-Compliance in Form eines Zwiebelmodells entworfen, das sich auch allgemein auf die Compliance anwenden lässt. Im Inneren dieses Zwiebelmodells stehen rechtliche Vorgaben, worunter alle Rechtsnormen verstanden werden, die zur Rechtsprechung herangezogen werden. In der zweiten Schicht von Innen, werden Verträge dargestellt, die mit

Kunden, Lieferanten oder sonstigen Geschäftspartnern abgeschlossen wurden. Danach kommen externe Regelwerke, die keinen rechtlichen Charakter haben. Hierzu gehören Standards und Best Practice-Rahmenwerke unterschiedlicher Institutionen, die Grundlage für eine Zertifizierung der Organisation sein können. In der äussersten Schicht befinden sich unternehmensinterne Regelwerke. Hierzu werden unter anderem Unternehmensrichtlinien, Verfahrensanweisungen oder Service Level Agreements (SLA) gezählt. Sowohl die Bindung als auch das Risiko aus einer Verletzung der Vorgaben (Compliance-Risiko) ist von Außen nach Innen zunehmend.

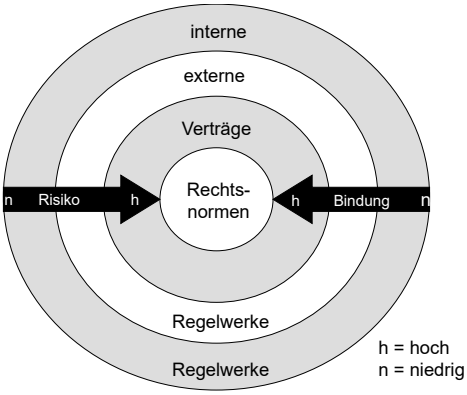

Abb. 3: Zwiebelmodell für Regelwerke der Compliance nach Klotz und Dorn (2008, S. 11-14) bzw. Klotz (2009, S. 20-25)

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) definiert im Entwurf zum Prüfungsstandard für Compliance Management-Systeme (IDW 2010) insgesamt sieben Grundelemente. Diese sind Compliance-Kultur, Compliance-Ziele, Compliance-Organisation, Compliance-Risiken, Compliance-Programm, Compliance-Kommunikation sowie Compliance-Überwachung und Verbesserung. Im Zentrum steht hier das Compliance-Programm, das alle Maßnah-

men, die zur Reduzierung der Compliance-Risiken beitragen sollen, beinhaltet.

Rath und Sponholz (2009, S. 135-136) konkretisieren den Managementprozess hinsichtlich der IT-Compliance. In einem ersten Schritt sollte demnach analysiert werden, welche regulatorischen Vorgaben für das betrachtete Unternehmen relevant sind. Dies ermöglicht die Feststellung, ob das Unternehmen diese Vorgaben einhält bzw. ob Abweichungen existieren. Hierfür ist ein Abgleich des Ist-Zustands mit dem Soll-Zustand notwendig („Abweichungsanalyse"). Werden Abweichungen erkannt, müssen entsprechende Maßnahmen zur Herstellung der Compliance eingeleitet werden („Deficiency Management"). Diese Prozessschritte sind zu wiederholen bis keine Abweichungen mehr festgestellt werden. In einem letzten Schritt ist eine Berichterstattung und Dokumentation der Normeinhaltung für verschiedene Adressaten notwendig. Andere Autoren wie Pupke (2008, S. 29-31) und Menzies (2006, S. 67) unterscheiden lediglich drei Phasen. Diese sind die Phase der Identifikation und Evaluierung, in welcher die für das Unternehmen relevanten Vorgaben identifiziert und analysiert werden, die Phase der Implementierung, in welcher die Vorgaben umgesetzt werden sowie die Sustainment-Phase, in der die Normeinhaltung überwacht und weiterentwickelt wird.

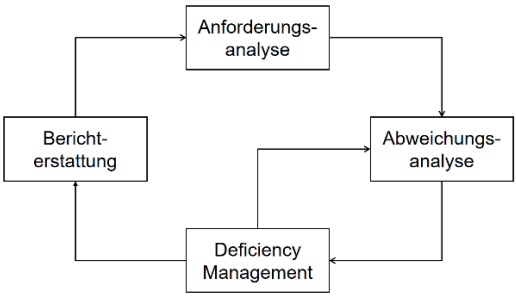

Abb. 4: IT-Compliance-Managementprozess nach Rath und Sponholz (2009, S. 136)

2.5 Beziehungen und Integrationsaspekte von Governance, Risiko- und Compliance-Management

2.5.1 Beziehungen und Integrationsaspekte von Compliance- und Risikomanagement

Zur Beziehung von Compliance- und Risikomanagement existieren zwei Sichtweisen. Einerseits wird Compliance-Management als Teil des Risikomanagements betrachtet. Andererseits kann Risikomanagement auch als Teil des Compliance-Managements aufgefasst werden. Versteht man Compliance als Teil das Risikomanagements (IDW 2010; Withus 2010, S. 100), so rücket die Betrachtung des Risikos der Normverletzung (Non-Compliance-Risiko) ins Zentrum. Aus der Verletzung von normativen Vorgaben können für das Unternehmen materielle Verluste, wie z.B. Strafzahlungen, und immaterielle Verluste, wie z.B. Imageverluste, entstehen. Withus (2010, S. 100) argumentiert darüber hinaus, dass auch die Verletzung interner Vorgaben mit Risiken in Form von Ineffizienzen verbunden ist. Diese Betrachtungsweise wird insbesondere auch im Risikomanagement-Standard der COSO (2004, S. 3) eingenommen, welcher das Risikomanagement, wie dargestellt, in die

Bereiche Strategie, betriebliche Prozesse, Berichterstattung und Compliance unterteilt.

Versteht man Risikomanagement als Teil von Compliance rückt das Verständnis, dass regulatorische Vorgaben die Umsetzung des Risikomanagements fordern, ins Zentrum der Betrachtung. Die Umsetzung des Risikomanagements bzw. des internen Kontrollsystems unterliegt regulatorischen Vorgaben und ist somit auch als Compliance-Vorgabe zu verstehen. Das interne Kontrollsystem kann als ein Prozess, der hinreichende Sicherheit bzgl. der Erreichung von Zielen in den Kategorien Effektivität und Effizienz der Unternehmensabläufe, Zuverlässigkeit der Finanzberichterstattung und Einhaltung von Gesetzen und Regularien (COSO 1994, S. 3)[13] gewährleistet, definiert werden. Es ist Teil des Risikoüberwachungssystems, welches wiederum Bestandteil des Risikomanagements ist (Gleißner 2011, S. 35). Das interne Kontrollsystem besteht der COSO (1994, S. 4) folgend aus den vier miteinander in Beziehung stehenden Komponenten Kontrollumfeld, Risikoanalyse, Kontrollaktivitäten sowie Information und Kommunikation. Zur Umsetzung des regulatorisch geforderten internen Kontrollsystems können Kontrollmodelle wie für die IT-Prozesse COBIT, ITIL oder der Informationssicherheitsstandard ISO 27001 (DIN 2008a) eingesetzt werden (Johannsen und Goeken 2006, S. 16). Normkonformität kann also mit einem Nachweis der Umsetzung von Kontrollmodellen ver-

[13] Im Mai 2013 ist die neue Version des COSO Rahmenwerks für interne Kontrollen erschienen (COSO 2013). Diese neue Version stellt eine Weiterentwicklung des Rahmenwerks von 1994 dar, wobei unter anderem die Definition und die fünf Komponenten von "Internal Controls" erhalten bleiben. Die neue Version formalisiert zudem 17 Prinzipien zu den Komponenten. Auf Grund der weiten Verbreitung wird das ursprüngliche Rahmenwerk weiterverwendet. Es wird zudem davon ausgegangen, dass die Weiterentwicklungen nur geringfüge Auswirkungen auf die in dieser Arbeit angestellten Analysen haben.

bunden sein. Außerdem existieren GRC-Vorgaben wie die MaRisk, die Regeln beinhalten, die Kontrollcharakter aufweisen (siehe MaRisk BTO 1.1 Funktionstrennung und Votierung). Es können jedoch auch Kontrollen aus Risikoanalysen gewonnen und im Hinblick auf Ziele definiert werden, deren Erreichung durch Risiken gefährdet ist (COSO 1994, S. 51-52). Außerdem sollten Kontrollen die wirksame Reaktion auf Risiken sicherstellen (COSO 2004, S. 4). Dies bedeutet zusammenfassend, dass eine Beziehung zwischen Compliance-Vorgaben und Risiken hergestellt werden kann, und die Risikosteuerung sowohl standardmäßig durch Umsetzung verpflichtender Vorgaben als auch durch individuelle Risikoreaktionen erfolgen kann. Ein weiterer Aspekt des Risikomanagements, der für das Compliance-Management relevant ist, ist die risikoorientierte Planungsmethodik, wie bspw. die risikoorientierte Prüfungsplanung in der internen Revision (IIA 2009, S. 36).

2.5.2 Beziehungen und Integrationsaspekte von Governance und Compliance-Management

Zwischen den Begriffen Corporate Governance und Compliance wird teilweise die Unterscheidung getroffen, dass im Compliance-Management externe überwiegend verpflichtende Anforderungen und im Bereich der Corporate Governance interne und somit nicht obligatorische Richtlinien im Vordergrund stehen (Racz et al. 2010b, S. 113). Diese Unterscheidung ist jedoch nicht exakt aus den Definitionen herzuleiten und stellt eher eine Schwerpunktsetzung dar. Die Verpflichtung zur Einhaltung von Vorgaben ist in beiden Ansätzen identisch. Im Zentrum der Corporate Governance stehen Kontroll- und Steuerungsmechanismen, die opportunistisches Verhalten des Managements gegenüber den Anteilseignern verhindern sollen (siehe bspw. Schewe 2005). Im Jahre 2002 wurde der DCGK (Regierungskommission

DCGK 2010) verabschiedet. Dieser ist zwar selbst nicht als Gesetz ausgestaltet, gemäß §161 Aktiengesetz müssen jedoch alle börsennotierten Unternehmen eine sogenannte Entsprechenserklärung abgeben, in welcher die Anwendung des Kodex dargestellt werden muss. Der DCGK kann somit einerseits als Compliance-Vorgabe verstanden werden, womit Corporate Governance unter das Compliance-Management zu subsumieren wäre. Wie Sidhu (2005) ausführt beinhaltet der DCGK auch selbst die Verpflichtung zur Compliance durch die Forderung nach entsprechenden organisatorischen Maßnahmen, womit Compliance auch als Bestandteil der Corporate Governance verstanden werden kann. Verschiedene Gesetzesinitiativen wie das KonTraG und der SOX können als eine Kodifizierung der Corporate Governance verstanden werden. In diesem Bereich besteht also eine Überschneidung zwischen Corporate Governance und Compliance (Teubner und Feller 2008, S. 400). Compliance bezieht sich hierbei jedoch schwerpunktmäßig auf eine andere Hierarchieebene als Corporate Governance und beinhaltet somit nicht lediglich Regeln für den Vorstand bzw. die Beziehung von Vorstand und Aufsichtsrat, sondern für alle Unternehmensmitglieder. Hauschka (2007, S. 3) sieht in Corporate Governance und Compliance unterschiedliche Perspektiven auf ein Themengebiet. Corporate Governance nimmt demnach überwiegend die Sichtweise der Investoren ein, die aufgrund einer zu schwachen Regulierung Nachteile befürchten. Hingegen ist Compliance von der Sichtweise der Unternehmen geprägt, die in der Vielzahl an regulatorischen Vorgaben eine Überregulierung sehen. Der Begriff Governance wird darüber hinaus mit der wertorientierten Unternehmensführung in Verbindung gebracht (Gericke et al. 2009b, S. 3; Teubner und Feller 2008, S. 400). Unterstützt wird dieses Verständnis vom IT-Governance-Begriff, der auch die wirtschaftliche Steuerung der IT einschließt (ITGI 2007, S. 5). Wie bereits im Rahmen der Definition von IT-Governance erwähnt,

wird Compliance auch als Teilaufgabe der IT-Governance gesehen (Grant et al. 2007, S. 5; Johannsen und Goeken 2006, S. 14; ITGI 2007, S. 6; van Grembergen et al. 2004, S. 7).

2.5.3 Beziehungen und Integrationsaspekte von Governance und Risikomanagement

Risikomanagement wird ebenfalls als Teil der Corporate Governance verstanden, da es zu einem risikobewussten Kapitaleinsatz und der Schaffung von Transparenz über diesen beiträgt (Regierungskommission DCGK 2010; OECD 2004).[14] Ebenso wird im Kontext der Corporate Governance gefordert, Informationen über das Risikomanagement offen zu legen (OECD 2004, S. 65). Gemäß dem DCGK ist die Etablierung eines Risikomanagementsystems Aufgabe des Vorstandes. Der Aufsichtsrat hat die Aufgabe, die Etablierung des Risikomanagements zu überprüfen (Regierungskommission DCGK 2010). Insbesondere trägt Risikomanagement somit zur Vermeidung von ungewollten Nachteilen für die Investoren bei. Dieser Aspekt wird in den Gesetzen, die eine gute Unternehmensführung im Sinne der Corporate Governance sicherstellen sollen, deutlich. Bspw. macht das KonTraG umfangreiche Vorschriften für die Etablierung eines Risikomanagementsystems. Der Schutz von Investoren ist ebenso erklärtes Ziel des SOX, der insbesondere Vorgaben zur Etablierung eines internen Kontrollsystems als Teilaufgabe des Risikomanagements macht (Gleißner 2011, S. 38; Romeike und Brühwiler 2010, S. 104). Risikomanagement als zentrale Aufgabe der Governance findet sich auch in Arbeiten zur IT-Governance wieder, wobei Risikomanagement oftmals, ebenso wie die Compliance, als

[14] Siehe hierzu auch Gleißner (2011, S. 34-47) sowie Romeike und Brühwiler (2010, S. 100-101).

eine der Aufgaben der IT-Governance verstanden wird (Grant et al. 2007, S. 5; Johannsen und Goeken 2006, S. 14; ITGI 2007, S. 6; van Grembergen et al. 2004, S. 7).

Da das Risikomanagement zudem die dargestellten Überscheidungen zum Compliance-Management aufweist, ist die Beziehung des Risikomanagements zur Governance eng verwoben mit der Beziehung der Compliance zur Governance. Nach Racz et al. (2010c, S. 11-12) ist die Beziehung von Corporate Governance zu Risiko- und Compliance-Management zweigeteilt. Zum einen unterstützt Risiko- und Compliance-Management die Corporate Governance. Zum anderen übernimmt die Corporate Governance die Steuerung von Risiko- und Compliance-Management. Corporate Governance legt demnach die Spitzenorganisation fest und bietet den Rahmen für das Risiko- und Compliance-Management. Gleichzeitig liefert Risiko- und Compliance-Management wichtige Informationen an die Governance-Ebene.

2.6 GRC und strategisches GRC-Management

Auf der Basis der Analyse der Beziehungen und Integrationsaspekte von Governance, Risiko- und Compliance-Management kann insgesamt festgestellt werden, dass die Konzepte kaum voneinander getrennt werden können. Obwohl die Konzepte eine unterschiedliche Historie und teilweise unterschiedliche Perspektiven und Annahmen (Hardy und Leonard 2011) aufweisen, sind die Zielsetzungen ähnlich und es besteht eine Vielzahl von Überschneidungen, Berührungspunkten und Ergänzungsmöglichkeiten (Teubner und Feller 2008). Insbesondere die einleitend dargestellten Herausforderungen führen dazu, dass eine Ausweitung der Konzepte stattfindet. So bezieht sich der weitgefasste Compliance-Begriff nicht nur auf Gesetze, sondern auf interne und externe sowohl verpflichtende als auch freiwillige Vorgaben. Dies beinhaltet

also auch Standards und Best Practices sowie Verträge und interne Richtlinien (Johannsen und Goeken 2006, S. 10). Somit lässt sich ein hohes Integrationspotential konstatieren, da eine Vielzahl von Überschneidungen, Berührungspunkten und Ergänzungsmöglichkeiten existieren, die in der Unternehmenspraxis häufig nicht adäquat berücksichtigt werden. Vielmehr werden siloartige Ansätze auch innerhalb der Teilbereiche von GRC, wie z.B. zu unterschiedlichen Risikobereichen oder verschiedenen Compliance-Vorgaben, wie Datenschutz, Informationssicherheit, Qualitätsmanagement oder Compliance mit Bezug zur Finanzberichterstattung, eingerichtet. Dies resultiert weiterhin in unterschiedlichen methodischen Ansätzen und nicht-integrierten Informationssystemen (Böhm 2008, S. 22; Gericke et al. 2009a, S. 1; Marinos et al. 2009, S. 367; Menzies 2006, S. 63-64; Oh et al. 2007, S. 1; Racz et al. 2010a, S. 1; van der Veen et al. 2011, S. 265). Schwerpunktmäßig beziehen sich die Teilbereiche von GRC in der Praxis auch auf unterschiedliche Hierarchieebenen. Während Corporate Governance vor allem für die Vorstandsebene relevant ist, wird Risikomanagement überwiegend als Aufgabe des Managements verstanden. Compliance-Management hat oftmals einen operativen Fokus und hat bspw. durch Dokumentationsvorschriften eine Bedeutung bei der täglichen Ausführung der Geschäftsprozesse (Menzies 2006, S. 334-336).

Es existieren bereits einige forschungsbezogene und praxisorientierte Veröffentlichungen, die das Schlagwort GRC verwenden, wobei nicht immer klar ist, wie sich die gemachten Vorschläge von nicht integrierten Ansätzen abgrenzen (Deloitte 2008; Gericke et al. 2009a; Gill und Purushottam 2008; Götz et al. 2008; Hardy und Leonard 2011; Krcmar et al. 2011; Krey 2012; Krey 2010; Krey et al. 2012; Krey et al. 2011; OCEG 2009; Pohlman 2008; Puspasari et al. 2011; PwC 2004; PwC 2007; Racz et al. 2011b; Racz et al. 2010a; Racz et al. 2011a; Racz et al.

2011c; Racz et al. 2010b; Racz et al. 2010c; SAP 2009; Schöler und Zink 2008; Spanaki und Papazafeiropoulou 2013; Tarantino 2007; Tüllner 2012; van der Veen et al. 2011; Vicente und da Silva 2011a; Vicente und da Silva 2011b; Wiesche et al. 2011a; Wiesche et al. 2011b). Des Weiteren existieren einige Arbeiten, die sich mit der Terminologie und teilweise auch mit den Zusammenhängen von GRC auseinandersetzen (Hardy und Leonard 2011; Klotz 2009; Klotz und Dorn 2008; Krey 2010; Krey 2012; Krey et al. 2012; Menzies 2006; OCEG 2009; Puspasari et al. 2011; PwC 2004; PwC 2007; Racz et al. 2010b; SAP 2009; Schöler und Zink 2008; Tarantino 2007; Teubner und Feller 2008; Vicente und da Silva 2011a; Vicente und da Silva 2011b). Racz et al. (2010b) entwickeln in diesem Kontext auf Grundlage eines Literaturreviews sowie einer Online-Befragung die folgende Definition für GRC. „GRC is an integrated, holistic approach to organisation-wide governance, risk and compliance ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness" (Racz et al. 2010b, S. 8). Zusätzlich wird ein Rahmenwerk entwickelt, das die Komponenten der Definition auf der Grundlage der sogenannten „GRC-Trias" grafisch darstellt. Die „GRC-Trias" bzw. das „GRC-Dreieck" ist eine schematische Darstellung der Beziehungen von GRC, die sich mittlerweile in der Literatur etabliert hat (Klotz 2009, S. 8-11; Klotz und Dorn 2008, S. 6-10; Kranawetter 2009, S. 6-10; Puspasari et al. 2011, S. 312; Racz et al. 2010b; SAP 2009, S. 8; Schöler und Zink 2008, S. 17-18) (siehe Abb. 5).

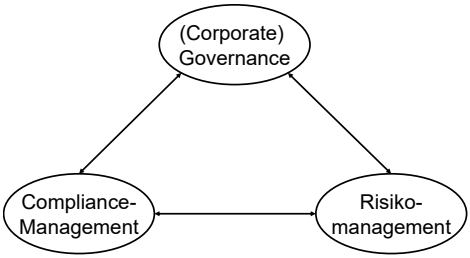

Abb. 5: GRC-Dreieck (in Anlehnung an Klotz 2009, S. 8-11; Klotz und Dorn 2008, S. 6-10; Kranawetter 2009, S. 24; Puspasari et al. 2011, S. 312; Racz et al. 2010b; SAP 2009, S. 8; Schöler und Zink 2008, S. 17-18)

Das GRC Capability Model der OCEG (2009) besteht im Kern aus insgesamt acht Komponenten, welche die Aktivitäten eines GRC-Systems zusammenfassen und strukturieren. Die Komponenten sind „Organize & Oversee", „Assess & Align", „Prevent & Promote", „Detect & Discern", „Respond & Resolve", „Monitor & Measure", „Inform & Integrate" und „Context & Culture". Die Komponenten werden durch insgesamt 32 Praktiken, die wiederum in Sub-Praktiken aufgespalten werden, detailliert. Des Weiteren sind zu allen Komponenten Prinzipien, allgemeine Fehlerquellen, in Beziehung stehende Anforderungen, Lieferobjekte oder Technologiemodule bestehend aus Geschäftsapplikationen, GRC-Kernapplikationen und Infrastruktur, ergänzt. Das GRC Capability Modell soll zur Erreichung von insgesamt acht universellen Ergebnissen eines GRC-Systems beitragen. Diese sind recht allgemein gehalten und werden bspw. mit Erreichung von Geschäftszielen, die Verbesserung der Organisationskultur oder verbessertes Stakeholdervertrauen angegeben. Insgesamt listet der Ansatz somit detailliert die relevanten Aktivitäten von GRC auf. Obwohl explizit eine Komponente auf die Integration hinweist, bleibt dieser Aspekt jedoch

recht unspezifisch, und es lässt sich kaum erkennen, wie die Integration im Zuge der einzelnen Komponenten erfolgt.[15]

Insgesamt stellt die Definition ebenso wie die Darstellung des GRC-Dreiecks zwar eine erste Annäherung an das Themengebiet dar, liefert jedoch weder eine exakte Eingrenzung noch eine Detaillierung der Integrationsaspekte. Des Weiteren ist davon auszugehen, dass GRC nicht auf den Integrationsaspekt beschränkt werden kann, sondern vielfältige Anforderungen zu erfüllen hat. Wie bereits einleitend ausgeführt, soll in diesem Forschungsvorhaben, neben der Integration, die Idee eines proaktiven und strategisch ausgerichteten GRC-Managements verfolgt werden. Um dies auszudrücken wird der Begriff des strategischen GRC-Managements verwendet. Dieser soll neben einer Abgrenzung zu existierenden Ansätzen, die Leitideen der Integration und strategischen Ausrichtung sowie die Management-Aspekte von GRC betonen. Hierzu gehören, wie bereits angesprochen, eine umfassende Steuerung des GRC-Status, die Integration der Teilaspekte, die Ausrichtung der GRC-Aktivitäten an den strategischen Zielen des Unternehmens sowie eine kontinuierliche Verbesserung von GRC.

Unternehmen lassen sich grundsätzlich in zweifacher Weise strukturieren. Die horizontale Gliederung teilt das Unternehmen in funktionale Einheiten, wie Beschaffung, Produktion und Absatz auf. Die vertikale Gliederung strukturiert das Unternehmen hingegen nach hierarchischen

[15] Eine detaillierte Analyse der Integration findet im Rahmen der Analyse der gleichnamigen Anforderungskategorie in Abschnitt 3.4.2.2 statt. Zusätzlich erfolgt eine Evaluierung der existierenden Management-Ansätze anhand der noch herzuleitenden Anforderungen an das strategische GRC-Management. Hierzu gehört auch die Integration (siehe Abschnitt 3.5.2.2). Eine Analyse von konzeptionellen Modellen hinsichtlich der Integration findet im Rahmen der Entwicklung des datenseitigen Modells für das strategische GRC-Management in Abschnitt 5.3 statt.

Gesichtspunkten, wobei üblicherweise die Unternehmensleitung, die mittlere Führungs- und die untere Führungsebene unterschieden werden. Die Unternehmensleitung ist mit der strategischen Planung beauftragt, die einen langfristigen Zeithorizont aufweist. Die taktische und operative Planung ist Aufgabe der mittleren und unteren Führungsebene, wobei ein mittel- bzw. kurzfristiger Planungshorizont zu Grunde liegt. Die Ausführungsebene ist wiederum von der Führung getrennt (Wöhe und Döring 2013, S. 164). Walser und Goeken (2011) unterscheiden im Kontext der IT-Governance zwischen Führungsaufgaben, die der strategischen Ebene zuzuordnen sind und Umsetzungsaufgaben, die der operativen Ebene zuzuordnen sind. Diese Unterscheidung ist in Übereinstimmung mit anderen Arbeiten zur IT-Governance, die zwischen einer strategischen Ebene, einer Management-Ebene und einer operativen Ebene unterscheiden (siehe van Grembergen et al. (2004, S. 10-11) sowie De Haes und Van Grembergen (2006, S. 7-8; 2009, S. 125; 2008a, S. 445; 2008b, S. 2)). Verschiedene Studien von De Haes und Van Grembergen (2006; 2009; 2008a; 2008b) im Kontext der IT-Governance schränken ebenfalls den Gegenstandsbereich der Untersuchungen ein, indem operative Aspekte nicht berücksichtigt werden.

In dieser Arbeit soll eine Fokussierung auf die strategische und Management-Ebene stattfinden. Dies bedeutet auch, dass konkrete Empfehlungen zur Umsetzung von bestimmten regulatorischen Vorgaben nicht Bestandteil dieser Arbeit sind. Auch wird nicht auf spezifische Methoden der Risikoanalyse oder Risikobehandlung eingegangen. Vielmehr soll GRC als Management-Ansatz verstanden und weiterentwickelt werden.

2.7 GRC und Informationstechnologie

In der vorliegenden Arbeit wird keine explizite Einschränkung auf die IT als Gegenstand von GRC gemacht, sondern es wird angenommen, dass die Forschungsergebnisse sowohl für IT-bezogene als auch unternehmensweite Fragestellungen relevant sind.

Die Beziehung zwischen IT-bezogenen und unternehmensweiten GRC-Ansätzen wird in der Literatur diskutiert. Hierbei werden IT-bezogene Ansätze, IT-GRC genannt, als Subdomäne unternehmensweiter Ansätze gesehen (Klotz und Dorn 2008, S. 7-8, Racz et al. 2010c, S. 4-5). Die konkreten Beziehungen werden jedoch bislang kaum thematisiert. Racz et al. (2010d) stellen in diesem Kontext die Notwendigkeit eigenständiger Ansätze für ein unternehmensweites Risikomanagement und ein IT-Risikomanagement auf der Basis des Vergleichs von Best Practice-Ansätzen in Frage. Insbesondere wird anhand des Vergleichs festgestellt, dass die methodische Vorgehensweise viele Ähnlichkeiten aufweist.

GRC und IT-GRC sind nur schwer voneinander abzugrenzen. Dies liegt darin begründet, dass fast alle Geschäftsprozesse automatisiert oder durch IT-Systeme unterstützt sind. Hierdurch werden die allgemeinen Vorgaben und Risiken mittelbar auch für die IT relevant. Auf der anderen Seite können IT-spezifische Anforderungen bspw. hinsichtlich des Betriebs von IT-Systemen nur durch das Wissen der Kritikalität der durch die IT unterstützten Geschäftsprozesse erfolgen. So ist ein Informationssystem, das Geschäftsprozesse im Anwendungsbereich des SOX unterstützt, auch hinsichtlich des Betriebs, wie dem Changemanagement, anderen Anforderungen unterworfen, als ein Informationssystem, das nicht in diesen Anwendungsbereich fällt.

Die IT hat im Kontext von GRC weiterhin eine zweifache Bedeutung und kann sowohl als Gegenstand von GRC angesehen werden als auch das GRC-Management unterstützen (Klotz und Dorn 2008, S. 9-10; Klotz 2009, S. 6-8; Teubner und Feller 2008, S. 401; Rath und Sponholz 2009, S. 119) (siehe Abb. 6).

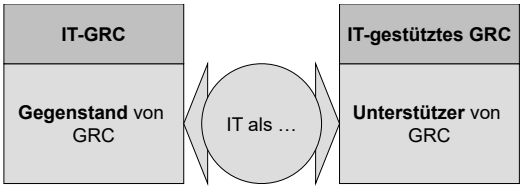

Abb. 6: Bedeutungsvarianten der IT im Kontext von GRC (in Anlehnung an Klotz und Dorn 2008, S. 9)

2.8 Erläuterung weiterer Begriffe

Im weiteren Verlauf der Forschungsarbeit werden einige weitere Begriffe verwendet, wovon die wichtigsten, die an mehreren Stellen verwendet werden, in diesem Abschnitt erläutert werden sollen. Weitere relevante Begriffe werden im Rahmen des jeweiligen Kapitels bzw. Abschnitts definiert.

Integration stellt als Tätigkeit oder Ziel einen wichtigen Bestandteil vieler Arbeiten der Wirtschaftsinformatik dar. Aus etymologischer Sicht beinhaltet Integration die „(Wieder-)Herstellung eines Ganzen“ und kann sich sowohl auf den Vorgang als auch das Ergebnis beziehen. Integration kann auf zwei Wegen erfolgen. Integration im Sinne von Verbinden schafft ein System aus unverbundenen Elementen, die eine logische Beziehung aufweisen. Integration im Sinne von Vereinigen führt gleichartige Elemente zusammen, womit eine Komplexitätsreduktion durch die Reduktion von Elementen und Beziehungen einhergeht. Integration ist sowohl auf technischer als auch auf organisatorischer

Ebene relevant. Organisatorisch ergibt sich ein Integrationsbedarf aus der Arbeitsteilung. Informationstechnisch existieren insbesondere durch historisch gewachsene Anwendungslandschaften Integrationsbedarfe. Integration weist verschiedene Dimensionen auf. Als Integrationsgegenstand werden Daten, Funktionen, Prozesse und Objekte unterschieden. Hinsichtlich der Dimension Integrationsrichtung lassen sich die vertikale und horizontale Integration unterscheiden.[16] Hinsichtlich der Reichweite kann sich Integration auf Aufgaben, Individuen, Organisationen und Unternehmen erstrecken bzw. ein inner-, zwischen- oder überbetriebliches Ausmaß aufweisen. Die Integrationsrealsierung befasst sich mit dem Ort bzw. Abstraktionsgrad der Integration, wobei die Organisation, Informationssysteme und Modelle unterschieden werden (Rosemann 1999, S. 5-12).

In dieser Arbeit wird zudem der Begriff GRC-Teildisziplin bzw. GRC-Bereich verwendet. Im Kontext der Information Systems-Forschung werden bspw. Psychologie, Ökonomie oder Soziologie als Referenzdisziplinen bezeichnet, da diese bedeutsame Theorien aufweisen, die zur Erklärung von Phänomenen der Information Systems-Forschung hilfreich sind (Lim et al. 2009; Westin et al. 1994). Es ist naheliegend, Governance, Risiko- und Compliance-Management als Referenzdisziplinen von GRC zu bezeichnen, die wiederum Wissen aus Bereichen wie Psychologie, Ökonomie und Soziologie anwenden. In dieser Arbeit wird daher von den GRC-Teildisziplinen bzw. den GRC-Bereichen oder Teilbereichen gesprochen, wenn nicht auf den integrierten Forschungsbereich GRC, sondern auf die zugrundeliegenden Disziplinen

[16] Siehe zur Erläuterung der horizontalen und vertikalen Gliederung von Unternehmen Abschnitt 2.6.

Governance, Risiko- und Compliance-Management verwiesen werden soll.

Des Weiteren sind für diese Arbeit die Begriffe Management, Management-Ansatz und Management-System von Bedeutung. Hinsichtlich des Begriffs Management können zwei Bedeutungsvarianten unterschieden werden (Staehle und Conrad 1999, S. 71). Management im funktionalen Sinne weist auf die Prozesse und Funktionen von Management, wie Planung, Organisation, Führung und Kontrolle hin (siehe auch Fayol 1949, S. 3). Im funktionalen Sinne definiert die International Organization of Standardization (ISO) Management als „[a]ufeinander abgestimmte Tätigkeiten zum Leiten und Lenken einer Organisation" (DIN 2000, S. 20). Management im institutionellen Sinn beinhaltet hingegen die Ressourcen, welche Managementaufgaben ausführen. Der Begriff Management wird durch Unternehmensführung, Führung oder Leitung übersetzt (Staehle und Conrad 1999, S. 72).

Hinsichtlich der Entwicklung eines Management-Ansatzes oder Konzeptes sind weiterhin die unterschiedlichen Perspektiven des Managements relevant (Reiß und Corsten 1995, S. 6-9). Die institutionelle Perspektive beinhaltet die Aufbauorganisation einschließlich der Rollen und Verantwortlichkeiten. Die funktionale Perspektive erfasst alle Handlungen, die zur Steuerung der Leistungsprozesse dienen. Hierzu gehören insbesondere die Managementprozesse. Die instrumentelle Perspektive beschreibt die Gesamtheit der Hilfsmittel bei der Durchführung der Managementaufgaben. Relevant sind hier Methoden und Werkzeuge (bspw. Informationssysteme) zur Unterstützung des strategischen GRC-Managements. Unter Konzepten sind in Anlehnung an

Stölzle (siehe zum Konzeptbegriff Stölzle 1999, S. 143-160) Modelle als statische Repräsentationen sowie systematische Vorgehensweisen zu deren Umsetzung zu verstehen.[17]

Modelle können in Anlehnung an die weit verbreitete Definition von Stachowiak (1974, S. 131-133) durch drei Merkmale charakterisiert werden: das Abbildungs-, das Verkürzungs- und das pragmatische Merkmal. Modelle dienen somit zur Abbildung eines Originalobjekts, wobei eine Verkürzung auf die für die jeweilige Modellierung relevanten Eigenschaften stattfindet. Das pragmatische Merkmal drückt die Ausrichtung des Modells auf einen bestimmten Zweck aus.

Der Begriff System wird in unterschiedlichen Anwendungsdomänen verwendet und ist sowohl in technischen als auch in sozialen Kontexten üblich (Forrester 1972, S. 16-17; Witte 1973, S. 2; Wilson 1990, S. 24-25; Lehner et al. 1995, S. 44-47)[18]. In dieser Arbeit wird der verbreiteten Definition von Witte (1973, S. 3) gefolgt, die versucht, die aus den unterschiedlichen Hintergründen stammenden Begriffsverständnisse zusammenzufassen. System wird demnach als „Gesamtheit von Elementen zwischen denen Beziehungen bestehen" definiert (Witte 1973, S. 3).[19] Neben den Elementen sind somit Beziehungen Bestandteil des Systems (Witte 1973, S. 4). Die Systemtheorie grenzt Elemente eines Systems von der Umwelt ab. In diesem Zusammenhang ist zwischen

[17] Wie in Abschnitt 1.2 dargestellt, ist die Entwicklung eines Management-Ansatzes für das strategische GRC-Management lediglich ein Fernziel und nicht Bestandteil dieser Arbeit. Trotzdem stellen Management-Ansätze einen wichtigen Aspekt in dieser Arbeit dar und werden unter anderem bei der Aufarbeitung des Forschungsstandes (siehe Abschnitt 3.5) mit Hilfe der genannten Charakteristika gegen andere Artefakte abgegrenzt.

[18] Die Ausführungen zum Begriff System basieren auf Kloos (2014, S. 18-20).

[19] Zum Begriff System bzw. Informationssystem im Kontext der Wirtschaftsinformatik siehe Abschnitt 1.3.

offenen und geschlossenen Systemen zu unterscheiden. Offene Systeme stehen im Austausch mit ihrer Umwelt. Alle anderen Systeme werden als geschlossen bezeichnet (Kloos 2014, S. 19). Im Rahmen dieser Arbeit wird weiterhin der Begriff des Management-Systems verwendet. Hiermit sind real existierende Systeme gemeint, die Management-Aufgaben wahrnehmen. Diese Unterscheidung zwischen Management-Ansatz als eher theoretisches Konstrukt und Management-System, als Benennung real existierter Umsetzungen in der Unternehmenspraxis ist auch in der Literatur vorzufinden (Strohmeier 2007, S. 83; Pischon 1999, S. 98). Strohmeier (2007, S. 83) unterscheidet z.B. zwischen dem Begriff Management-Konzept, der den gedanklichen Rahmen beinhaltet und Management-Systemen, als real existierende Elemente in der Unternehmenspraxis. Der Begriff Management-System findet sich außerdem in praxisbezogenen Veröffentlichungen wie Standards wieder, die in Übereinstimmung mit dem hier verwendeten Begriffsverständnis eher auf konkrete Implementierungen in der Praxis als auf theoretische Konstrukte abzielen. Beispiele hierfür sind die Standards zum Qualitätsmanagementsystem (DIN 2000; DIN 2008b), Umweltmanagementsystem (DIN 2004) und Informationssicherheitsmanagementsystem (DIN 2008a) der ISO sowie die Verwendung des Begriffs Compliance Management-System durch das IDW (2010).

Im Rahmen dieser Arbeit soll weiterhin der Begriff GRC-Vorgabe verwendet werden. Dieser Begriff soll alle Vorgaben erfassen, die sich aus der Governance, dem Risiko- und dem Compliance-Management ergeben. Die Governance beinhaltet hierbei insbesondere interne Vorgaben wie den „Code of Conduct“. Das Compliance-Management erfasst, wie zuvor ausgeführt, interne als auch externe sowohl verpflichtende als auch freiwillige Vorgaben, die teilweise eine Überschneidung mit den Governance-Vorgaben aufweisen. Aus dem Risikomanagement ergeben

sich Vorgaben aus den Risikoanalysen, die, wie bereits ausgeführt, ebenso teilweise auf Kontrollmodelle des Compliance-Managements abgebildet werden können. Im Rahmen dieser Arbeit wird für den zuvor dargestellten Aspekt bewusst nicht der Begriff Anforderung verwendet, da dieser in einem anderen Kontext verwendet wird.[20]

[20] Siehe Abschnitt 3.4.1.

3 Anforderungen und Forschungsagenda für das strategische GRC-Management[21]

3.1 Zielsetzung, Auswahl und Methodik des Literaturreviews

Zur Aufarbeitung des Forschungsstandes sowie Identifikation des weiteren Forschungsbedarfs soll ein systematischer Literaturreview durchgeführt werden. Diese Literaturauswertung wird ebenfalls zur Herleitung der Anforderungen an das strategische GRC-Management verwendet. Ein Literaturreview analysiert eine Menge von Primäruntersuchungen mit dem Ziel, diese zu beschreiben, zusammenzufassen oder zu integrieren (Fettke 2006a, S. 259, Cooper 1988, S. 108). Vom Brocke et al. (vom Brocke et al. 2009, S. 8) sieht in seinem Rahmenkonzept für Literaturreviews die Erarbeitung einer Forschungsagenda und somit die Explikation des Forschungsbedarfs als zentrale Aufgabe. Die Bedeutung der Explikation des Forschungsbedarfs wird auch von anderen Autoren gestärkt (Webster und Watson 2002, S. xix). In der Wirtschaftsinformatik-Forschung wird aufgrund der steigenden Anzahl von Fachzeitschriften, wissenschaftlichen Konferenzen sowie Fachbüchern vermehrt die Notwendigkeit einer systematischen Auswertung vorhandener Literatur betont (Fettke 2006a; vom Brocke et al. 2009). Hiermit soll kumulative Forschung stärker unterstützt werden, die bislang nur unzureichend erfolgt ist (Benbasat und Zmud 2003; Vessey et al. 2002; Kitchenham et al. 2009). Fettke (2006a) merkt an, dass insbesondere

[21] Die Forschungsergebnisse, welche in diesem Kapitel dargestellt werden, wurden bereits in folgenden Veröffentlichungen thematisiert: Marekfia und Nissen (2012); Marekfia und Nissen (2014); Nissen und Marekfia (2013).

nicht die Auswertung sämtlicher Publikationen als Anforderung eines Literaturreviews angesehen werden kann. Dies scheint auch aufgrund der Vielzahl an Veröffentlichungen in den meisten Fällen nicht möglich zu sein (vom Brocke et al. 2009, S. 2). Vom Brocke et al. (2009) greifen diese Problematik auf und argumentieren für eine rigorose Dokumentation des Forschungsprozesses und meinen hiermit insbesondere die Literatursuche und -auswahl. Nur hierdurch kann die Möglichkeit der Replikation eines Literaturreviews geschaffen werden. Ein Literaturreview kann in verschiedene Schritte unterteilt werden (siehe bspw. Fettke 2006a, S. 269, vom Brocke et al. 2009, S. 8). Vom Brocke et al. (2009, S. 8) unterscheiden die fünf Phasen Definition des Umfangs des Reviews (I), Konzeptualisierung des Themas (II), Literatursuche (III), Literaturanalyse und Synthese (IV) und Erarbeitung der Forschungsagenda (V).[22]

Zur Strukturierung des Reviews wird, neben dem Rahmenwerk von Hevner et al. (2004)[23] ebenfalls auf die Arbeiten von Walls et al. (1992; S. 2004) zur Gestaltungstheorie zurückgegriffen. Nach Walls et al. kann eine Gestaltungstheorie als „präskriptive Theorie, die sich auf theoretische Grundlagen stützt und Aussagen darüber macht, wie ein Gestaltungsprozess ausgeführt werden kann, sodass er sowohl effizient als auch umsetzbar ist“ (Walls et al. 1992, S. 37, Übersetzung wörtlich nach Fischer et al. 2010, S. 384) definiert werden. Wichtige Bestandteile einer Gestaltungstheorie sind gemäß Walls et al. verallgemeinerte Anforderungen, Artefakte, welche die Anforderungen umsetzen sollen, (Kern-

[22] Eine Diskussion, warum andere denkbare Quellen als weniger geeignet erscheinen als die Auswertung der existierenden Literatur, ist in Abschnitt 3.4.1 zu finden.

[23] Siehe Abschnitt 1.3.

)Theorien[24] zur Begründung der Anforderungen sowie Gestaltungshypothesen, die eine Nachprüfbarkeit gewähren, ob die Artefakte den Anforderungen genügen (siehe Walls et al. 1992, S. 42-43 und Fischer et al. 2010, S. 384). Anforderungen stellen eine Klasse von Zielen dar, die aus Theorien hergeleitet werden. Die Artefakte, welche diese Anforderungen umsetzen, werden auch als Design oder (Design)-Komponenten bezeichnet (siehe hierzu auch Baskerville und Pries-Heje 2010, S. 263). Die Entwicklung dieser Komponenten ist somit nicht ohne die Kenntnis der relevanten Anforderungen möglich.[25]

Um gestaltungsorientierte Forschung zum strategischen GRC-Management zu ermöglichen und somit letztlich einen wissenschaftlich begründeten strategischen GRC-Management-Ansatz entwickeln zu können, sind, die vorangegangenen Ausführungen berücksichtigend, folgende Aspekte relevant, die in sequentieller Weise die Kernelemente der gewählten Vorgehensweise beinhalten.

1. **Theorien:** Es sind die relevanten Theorien zu identifizieren und zu diskutieren. Diese bilden die Grundlage zur Herleitung der Anforderungen.
2. **Anforderungen:** Es werden Anforderungskategorien aus der relevanten Literatur hergeleitet. Unter Verwendung der einschlägigen Theorien werden Anforderungen an einen GRC-

[24] In den Begriff der (Kern-)Theorie wird in Abschnitt 3.3 eingeführt.

[25] Aus dem Kontext der Arbeit von Walls (1992) zur Gestaltungstheorie werden lediglich die Anforderungen aufgegriffen, deren integrale Bedeutung für die gestaltungsorientierte Forschung in diesem Kontext betont wird. Die Entwicklung einer Gestaltungstheorie ist nicht Bestandteil der vorliegenden Forschungsarbeit.

Management-Ansatz konkretisiert, welche die relevanten Aspekte und Ziele eines solchen Ansatzes spezifizieren.

3. **Forschungsstand:** Zu den Anforderungskategorien wird der Forschungsstand aufgearbeitet, der die „Knowledge Base" zur Entwicklung eines strategischen GRC-Management-Ansatzes darstellt. Der Forschungsstand wird anhand der Forschungsziele „Beschreiben und Erklären" sowie „Gestalten" diskutiert.
4. **Forschungsagenda:** Mit Hilfe der vorangegangenen Analysen wird der weitere Forschungsbedarf abgeleitet und zur weiteren Verwendung hinsichtlich der Bedeutung und Zusammenhänge aufbereitet, wodurch eine Priorisierung der Forschungsbedarfe ermöglicht wird. Die Forschungsagenda soll es der Forschungsgemeinschaft ermöglichen, die notwendigen Schritte zur Entwicklung eines GRC-Management-Ansatzes zu ergreifen.

Aufgrund des frühen Stadiums der Forschung zu integrierten GRC-Ansätzen auf strategischer Ebene, ist das Forschungsziel dieses Literaturreviews die Entwicklung einer systematischen Forschungsagenda für das strategische GRC-Management. Neben den hier erwähnten Aspekten wären außerdem Forschungsmethoden gemäß Hevner ein relevanter Aspekt (Hevner et al. 2004) der Wissensbasis. Allgemeine Empfehlungen zur Anwendung bestimmter Forschungsmethoden sind jedoch schwierig, da die Auswahl der Forschungsmethode sehr spezifisch für ein bestimmtes Forschungsvorhaben ist.

Die konkreten Methoden, die im Rahmen der oben erwähnten Kernbereiche angewendet werden, sind in den jeweiligen Abschnitten erläutert. An dieser Stelle sei darauf hingewiesen, dass die gewählte Vorgehensweise eine Kombination von induktiven und deduktiven Elementen

beinhaltet. Zur Entwicklung der Anforderungskategorien[26] wird auf die qualitative Inhaltsanalyse (Krippendorff und Bock 2009; Mayring 2008), die eine wesentliche Methode der Grounded Theory (Goulding 2002) ist, zurückgegriffen.[27] Die Vorgehensweise ist daher als induktiv zu bezeichnen, da vorhandenes Wissen in Form von publizierten Arbeiten, die teilweise auch auf empirischen Methoden beruhen, ausgewertet wird. Die Entwicklung der konkreten Anforderungen innerhalb der Anforderungskategorien erfolgt wiederum deduktiv, mit Hilfe einschlägiger Theorien. Durch die Kombination dieser Vorgehensweisen soll die vorhandene Wissensbasis bestmöglich genutzt werden.

Da die verwendete Suchstrategie für die vorliegende Forschungsarbeit von entscheidender Bedeutung ist, wird diese nachfolgend näher betrachtet. Es sollen hierbei Arbeiten zu integrierten GRC-Management-Ansätzen ebenso wie Arbeiten aus den GRC-Teildisziplinen berücksichtigt werden. Allgemein wird empfohlen qualitativ-hochwertige Veröffentlichungen ins Zentrum zu stellen (vom Brocke et al. 2009; Levy und Ellis 2006, S. 185). Solche Veröffentlichungen sind vorwiegend in wissenschaftlichen Zeitschriften (Rowley und Slack 2004, S. 32) bzw. in Konferenz-Proceedings (Webster und Watson 2002, S. xvi) zu erwarten. Van Brocke et al. (2009, S. 9) empfiehlt daher in einem ersten Schritt die Auswahl von wissenschaftlichen Zeitschriften und Konferenzen. Diese Vorauswahl ermöglicht die Identifikation von geeigneten Datenbanken, die für eine Suche mit Schlüsselbegriffen geeignet sind und gleichzeitig die wichtigsten Publikationsorgane berücksichtigen. Die hierbei gefundenen Veröffentlichungen müssen dann inhaltlich auf

[26] Siehe Abschnitt 3.4.1 zur Begriffserläuterung.

[27] Siehe ebenfalls Abschnitt 3.4.1.

ihre Relevanz evaluiert werden. Aufgrund der Vielzahl der durch die bisher beschriebenen Schritte gefundenen Publikationen wird auf eine Vorwärts- und Rückwärtssuche (Webster und Watson 2002, S. xvi) verzichtet. Außerdem wurde die Suche zeitlich auf die Jahre ab 2005 eingeschränkt. Es ist davon auszugehen, dass durch die zeitliche Eingrenzung keine relevanten Aspekte unberücksichtigt geblieben sind, da diese Aspekte durch kumulative Forschung auch in neueren Arbeiten berücksichtigt wurden. Zudem erscheint eine Berücksichtigung von mehr als 300 Publikationen für die weitere Analyse als nicht zweckmäßig. Zusammenfassend besteht die Suche demnach aus den vier Phasen (1) Identifikation relevanter Zeitschriften und Konferenzen, (2) Identifikation von Datenbanken, (3) Durchsuchung der Datenbanken und (4) Auswahl relevanter Beiträge. Diese Phasen werden im Anschluss näher betrachtet.

Zu (1): Es wurden Zeitschriften mit hoher Qualität ausgewählt, wobei Wert auf die Berücksichtigung der führenden Zeitschriften aus Betriebswirtschaft, Wirtschaftsinformatik und Information Systems gelegt wurde. Daher wurden die mit A bewerteten Journale der WI-Journalliste und des VHB-JOURQUAL2 Zeitschriftenrankings ebenso wie die ersten zehn gelisteten Journale des MIS Journal Rankings ausgewählt. Ergänzend wurden wissenschaftliche Konferenzen in die Literaturrecherche aufgenommen, um der Neuigkeit des Themas Rechnung zu tragen. Hierzu wurden die Einträge der Kategorie A der WI-Liste der Konferenzen, Proceedings und Lecture Notes 2008 berücksichtigt.[28] Es wurden auch weitere insbesondere GRC-spezifische Konfe-

[28] Die aufgeführten Zeitschriftenrankings sind unter folgenden Adressen im Internet verfügbar (Letzter Abruf Oktober 2014): http://www.wiso.uni-

renzen und Zeitschriften nach Relevanz und Qualität (bspw. sichergestellt durch Peer-Reviews) ausgewählt. Hierzu gehören auch Zeitschriften und Konferenzen mit entsprechenden thematischen Schwerpunktheften oder Konferenz-Tracks.

Zu (2): Anhand der Auswahl der Journale und Konferenz-Proceedings wurden die relevanten Datenbanken identifiziert. Zu diesen gehören ACM Digital Library, AIS Electronic Library (AISeL), Cambridge Journals, CS Digital Library, EBSCOhost (Business Source Premier), Elsevier Journals, Emerald Insight, IEEE Xplore, INFORMS PubsOnLine, JSTOR, Oxford Journals, Palgrave Macmillan Journals, SAGE Journals Online, ScienceDirect, SIAM Journals Online, SpringerLink, WILEY Online Library. Zeitschriften bzw. Konferenz-Proceedings, die nicht mit Hilfe einer wissenschaftlichen Datenbank durchsucht werden konnten, wurden an Hand der jeweiligen Homepage ausgewertet.

Zu (3): Bei der Identifikation potentiell relevanter Arbeiten wurde nach Möglichkeit eine Suche in Titeln, Schlagwörtern und Abstracts vorgenommen.[29] Dies liegt darin begründet, dass die Begriffe Governance,

---

hamburg.de/fileadmin/sozialoekonomie/bwl/marketing_innovation/13-14-kv-sem/VHB_Ranking_Journals.pdf (VHB-JOURQUAL2); http://aisnet.org/?JournalRankings (MIS Journal Ranking); http://gcc.uni-pader-born.de/www/WI/WI2/wi2_lit.nsf/0/549991b84925b9d5c12573d200360077/$FILE/Orientierungslisten_WKWI_GIFB5_ds41.pdf (WI-Journalliste 2008 und WI-Liste der Konferenzen, Proceedings und Lecture Notes 2008).

[29] Grundsätzlich wurden alle Datenbanken mit den Schlagwörtern GRC, Governance, Risk, Risiko und Compliance durchsucht. Führte eine Suche zu einer zu hohen Trefferzahl wurden spezifischere Suchbegriffe wie Corporate Governance, IT-Governance, Risk Management, Risikomanagement, Compliance Management, Compliance-Management oder Compliancemanagement bzw. UND-Verknüpfungen wie (Governance und Risk und Compliance), (Governance und Risiko und Compliance), (Corporate und Governance), (IT und Governance), (Risk und Management), (Risiko und Management) sowie (Compliance und Management) verwendet.

Risk bzw. Risiko und Compliance in sehr vielen Arbeiten zwar erwähnt jedoch nur eingeschränkt Gegenstand der Betrachtung sind. Zusätzlich zu dieser Suche wurden die in Schritt 1 erwähnten Zeitschriften und Konferenz-Proceedings an Hand der Inhaltsverzeichnisse manuell durchsucht um auch Arbeiten, die nicht explizit die Begriffe Governance, Risk und Compliance verwenden, jedoch bspw. bestimmte GRC-Vorgaben wie den SOX betrachten, zu identifizieren.

Zu (4): Die inhaltliche Auswahl der relevanten Beiträge ist von besonderer Bedeutung, da einerseits viele Arbeiten Governance, Risikomanagement und Compliance zwar als Schlagworte erwähnen, jedoch inhaltlich nur am Rande behandeln. Zum anderen besteht die Gefahr, durch das Aussortieren von Arbeiten relevante Aspekte nicht zu berücksichtigen. Inhaltlich wurden Arbeiten ausgewählt, die allgemein relevant für das GRC-Management sind bzw. bei denen zu erwarten ist, dass sie zur Herleitung von Anforderungen an das GRC-Management einen Beitrag leisten.[30] Um die Relevanz von Beiträgen festzustellen, wurde der Titel und die Zusammenfassung herangezogen und mit der zu diesem Zeitpunkt verfügbaren Liste von Anforderungen bzw. Anforderungskategorien hinsichtlich Relevanz beurteilt. Somit wurden die relevante Literatur und die Anforderungskategorien iterativ identifiziert. Dies ist in Übereinstimmung mit der Methode der qualitativen Inhaltsanalyse, die im Zuge des selektiven Kodierens eine Nacherhebung einschließt.[31] Insbesondere von hoher Relevanz für das vorliegende Literaturreview sind Arbeiten die integrierte GRC-Konzepte thematisieren oder zumindest teilweise eine Integration bspw. von Risiko- und Com-

[30] Die Herleitung der Anforderungen ist in Abschnitt 3.4 dargestellt.

[31] Siehe Abschnitt 3.4.1.

pliance-Aspekten berücksichtigen. Um neben den genannten inhaltlichen Kriterien eine sinnvolle Literaturauswahl treffen zu können, wurden insbesondere Veröffentlichungen, die lediglich eines der Teilbereiche von GRC thematisieren, im Wesentlichen aus Publikationsorganen mit einem Ranking von A und B gemäß dem VHB-JOURQUAL2 Zeitschriftenranking bzw. der WI-Orientierungslisten ausgewählt.[32] In diesem Zusammenhang sei nochmals darauf verwiesen, dass es angesichts der Vielzahl an verfügbarer Literatur nicht möglich und zielführend ist alle Veröffentlichungen, die bspw. Governance, Risikomanagement oder Compliance-Management als Bestandteil des Titels haben, zu berücksichtigen. Vielmehr wurden qualitativ hochwertige Arbeiten mit besonderer inhaltlicher Relevanz ausgewählt. Aufgrund der Vielzahl und inhaltlichen Breite der berücksichtigten Arbeiten kann davon ausgegangen werden, dass keine relevanten Aspekte vollständig unberücksichtigt geblieben sind. Zusätzlich wurden sehr selektiv weitere besonders relevante Veröffentlichungen zu integrierten GRC-Ansätzen, praxisnahe Publikationen (White Papers, Handbücher, Standards und Best Practices) und relevante Dissertationen durch eine Online-Recherche identifiziert. Hierbei wurden allgemeine Suchmaschinen wie Google bzw. Google Scholar sowie Bibliotheksdatenbanken wie der Gemeinsame Verbundkatalog (GVK) herangezogen.

Insgesamt berücksichtigt der Literaturreview 282 für das strategische GRC-Management relevante Veröffentlichungen. Publikationen, die

[32] Es ist darauf hinzuweisen, dass bei der Datenbanksuche grundsätzlich alle in der Datenbank verzeichneten Publikationsorgane berücksichtigt wurden, zu welchen auch Publikationsorgane gehören, die nicht in Schritt 1 aufgeführt sind. Um neben der manuellen Suche in den Inhaltsverzeichnissen, der in Schritt 1 genannten Publikationsorgane, einen Fokus auf hochwertige Veröffentlichungen zu legen, wurde daher die erwähnte Selektionsrichtlinie eingeführt.

Teil dieses Reviews sind, wurden im Literaturverzeichnis mit „#“ gekennzeichnet. Tab. 1 stellt die wichtigsten deskriptiven Angaben zu den berücksichtigten Veröffentlichungen dar. Gemäß der Suchstrategie wurden im Wesentlichen Konferenz- und Zeitschriftenbeiträge berücksichtigt. Unterscheidet man nach Forschungsbeiträgen und praxisbezogenen Veröffentlichungen, kann festgestellt werden, dass überwiegend Forschungsbeiträge berücksichtigt wurden, was ebenfalls ein konsistentes Ergebnis hinsichtlich der beschriebenen Suchstrategie ist. Forschungsarbeiten sind durch eine Anwendung von Forschungsmethoden gekennzeichnet. Essays, die argumentativ-deduktiven Analyse beinhalten, werden ebenso als Forschungsarbeiten betrachtet. Arbeiten die Konzepte aus der Praxis darstellen, wurden nicht als Forschungsarbeiten klassifiziert. Insbesondere werden auch White Paper sowie berücksichtigte Standards und Best Practices nicht als Forschungsarbeiten betrachtet. Zur Auswertung der Theorien wurden lediglich Forschungsarbeiten berücksichtigt. Zudem liegt aufgrund der Internationalisierung der Forschung, der überwiegende Teil der Beiträge in englischer Sprache vor.

Betrachtet man die in den Titeln verwendeten Schlagwörter berücksichtigt nur ein geringer Teil der Veröffentlichungen eine vollständige oder teilweise Integration der GRC-Teildisziplinen. Auffällig ist zudem, dass Arbeiten zum Compliance-Management stärker vertreten sind als Publikationen zur Governance und zum Risikomanagement. Zum einen ist hierzu anzumerken, dass Governance (Corporate und IT-Governance) sowie Risikomanagement bereits länger in der Literatur diskutiert werden als der Begriff Compliance. Bei der Durchsicht der Suchergebnisse in den Datenbanken ist zwar aufgefallen, dass Governance und Risiko zwar mehr Treffer in den Titeln ergeben, jedoch in viel größerem Maß Fragen betrachten, die nicht von besonderem Interesse für das strategi-

sche GRC-Management sind.[33] Zum einen werden Governance und Risk bzw. Risiko noch stärker als Schlagwörter verwendet, ohne dass die Konzepte selbst diskutiert werden. Zum anderen erscheint die Forschung sich von der Entwicklung allgemeiner Konzepte hin zur Beantwortung von Detailfragen entwickelt zu haben. Es ist nicht davon auszugehen, dass dieser Umstand einen signifikanten Einfluss auf den weiteren Forschungsprozess hat, da ein qualitativer Forschungsansatz gewählt wurde. Als Forschungsziele werden „Beschreiben und Erklären" sowie „Gestalten" berücksichtigt,[34] wobei die Publikationen keine Dominanz für eines der Forschungsziele aufweisen.

---

[33] Bspw. wurden in der AISeL 272 für Governance, 335 für Risk, 111 Treffer für Compliance (suche in Titeln ohne Jahresbeschränkung; Stand: 25.11.2014) gefunden.

[34] Siehe Abschnitt 3.5.1.

Tab. 1: Einige allgemeine Angaben zur ausgewerteten Literatur

Deskriptive Angaben	Häufigkeit	Prozent
Publikationsart		
Arbeitsbericht	1	0,35%
Buchkapitel	3	1,06%
Konferenzbeitrag	150	53,19%
Monografie	10	3,55%
Sonstige Veröffentlichung (Regularien, Standards, Best Practices)	11	3,90%
White Paper	7	2,48%
Zeitschriftenbeitrag	100	35,46%
Beitragsfokus		
Forschungsbeitrag	241	85,46%
Praxisbezogene Veröffentlichung	41	14,54%
Sprache		
Deutsch	65	23,05%
Englisch	217	76,95%
Betrachtete GRC-Disziplinen nach Nennung in Titel		
GRC	31	10,99%
Governance / Compliance	6	2,13%
Governance / Risikomanagement	2	0,71%
Risikomanagement / Compliance	7	2,48%
Compliance	117	41,49%
Governance	32	11,35%
Risikomanagement	27	9,57%
Sonstiges	60	21,28%
Forschungsziel[35]		
Beschreiben und Erklären	136	56,43%
Gestalten	105	43,57%

[35] Das Forschungsziel wurde nur für Forschungsbeiträge ausgewertet. Die Gesamtzahl der Forschungsbeiträge ist gemäß Tab. 1 241. Die Prozentangabe bezieht sich ebenfalls auf diese Zahl.

Tab. 2 enthält Publikationsorgane mit mehr als 10 berücksichtigten Veröffentlichungen. Es wird deutlich, dass ein Großteil der berücksichtigten Beiträge, wie im Rahmen der Suchstrategie angestrebt, aus qualitativ hochwertigen Publikationsorganen stammt.

Tab. 2: Publikationsorgane mit 10 oder mehr berücksichtigten Veröffentlichungen

Publikationsorgan	Einteilung gemäß WI-Orientierungsliste	Anzahl berücksichtigter Beiträge	Prozent[36]
Proceedings of the Annual Hawaii International Conference on System Sciences (HICSS)	B	23	8,16%
Proceedings of the Americas Conference on Information Systems (AMCIS)	B	19	6,74%
Proceedings of the European Conference on Information Systems (ECIS)	A	17	6,03%
Proceedings Internationale Tagung Wirtschaftsinformatik (WI)	A	11	3,90%
HMD - Praxis der Wirtschaftsinformatik	B	10	3,55%
Zeitschrift Wirtschaftsinformatik	A	10	3,55%

[36] Die Prozentangabe bezieht sich auf alle 282 relevanten Publikationen.

Aus Gründen der Vollständigkeit wurden auch die in den Veröffentlichungen (nur Forschungsbeiträge) angewendeten Forschungsmethoden erfasst. Eine Übersicht der angewendeten Forschungsmethoden einschließlich der Darstellung der methodischen Vorgehensweise ist im Anhang verfügbar (siehe Tab. 58).

3.2 Verwandte Arbeiten

Im Kontext der GRC-Teildisziplinen bzw. integrierten GRC-Ansätzen existieren einige Arbeiten, die ebenfalls der Forschungsmethode des Literaturreviews zugeordnet werden können. Auf diese Arbeiten soll in diesem Abschnitt kurz eingegangen werden. Ziel dieser Untersuchung ist es herauszufinden, welche Bereiche bereits durch Literaturreviews adressiert wurden und welche Schwachstellen diese Reviews aufweisen. Die Ausrichtung der eigenen Studie orientiert sich an den Ergebnissen dieser Analyse. Es wird zwischen Literaturreviews zu Teilbereichen von GRC und Literaturreviews zu integrierten GRC-Ansätzen unterschieden. Ein Überblick der Literaturreviews zu integriertem GRC ist in Tab. 3 zu finden. Literaturreviews zu Teilbereichen von GRC sind in Tab. 59 bis Tab. 63 (im Anhang) zusammengefasst.

Literaturreviews zu einem integrierten GRC-Management existieren von Racz et al. (2010b) sowie Hardy und Leonard (2011). Teubner und Feller (2008) betrachten zumindest teilweise eine Integration, wobei neben Governance und Compliance auch explizit die Informationstechnologie betrachtet wird. Racz et al. (2010b) untersuchen die Integration von GRC, wobei IT-Aspekte im Vordergrund stehen sollen, ohne dass diese von allgemeinen Ansätzen klar abgegrenzt werden. Diese Autoren untersuchen im Wesentlichen Arbeiten, die sich explizit mit einer Integration von GRC auseinandersetzen. Dies führt zu einer Berücksichtigung einer Vielzahl von praxisnahen Publikationen. Aktuel-

le wissenschaftliche Ansätze aus den GRC-Teildisziplinen werden vernachlässigt. Des Weiteren wird lediglich auf die Entwicklung einer GRC-Definition abgezielt, wobei diese in einem Rahmenwerk grafisch veranschaulicht wird.[37] Eine konkrete Auseinandersetzung mit den Überschneidungen und Beziehungen der GRC-Teildisziplinen findet nicht statt. Weitere Anforderungen werden nicht hergeleitet, womit auch eine strategische Perspektive auf das Themengebiet ausbleibt. Hardy und Leonard (2011) setzten an den Ergebnissen der Literatursuche von Racz et al. (2010b) an. Sie wählen einen interpretativen Ansatz um die unterschiedlichen Perspektiven auf das Themengebiet zu beleuchten. Hierbei werden ein Überblick zu unterschiedlichen Begriffsauffassungen von GRC sowie eine Übersicht von GRC-Rahmenwerken gegeben. Teubner und Feller (2008) liefern zwar interessante Ergebnisse zu den Zusammenhängen und Überschneidungen von GRC im Zusammenspiel mit der IT, ihr Review bezieht sich jedoch lediglich auf Webseiten und es wird eine Übersicht zu Anbietern von GRC-Software bzw. GRC-bezogenen Dienstleistungen gegeben.

[37] Siehe ebenfalls Abschnitt 2.6.

Tab. 3: Überblick über Literaturreviews zu integrierten GRC-Konzepten

Zitation	Hardy und Leonard 2011
Forschungsziel(e)	Der Beitrag versucht die bestehende GRC-Literatur zusammenzufassen und zu diskutieren, wobei ein Augenmerk auf die unterschiedlichen Standpunkte gelegt wird, unter denen GRC derzeit diskutiert wird.
Berücksichtigte Publikationen und Publikationsorgane	Es wird Literatur ab dem Jahr 2009 berücksichtigt. Hierbei wird auf der von Racz et al. (2010b) durchgeführten Literatursuche aufgesetzt. Es wird weiterhin ausgeführt, dass den Empfehlungen von Webster und Watson (2002) gefolgt wurde, wobei eine Datenbanksuche ebenso durchgeführt wurde wie eine Analyse von relevanten Internetseiten. Die Autoren geben an, dass die Literatursuche eher einem „critically reflective process" und nicht einem systematischen Reviewansatz gefolgt ist. Wie viele Publikationen insgesamt ausgewertet wurden, ist nicht angegeben.
Forschungsergebnis	Es wird die Bedeutung und der Anwendungsbereich von GRC sowie GRC als Technologieansatz diskutiert. Außerdem wird eine Übersicht zu dem Begriff GRC in unterschiedlichen Forschungsarbeiten, zu allgemeinen GRC-Rahmenwerken und GRC-bezogenen Forschungsarbeiten gegeben. Es wird festgestellt, dass GRC derzeit auf verschiedenen Ebenen und aus unterschiedlichen Blickwinkeln diskutiert wird. Die Autoren schlagen Latour's „panorama" Konzept (Latour 2005) vor, um GRC als „Ganzes" zu verstehen.
Zitation	Racz et al. 2010b
Forschungsziel(e)	Der Beitrag verfolgt die Entwicklung einer 1-Satz Definition für GRC.

Berücksichtigte Publikationen und Publikationsorgane	Es wurden folgende Datenbanken durchsucht: WISO, EBSCO, ACM, IEEE Xplore, SpringerLink, Emerald, Google sowie die Bibliothekskataloge der TU Wien und der Fachhochschule Ludwigshafen. Außerdem wurden Webseiten manuell durchsucht. Insgesamt wurden 107 Publikationen aus den Jahren 2004-2009 berücksichtigt.
Forschungsergebnis	Es wird die folgende 1-Satz-Definition für GRC hergeleitet: „GRC is an integrated, holistic approach to organisation-wide governance, risk and compliance ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness." (Racz et al. 2010b, S. 8)
Zitation	Teubner und Feller 2008
Forschungsziel(e)	Der Beitrag versucht einen Überblick über relevante Internetseiten zum Themengebiet „Informationstechnologie, Governance und Compliance" zu geben. Außer Internetseiten werden keine weiteren Veröffentlichungsorgane wie Zeitschriften, Konferenzbeiträge oder Bücher berücksichtigt.
Berücksichtigte Publikationen und Publikationsorgane	Die Suchstrategie ist nicht dokumentiert.
Forschungsergebnis	Der Beitrag liefert eine strukturierte Übersicht zu relevanten Internetseiten im Bereich Governance und Compliance mit Bezug zur Informationstechnologie. Es wird hierbei die Doppelrolle der IT als Gegenstand und Unterstützer von Governance und Compliance hervorgehoben. Ebenso werden die Überschneidungen zwischen den Themengebieten herausgearbeitet.

Literaturreviews zu Teilaspekten von GRC existieren von Abdullah et al. (2009), Abraham (2011), Aurigemma und Panko (2012), El Kharbili et al. (2008a), Haghjoo (2012), Lebek et al. (2013), Milicevic und Goe-

ken (2012; 2013a; 2013b), Rinderle-Ma et al. (2008) sowie Simonsson und Johnson (2006).

Abdullah et al. (2009) diskutieren das Thema Compliance aus einer Management-Perspektive. Die Autoren versuchen den Forschungsstand zum Compliance-Management in der Information Systems-Literatur aufzuarbeiten. Hierbei werden Integrationsaspekte zwischen einzelnen Anforderungen bzw. den GRC-Teildisziplinen nicht thematisiert. Es werden zudem nur Publikationen aus ausgewählten wissenschaftlichen Journalen berücksichtigt. Haghjoo (2012) sowie Simonsson und Johnson (2006) konzentrieren sich auf IT-Governance, wobei Haghjoo mögliche Nutzenpotentiale von IT-Governance untersucht und Simonsson und Johnson eine Konsolidierung von IT-Governance-Definitionen vornehmen. Die Literaturreviews von El Kharbili et al. (2008a) und Rinderle-Ma et al. (2008) beschäftigen sich aus IT-Sicht mit der Automatisierung von Kontrollen, wobei Methoden des Geschäftsprozessmanagements (GPM) aus gestaltungsorientierter Sicht im Vordergrund stehen (El Kharbili et al. 2008a; Rinderle-Ma et al. 2008). Im Gegensatz hierzu liefern sowohl Lebek et al. (2013) als auch Milicevic und Goeken (2012; 2013a; 2013b) systematische Reviews zu empirischen Arbeiten hinsichtlich der Compliance zu Vorgaben der Informationssicherheit.

Die Übersicht der Arbeiten macht deutlich, dass Reviews zu einzelnen Aspekten des GRC-Managements existieren, die wichtige Einblicke in Teilaspekte liefern und in der weiteren Forschung berücksichtigt werden sollten, jedoch derzeit nur schwer in den Gesamtzusammenhang eines integrierten GRC-Managements auf strategischer Ebene eingeordnet werden können. Insbesondere die Literaturauswertung von Racz et al. (2010b) versucht als erste dem Autor bekannte Arbeit eine systematische Aufarbeitung des Forschungsstandes eines integrierten GRC-

Managements. Diese Arbeit ist nützlich um einen ersten Überblick des Themengebiets zu erlangen. Wie bereits ausgeführt wurde, weist diese Arbeit jedoch sowohl Schwächen hinsichtlich der Suchstrategie als auch der Aufarbeitung des Wissenstandes basierend auf den gefundenen Arbeiten auf.

Der hier dargestellte Literaturreview versucht diese Schwächen zu berücksichtigen, wobei drei Aspekte von besonderer Bedeutung sind. Zum einen wird im Rahmen der Suchstrategie auf die Auswertung von qualitativ hochwertigen wissenschaftlichen Publikationen fokussiert, was ebenfalls in der Literatur zur Reviewforschung empfohlen wird (vom Brocke et al. 2009; Levy und Ellis 2006, S. 185). Zum anderen wird, um der Forderung nach kumulativer Forschung gerecht zu werden, der Fokus auf Arbeiten aus den GRC-Teildisziplinen erweitert, die bereits ausgeprägte Forschungsanstrengungen vorweisen können. Letztlich wird eine Strukturierung des Themengebiets anhand von Anforderungen vorgeschlagen. Diese verdichten das gegenwärtige für GRC relevante Wissen und dienen in einem zweiten Schritt zur Strukturierung der Analyse des Forschungsstandes sowie zur Herleitung des weiteren Forschungsbedarfs.

3.3 Relevante Theorien für das GRC-Management

3.3.1 Bedeutung und Identifikation der Theorien

In der Literatur werden verschiedene Arten von Theorien wie erklärende, vorhersagende, normative und präskriptive Theorien unterschieden (Fischer et al. 2010, S. 384; Gregor 2006, S. 620). Allgemein anerkannt ist, dass Theorien der Erklärung und Vorhersage dienen. Weiterhin können Abstraktion und Verallgemeinerung, Interaktion sowie Kausalbeziehungen als bedeutende Eigenschaften von Theorien genannt wer-

den (Fischer et al. 2010, S. 383; Gregor 2006, S. 614-618). Theorien sind als Grundlage zur Konstruktion von Artefakten weitestgehend anerkannt (Fischer et al. 2010, S. 382). Hevner et al. (2004) betonen nicht explizit den Einsatz von Theorien für die Gestaltung von Artefakten. Vielmehr betonen diese Autoren die Wichtigkeit der „Knowledge Base" für gestaltungsorientierte Forschungsvorhaben, die auch Theorien beinhaltet. Im Gegensatz hierzu betonen Gregor (2006a), Gregor und Jones (2007), Gehlert et al. (2009c) und Walls et al. (1992, S. 42-43) explizit die Bedeutung von Theorien für die Konstruktion von Artefakten.

Durch die voranschreitende wissenschaftliche Fundierung der gestaltungsorientierten Forschung und die zunehmende Verbreitung dieses Forschungsansatzes auch in der Information Systems-Forschung (Fischer et al. 2010, S. 382), wird eine Unterscheidung von Kern- und Gestaltungstheorien relevant (Fischer et al. 2010, S. 383-384; Gehlert et al. 2009, S. 1-2). Diese Unterscheidung wird in der Literatur in Zusammenhang mit der Frage diskutiert, ob Theorien auch ein Ergebnis gestaltungsorientierter Forschung sein können (Fischer et al. 2010, S. 383-384). Kerntheorien stammen aus den Natur- und Sozialwissenschaften und betrachten im Wesentlichen Ursache-Wirkungs-Beziehungen (Fischer et al. 2010, S. 384; Walls et al. 1992, S. 40). Abzugrenzen hiervon sind Gestaltungstheorien. Fischer et al. (2010, S. 384) geben bezugnehmend auf Walls et al. (1992, S. 40) das Wesen von Gestaltungstheorien wie folgt an: „Zielorientierung und Ziel-Mittel-Relationen sind die Essenz einer Gestaltungstheorie". Die Diskussion hinsichtlich der Gestaltungsorientierung zeigt noch einige offene Fragen, wie bspw. ob Gestaltungstheorien immer nur das Ergebnis gestaltungsorientierter Forschung sind, und wie sie dann von Artefakten zu unterscheiden sind

(Fischer et al. 2010, S. 384). Nachfolgend wird diese Unterscheidung daher nicht aufgegriffen.

Die für das strategische GRC-Management relevanten Theorien sind bislang weitestgehend unbekannt und werden auch von den zuvor diskutierten existierenden Literaturreviews vernachlässigt. Bemerkenswert ist außerdem, dass eine Vielzahl der in der Literatursuche gefundenen Publikationen nicht explizit auf Theorien zurückgreift. Gleichzeitig existiert in den Managementwissenschaften und der Organisationsforschung eine Vielzahl von heterogenen Theorien (Pfeffer 1982, S. 1), die sich nur eingeschränkt systematisieren lassen (Wolf 2005, S. 434-443). Diese Problematik berücksichtigend wurde vorliegend ein pragmatischer Ansatz gewählt und die in der GRC-Literatur angewandten Theorien untersucht.

Zur Identifikation dieser Theorien wurde die von Lim et al. (2009, S. 2-3; 2013, S. 9-10)[38] dargestellte Vorgehensweise aufgegriffen, die zur Identifikation von Theorien in Arbeiten der Information Systems-Forschung angewendet wurde. Neben dem Durcharbeiten aller Forschungsarbeiten, was Teil des umfassenden Literaturreviews war, wurde hierbei nach Möglichkeit eine Suche mit dem Term „theo" vorgenommen, der sowohl für deutsch- als auch englischsprachige Arbeiten geeignet ist. Hierdurch sollten mögliche Fehler wie das Überlesen von Theorien, verhindert werden. Es wurde ebenfalls analog zu Lim et al. (2009, S. 2-3; 2013, S. 9-10) geprüft, dass die identifizierte Theorie zur Argumentation innerhalb des Forschungspapiers herangezogen und nicht lediglich referenziert wurde. Dies bedeutet insbesondere in quantitativ-empirischen Arbeiten eine Berücksichtigung im Forschungsmo-

[38] Diese Vorgehensweise wird ebenfalls von Houy et al. (2014b) aufgegriffen.

dell bzw. der Hypothesenentwicklung. Ebenso wurden, in Anlehnung an die Unterscheidung von Cushing (1990) zwischen Theorien und Rahmenwerken, keine Rahmenwerke berücksichtigt. Nach Cushing stellen Rahmenwerke eine Vorstufe bei der Entwicklung von Theorien dar, die zwar bereits Generalisierungen und Gesetzmässigkeiten beinhalten, jedoch noch nicht den Reifestatus einer Theorie erreicht haben. Rahmenwerke haben somit überwiegend beschreibenden Charakter und beinhalten weniger erklärende oder vorhersagende Bestandteile wie Kausalbeziehungen und testbare Hypothesen.[39] Letztlich wurden ebenfalls analog zu Lim et al. (2009, S. 2-3) zu breite theoretische Konzepte, wie der Begriff der Organisationstheorie oder ökonomische Theorie nicht berücksichtig. Stattdessen wurden jedoch die einzelnen Theorien, die diesen Oberbegriffen zugeordnet werden können, aufgenommen. In Übereinstimmung mit Houy et al. (2014b, S. 10) wurde ebenfalls ein Abgleich mit der Literaturliste von Schneberger et al. (2013) vorgenommen, um sicherzustellen, dass es sich bei den gefundenen Theorien um etablierte Theorien handelt. Es ist darauf hinzuweisen, dass selbstverständlich nicht alle Theorien die Begriffe „Theorie" bzw. „theory" in ihrer Bezeichnung tragen (bspw. Resource-based view). Die elektronische Suche ist daher, soweit diese überhaupt möglich war, lediglich als Ergänzung zum Durcharbeiten der Literaturbeiträge zu betrachten. Zur

[39] Des Weiteren ist auch darauf hinzuweisen, dass im Kontext der Wirtschaftsinformatik wie auch in dieser Arbeit viele Artefakte als Rahmenwerke bezeichnet werden. So werden bspw. auch COBIT (ITGI 2007) oder der Risikomanagement-Ansatz der COSO (2004) als Rahmenwerke bezeichnet. Diese erfüllen jedoch nicht die an eine Theorie gestellten Anforderungen. In der Wirtschaftsinformatik werden zudem grafische Rahmenwerke (hier bezeichnet als Ordnungsrahmen) zur überblicksartigen Darstellung von Referenzmodellen eingesetzt, welche die Kernbestandteile des Modells und deren Beziehungen beinhalten und somit auf die Teile des Modells verweisen (Meise 2001; Thomas et al. 2005). Für komplexe Referenzmodelle hat sich die Verwendung von Ordnungsrahmen bewährt (siehe bspw. Scheer 2002; Becker, und Schütte 2004). Diese Ordnungsrahmen werden ebenfalls nicht als Theorien berücksichtigt.

Zuordnung unterschiedlicher Bezeichnungen von Theorien wurden die innerhalb der einzelnen Beiträge zitierten Originalquellen herangezogen.

Um die Vielzahl an relevanten Theorien für eine weitere Analyse zugänglich zu machen und insbesondere eine nachvollziehbare Begründung für die Relevanz von Theorien für das strategische GRC-Management entwickeln zu können, sollen im Folgenden die in den bisherigen Veröffentlichungen verwendeten theoretischen Grundlagen dargestellt werden. Die Theorien wurden hierfür grob in die drei Gruppen strategisch, ökonomisch und verhaltenswissenschaftlich strukturiert. Eine ähnliche Strukturierung verwenden Dibbern et al. (2004, S. 17) im Kontext des Outsourcings von Informationssystemen. Es ist anzumerken, dass die Einteilung der Theorien lediglich eine Strukturierung ermöglichen soll, die im Weiteren eine Zuordnung der Theorien zu den noch zu entwickelnden Anforderungskategorien erleichtern soll. Insbesondere zwischen den strategischen und ökonomischen Theorien ist keine exakte Abgrenzung möglich. Jedoch ist diese Unterteilung, wie aufgezeigt, auch in anderen Zusammenhängen üblich und ermöglicht eine unterschiedliche Schwerpunktsetzung.

Strategische Theorien fokussieren auf die Erklärung der Entwicklung und Implementierung von Strategien zur Erreichung der Unternehmensziele. Ökonomische Theorien betrachten die Koordination von Akteuren bei Transaktionen. Verhaltenswissenschaftliche Theorien betrachten die Beziehungen zwischen Individuen und Gruppen. Sie befassen sich weiterhin mit der Motivation von Individuen bei der Ausführung bestimmter Handlungen.

Aufgrund der Vielzahl an Theorien, die in der GRC-Literatur angewendet werden, wurden im Rahmen des Literaturreviews nur Theorien mit zwei oder mehr Anwendungen in der relevanten GRC-Literatur be-

rücksichtigt. Die Stakeholdertheorie stellt hierbei eine Ausnahme dar und wird lediglich von Pupke (2008) angewendet, scheint jedoch gerade in Zusammenhang mit den weiteren von Pupke angewendeten Theorien, namentlich der Transaktionskostenökonomik und der Prinzipal-Agenten-Theorie, ein hohes Erklärungspotential für das strategische GRC-Management aufzuweisen. Des Weiteren werden Stakeholder explizit im Rahmen der Anforderungskategorie der strategischen Ausrichtung[40] angesprochen. Eine weitere Ausnahme stellt die Stewardship-Theorie dar, welche nur von Grundei (2006) eingeführt wird und eine Gegenposition zur Prinzipal-Agenten-Theorie darstellt. Tab. 4 zeigt diese Theorien mit der Anzahl der Publikationen, die die jeweilige Theorie anwenden.

[40] Siehe Abschnitt 3.4.2.1.

Tab. 4: Übersicht der Theorien aus der GRC-Literatur mit zwei oder mehr Anwendungen

Theorie	Anzahl Anwendungen	Berücksichtigung
Theorie des geplanten Verhaltens	13	ja
General Deterrence Theorie	9	ja
Institutionalistische Theorie	9	ja
Prinzipal-Agenten-Theorie	9	ja
Resource-based view	7	ja
Organisational Control Theorie	6	ja
Theorie des überlegten Handelns	6	ja
Technology Acceptance Model	5	ja
Theorie der Schutzmotivation	5	ja
Theorie der rationalen Entscheidung	3	ja
Transaktionskostenökonomik	3	ja
Kontingenztheorie	2	nein
Diffusionstheorie	2	ja
Market-based view	2	ja
Stakeholdertheorie	1	ja
Stewardship-Theorie	1	ja

Tab. 5 beinhaltet eine Übersicht, dieser, für das strategische GRC-Management relevanten, Theorien. Hierbei findet neben der Zuordnung in die Kategorien strategisch, ökonomisch und verhaltenswissenschaftlich, eine Angabe der Kernaussagen und wichtigen Konstrukte sowie der relevanten Grundlagenliteratur statt. Im Fokus dieser Arbeit ist eine theoretische Aufarbeitung der im Weiteren zu entwickelnden Anforderungskategorien für das strategische GRC-Management. Hierzu sind nicht alle Theorien relevant. Daher ist in Tab. 4 entsprechend

angegeben, welche Theorien für die theoretische Analyse der Anforderungskategorien berücksichtigt wurden (Spalte „Berücksichtigung“).

Die Nichtberücksichtigung der Kontingenztheorie ist wie folgt begründet. Die Kontingenztheorie (Donaldson 2001) geht davon aus, dass die optimale Organisationsstruktur von Kontingenzfaktoren abhängig ist. Unter Kontingenzfaktoren werden hierbei alle internen und externen Variablen verstanden, die einen moderierenden Effekt auf die Beziehung von Organisationgestaltung und Organisationsperformance haben. Becker et al. (2011b, S. 1973) argumentieren, dass der Regulierungsgrad, der Teil des Unternehmensumfelds ist, als Kontingenzfaktor angesehen werden kann. Es wird weiter ausgeführt, dass Unternehmen, die hochgradig reguliert sind, andere Maßnahmen treffen werden und bspw. entsprechende Kontrollmechanismen auch für Informationssysteme umsetzen, als Unternehmen, die lediglich schwach reguliert sind. Im Rahmen der Entwicklung der Anforderungen für das strategische GRC-Management wird nicht davon ausgegangen, dass es einen allgemeingültig optimalen Ansatz für das strategische GRC-Management gibt. Vielmehr werden relevante Bereiche identifiziert und allgemeine Handlungsempfehlungen abgeleitet, die unternehmensindividuell, unter Berücksichtigung der Kontingenzfaktoren, umzusetzen sind. Die Kontingenztheorie hat somit mehr Relevanz für die Umsetzung der Anforderungen als für die Anforderungskategorien und Anforderungen selbst.

Tab. 5: Übersicht der in der weiteren Analyse verwendeten Theorien[41]

Name (Abkürzung)	Kernaussage(n)	Wichtige Konstrukte	Quellen
Strategische Theorien			
Market-based view (MBV)	Aus marktorientierter Sicht ist die Berücksichtigung der Wettbewerbssituation sowie der Kundenwünsche und somit die Positionierung des Unternehmens im Wettbewerb zentral.	Strategischer Wettbewerbsvorteil, Wettbewerber, strategische Aktivitäten	Porter 1980; Porter 1985; Porter 1996; Tallon 2007
Resource-based view (RBV)	Die Basis zur Erzielung einer nachhaltigen Marktführerschaft liegt in den Ressourcen und in der Art wie diese eingesetzt werden.	Strategischer Wettbewerbsvorteil, Ressourcen	Barney 1991; Wade und Hulland 2004
Stakeholdertheorie (SHT)	Unterschiedliche Interessengruppen (Stakeholder) haben einen Einfluss auf den Unternehmenserfolg. Daher sind die Ziele der Interessengruppen bei der Ausrichtung des Unternehmens zu berücksichtigen.	Stakeholderinteressen, Firmenerfolg	Freeman 1984; Mitroff 1983
Ökonomische Theorien			
Theorie der rationalen Entscheidung (TRE)	Individuen treffen Entscheidungen, indem sie den erwarteten Nutzen und die erwarteten Kosten abwägen.	Entscheidung, Nutzen, Kosten	McCarthy 2002, Becker 1968 (für die Kriminologie)
Transaktionskostenökonomik /-theorie (TKT)	Unternehmen sollten Entscheidungen über geplante Investitionsvorhaben unter Berücksichtigung der gesamten ökonomischen Kosten bestehend aus Produktions- und Transaktionskosten treffen.	Transaktionskosten, Produktionskosten	Williamson 1985; Williamson 1991

[41] Die Zuordnung der Theorien zu den Anforderungskategorien wird in Abschnitt 3.4.1 dargestellt.

Name (Abkürzung)	Kernaussage(n)	Wichtige Konstrukte	Quellen
Prinzipal-Agenten-Theorie (PAT) / Organisational Control Theorie (OCT)	Prinzipale und Agenten haben unterschiedliche Interessen. Daher sollten Prinzipale das Verhalten der Agenten entweder überwachen oder durch Anreize eine Angleichung der Interessen bewirken.	Agenturkosten, Vertragsgestaltung	Arrow 1985; Jensen und Meckling 1976; Ouchi 1979
Stewardship-Theorie (SteT)	Die Stewardship-Theorie unterstellt eine überwiegend intrinsische Motivation und eine Zielkonformität in der Beziehung zwischen Prinzipal und Steward.	Agenturkosten, Vertragsgestaltung	Donaldson 1990; Donaldson und Davis 1991; Davis et al. 1997
Verhaltenswissenschaftliche Theorien			
Institutionalistische Theorie (InT)	Organisationen müssen Legitimität erlangen, indem sie institutionellen Anforderungen aus der Umwelt entsprechen.	Institutionen, Institutionalisierung, Legitimität, Isomorphismus	DiMaggio und Powell 1983; DiMaggio und Powell 1991; Meyer und Rowan 1997
Diffusionstheorie (DT)	Die Übernahme (Adoption) einer Innovation erfolgt in den fünf Phasen (1) Knowledge (2) Persuasion, (3) Decision, (4) Implementation, (5) Confirmation.	Übernahme, Innovation, Entscheidung	Rogers 2003
Theorie des überlegten Handelns (TÜH) Theorie des geplanten Verhaltens (TGV)	Die Theorie des geplanten Verhaltens postuliert die Intention (Verhaltensabsicht) als zentralen Indikator bzgl. der Ausführung eines bestimmten Verhaltens. Sie ist eine Weiterentwicklung der Theorie des überlegten Handelns.	Meinung, Einstellung, Verhaltensintention, subjektive Norm, Verhaltensabsicht, wahrgenommene Verhaltenskontrolle	Fishbein und Ajzen 1975; Ajzen 1985, Ajzen und Madden 1986
Technology Acceptance Model (TAM)	Der wahrgenommene Nutzen sowie der wahrgenommene Bedienungskomfort bestimmen die Akzeptanz von Informationssystemen.	Akzeptanz, wahrgenommener Nutzen, wahrgenommener Bedienungskomfort	Davis 1986, Davis 1989; Davis et al. 1989

Name (Abkürzung)	Kernaussage(n)	Wichtige Konstrukte	Quellen
Theorie der Schutzmotivation (TSM)	Liegt eine Bedrohung für die eigene Person oder das gesellschaftliche Umfeld vor, dann hängt das Verhalten vom Bedrohungspotential sowie vom Potential zur Bewältigung der Bedrohung ab.	Schutzmotivation, Folgen des gesundheitsschädlichen Verhaltens, persönliche Betroffenheit, Maßnahmen zu Verhinderung der Folgen, Belohnungen	Rogers 1983
General Deterrence Theorie (GDT)	Die Zuverlässigkeit, Härte und Schnelligkeit von Sanktionen hat Einfluss auf die Entscheidung von Personen zur Begehung von Straftaten.	Zuverlässigkeit, Härte und Schnelligkeit von Sanktionen	Straub und Welke 1998

In den folgenden Abschnitten werden die einzelnen relevanten Theorien zunächst vorgestellt und auf deren Anwendung in der GRC-Literatur eingegangen. Hierdurch soll die generelle Nützlichkeit der Theorien plausibilisiert werden. Zugleich wird hierdurch die Möglichkeit geschaffen die Theorien nachvollziehbar den Anforderungskategorien zuordnen zu können. Es wird hierbei grundsätzlich angenommen, dass die jeweiligen Theorien im Kontext des strategischen GRC-Managements ähnliche Anwendungsgebiete aufweisen wie in den Teilbereichen von GRC.

3.3.2 Strategische Theorien

3.3.2.1 Darstellung der strategischen Theorien

Der Market- und Resource-based view versuchen die Entstehung von strategischen Wettbewerbsvorteilen (engl. competitive advantage) zu erklären. Unter einem Wettbewerbsvorteil wird eine wertschaffende Strategie verstanden, die von keinem gegenwärtigen oder zukünftigen Wettbewerber ebenfalls verfolgt wird. Um die Überlebensfähigkeit sicherzustellen, sind langfristige Wettbewerbsvorteile (engl. sustained

competitive advantage) zu schaffen. Hierunter werden Strategien verstanden, die zusätzlich zur Bedingung für einen Wettbewerbsvorteil auch keine Imitation der Strategie durch Wettbewerber ermöglichen (Barney 1991, S. 102). Der Market-based view soll hier auf das Modell der generischen Wettbewerbsstrategien von Porter (1980, S. 1985) zurückgeführt werden. Nach Porter (1996, S. 64) können Strategien nur dann zu einem Wettbewerbsvorteil führen, wenn sie durch unternehmerische Aktivitäten adäquat unterstützt werden. Porter unterscheidet drei generische Strategien: die Kostenführerschaft, die Differenzierung und die Fokusstrategie. In der Kostenführerschaft operiert ein Unternehmen mit günstigeren Kosten als seine Wettbewerber. Aufgrund dieser Kostenführerschaft sind Unternehmen in der Lage, Produkte zu geringeren Preisen anzubieten. Unternehmen, die eine Differenzierungsstrategie verfolgen, sollten sich in wichtigen Merkmalen, wie der Produktqualität oder überlegenen funktionale Produkteigenschaften von ihren Wettbewerbern unterscheiden. In der Fokusstrategie findet eine Konzentration auf bestimmte Märkte statt, wodurch ein Wettbewerbsvorteil hergestellt wird. Wie Krell und Matook (2009, S. 32) basierend auf Slaughter et al. (2006) ausführen, kann das Modell der Wettbewerbsstrategien von Porter (1980, S. 1985) helfen zu erklären, welchen Beitrag Informationssysteme zur Erzielung von Wettbewerbsvorteilen liefern. Krell und Matook (2009, S. 33) weisen ebenfalls darauf hin, dass neuere Untersuchungen zeigen, dass viele Unternehmen die Strategie der Kostenführerschaft aufgeben und zu einer Niedrigkostenstrategie wechseln. Diese versucht nicht mehr einen absoluten Kostenvorteil zu erzielen, sondern versucht die Kosten niedrig zu halten und gleichzeitig eine Differenzierung vorzunehmen (Tallon 2007).

Der Resource-based view stellt bei der Erklärung von Wettbewerbsvorteilen die Ressourcen eines Unternehmens in den Mittelpunkt. Unter

Ressourcen werden sowohl die Assets eines Unternehmens als auch Fähigkeiten, Geschäftsprozesse oder Wissen verstanden (Barney 1991, S. 101). Als Ressourcen können nach Williamson (1985) physische, menschliche und organisatorische Ressourcen unterschieden werden. Es wird angenommen, dass Ressourcen heterogen auf Unternehmen verteilt und gleichzeitig immobil sind (Barney 1991, S. 105). Damit eine Ressource das Potential hat, einen Wettbewerbsvorteil zu generieren, müssen folgende Kriterien erfüllt sein: (1) Wertvoll im Sinne eines wesentlichen Beitrags zum wahrgenommenen Kundennutzen; (2) Nicht imitierbar; (3) Nicht handelbar und (4) Nicht transferierbar auf neue Produkte oder Dienstleistungen (Barney 1991, S. 105-112). Wie von Rennenkampff (2015, S. 72-76) im Kontext der IT-Agilität hinweist, hat sich der ressourcenorientierte Ansatz auch in der Wirtschaftsinformatik-Forschung etabliert (siehe u.a. Melville et al. 2004, S. 291 und Wade und Hulland 2004, S. 109). Des Weiteren wird darauf hingewiesen, dass in neueren Arbeiten die Kriterien für Ressourcen erweitert bzw. verfeinert worden sind. So verwenden Wade und Hulland (2004, S. 115-117) sechs Eigenschaften von Ressourcen. Demnach müssen Ressourcen wertvoll, knapp und verwertbar sein, um einen Wettbewerbsvorteil zu ermöglichen. Zusätzlich müssen diese auch unnachahmlich, nicht substituierbar und immobil sein, um einen nachhaltigen Wettbewerbsvorteil zu ermöglichen.[42] Weitere wichtige Aspekte in neueren Arbeiten sind die Komplementarität von Ressourcen und moderierende Variablen wie Fähigkeiten (engl. capabilities), die darauf hinweisen, dass die Beziehung zwischen Ressourcen und einem Wettbewerbsvorteil nicht

[42] Übersetzung in Anlehnung an von Rennenkampff (2015, S. 74).

zwangsläufig unmittelbar sein muss (Wade und Hulland 2004, Liang und You 2009).

In der Literatur geht der Begriff Stakeholder auf Freeman (1984, S. 46) zurück. Dieser bezeichnet Individuen oder Gruppen als Stakeholder, wenn diese einen materiellen oder immateriellen Anspruch an das Unternehmen haben. Es kann zwischen internen Stakeholdern, wie Mitarbeitern und Eigentümern sowie externen Stakeholdern, wie dem Staat, der Gesellschaft, Fremdkapitalgebern, Kunden und Lieferanten, unterscheiden werden. Im Rahmen des Stakeholder-Ansatzes wird unterstellt, dass die Unternehmensführung die Interessen aller Stakeholder im Rahmen der unternehmerischen Entscheidungsprozesse berücksichtigen sollte (Freeman 1984; Mitroff 1983). Somit werden die Strategie und Ziele des Unternehmens unter Berücksichtigung der Stakeholderinteressen hergeleitet. Das Konzept des Stakeholder-Ansatzes steht im Gegensatz zum Shareholder-Ansatz, der sich lediglich an den Interessen der Eigentümer (Shareholder) orientiert und die Maximierung des Shareholder Values in den Mittelpunkt stellt (Rappaport 1999, S. 39). Mit diesen theoretischen Ansätzen wird somit die Zielfunktion von Unternehmen betrachtet, die entweder aus der Nutzenfunktion der Shareholder besteht oder sich aus einer (gewichteten) Aggregation der Nutzen aller Stakeholder zusammensetzt.

3.3.2.2 Anwendung der strategischen Theorien in der GRC-Literatur

Krell und Matook (2008; 2009) untersuchen im Rahmen einer empirischen Studie den Einfluss strategischer Planung auf verpflichtende, also aufgrund von regulatorischen Vorgaben notwendigen, Investitionen in Informationssysteme, wobei konkret auf das IS Planning and Investment Model (Henderson und Sifonis 1988), welches auf den Überle-

gungen von Porter zu Wettbewerbsstrategien basiert, zurückgegriffen wird.

Auf der Grundlage von Erkenntnissen des Resource-based view geht Mossanen (2010, S. 180-184) der Frage nach, auf welcher Art von Ressourcen Compliance aufbaut und ob hierdurch ein Wettbewerbsvorteil erzeugt werden kann. Hierbei wird festgestellt, dass Compliance einen Mix aus physischen, menschlichen und organisatorischen Ressourcen erfordert. Die Frage, ob durch Compliance-spezifische Ressourcen ein Wettbewerbsvorteil erzielt werden kann, wird zwar verneint, jedoch wird gleichzeitig betont, dass durch Compliance ein Nutzen generiert werden kann, der über die reine Erfüllung der Compliance-Vorgaben hinausgeht.

Kwon und Johnson (2013) untersuchen auf der Grundlage des Resource-based views den Einfluss von Ressourcen und Fähigkeiten auf die regulatorische Compliance bzgl. Informationssicherheit im Healthcare-Sektor. Es wird im zugrundeliegenden Forschungsmodell zwischen Informationssicherheitsressourcen, wozu die IT-Anwendungen und sonstige Ausstattung gehören, sowie funktionalen und Managementfähigkeiten unterschieden. Die empirische Studie zeigt, dass Ressourcen einen Einfluss auf Compliance haben, macht jedoch keine Aussage darüber, ob auf Basis dieser Ressourcen auch ein Wettbewerbsvorteil erzielt werden kann.

Lazic et al. (2011) sowie Neff et al. (2013) untersuchen die Beziehung zwischen IT-Governance und Business Performance auf der Basis eines ressourcentheoretischen Forschungsansatzes, wobei argumentiert wird, dass eine Zunahme an Business Performance Einfluss auf die Erzeugung von Wettbewerbsvorteilen hat. Die Autoren nehmen weiterhin Beziehung zu den Konzepten der Synergie, der Beziehung zwischen Ressourcen bzw. der Komplementarität von Ressourcen. Es wird ar-

gumentiert, dass IT-Governance Einfluss auf ein gleichzeitiges (komplementäres) Auftreten von geteilten IT-Ressourcen und geteilten Geschäftsprozessen zwischen verschiedenen Geschäftsbereichen hat, was wiederum eine Verbesserung der Business Performance bewirkt.

Oh et al. (2007) verwenden den ressourcentheoretischen Ansatz im Kontext des Risikomanagements. Die Autoren entwickeln ein konzeptionelles Modell, das IT-Fähigkeiten und Top-Management-Unterstützung als wesentliche Einflussfaktoren auf IT-unterstützte Risikomanagementfähigkeiten identifiziert. Diese haben wiederum Einfluss auf die „Organizational Performance".

Stakeholder sind, wie Pupke (2008, S. 45-46) betont, im Kontext von Compliance von besonderer Bedeutung, da regulatorische Vorgaben Stakeholderinteressen einen institutionellen Rahmen geben. Pupke gibt einen Stakeholder-Ansatz zur Bestimmung des Einflusses des Compliance-Managements auf den Unternehmenserfolg jedoch auf. Im Wesentlichen wird hierfür ein Komplexitätsproblem angeführt. Im Gegensatz zum Shareholder-Ansatz in welchem lediglich der Nutzen der Shareholder analysiert werden muss, müssten im Rahmen einer Stakeholder-Betrachtung die Nutzenfunktionen aller Stakeholder expliziert werden.

3.3.3 Ökonomische Theorien

3.3.3.1 Darstellung der ökonomischen Theorien

Der Theorie der rationalen Entscheidung folgend handeln Individuen rational, indem auf Grundlage bestimmter Präferenzen ein nutzenmaximierendes Verhalten erfolgt. Die Theorie der rationalen Entscheidung wird in verschiedenen Kontexten angewendet. Hierzu gehört auch die Kriminologie, wobei argumentiert wird, dass Kriminelle die Entscheidung zur Begehung von Straftaten auf der Grundlage einer

Abwägung des erwarteten Nutzens sowie der erwarteten Strafe treffen (siehe bspw. Becker 1968; McCarthy 2002) zur Anwendung der Theorie der rationalen Entscheidung in Kontext der Kriminologie, auf welchen in den Anwendungen in der GRC-Literatur eingegangen wird).

Die grundlegenden Annahmen der Transaktionskostenökonomik sind neben begrenzter Rationalität, opportunistisches Verhalten der Akteure sowie Unsicherheit. Jeder Austausch von Gütern zwischen zwei oder mehreren Akteuren stellt eine Transaktion dar. Eine Transaktion besteht aus der Suche nach den Vertragspartnern, dem Aufstellten des Vertrages und dem Austausch der Güter (Jost 2001, S. 11). Nach Williamson (1985, S. 52-61) können drei Charakteristika von Transaktionen unterschieden werden. (1) Transaktionsspezifische Investition sind Investitionen in Inputfaktoren, die zur Erstellung eines Gutes spezifisch angepasst sind. (2) Unsicherheit kann sich aus den situativen Bedingungen der Transaktion ergeben (parametrische Unsicherheit) oder aus möglichem opportunistischen Verhalten der Transaktionspartner folgen. (3) Die Häufigkeit einer Transaktion zwischen gleichen Transaktionspartnern hat maßgeblichen Einfluss auf die Realisierung von Synergie- und Skaleneffekten. Williamson (1985, S. 20-22) unterscheidet fünf Arten von Transaktionskosten, die vor (ex ante) oder nach (ex post) Vertragsabschluss entstehen können. Dies sind (1) Informations- und Suchkosten (ex ante), (2) Verhandlungs- und Vertragskosten (ex ante), (3) Überwachungskosten (ex post), (4) Konflikt- und Durchsetzungskosten (ex post) und (5) Anpassungskosten für Vertragsänderungen (ex post). Um die relative Vorteilhaftigkeit eines institutionellen Arrangements beurteilen zu können, sind neben den Charakteristika der Transaktion die Charakteristika des institutionellen Arrangements entscheidend (Ebers und Gotsch 2006, S. 284; Williamson 1985, S. 68). Williamson (1985, S. 68-72) greift zur Analyse institutioneller Arrange-

ments von Transaktionen auf die Unterscheidung von Vertragsformen nach MacNeil (1974; 1978; 1987) zurück. Demnach können klassische, neoklassische und relationale Vertragsbeziehungen unterschieden werden. Klassische Vertragsbeziehungen bezeichnen typische Markttransaktionen (Williamson 1985, S. 69). Relationale Vertragsbeziehungen kennzeichnen Transaktionen, die innerhalb von Organisationen abgewickelt werden. Neoklassische Verträge sind ein Hybrid zwischen der Abwicklung des Leistungsaustauschs über den Markt oder innerhalb von Organisationen.

Die Prinzipal-Agenten-Theorie basiert auf den gleichen Annahmen wie die Transaktionskostenökonomik und untersucht die Beziehung zwischen mindestens zwei Personen, dem Prinzipal und Agenten, wobei die Handlungen des Agenten die Wohlfahrt des Prinzipals und des Agenten beeinflusst. Aufgrund unterschiedlicher Nutzenfunktionen kann der Prinzipal nicht erwarten, dass der Agent stets in seinem Interesse handelt (Arrow 1985, S. 37). Die Beziehung von Prinzipal und Agent ist häufig durch Informationsasymmetrien gekennzeichnet. Hierbei sind mit Hidden Action und Hidden Information zwei Typen zu unterschieden (Arrow 1985, S. 38). Im Fall von Hidden Action sind die Handlungen des Agenten nicht beobachtbar oder die Transaktionskosten hierfür prohibitiv hoch. Da das Verhalten des Agenten nicht verifizierbar ist, besteht ein moralisches Risiko (engl. moral hazard), dass der Agent diese Informationsasymmetrie zu seinem Vorteil ausnutzt. Hidden Information beschreibt eine Situation der Informationsasymmetrie, in welcher für den Prinzipal Informationen über die Eigenschaften des Agenten oder dessen Leistung nicht verfügbar sind (Arrow 1985, S. 38-40). In der Prinzipal-Agenten-Beziehung werden drei Kostenarten unterschieden (Jensen und Meckling 1976, S. 308). Monitoring-Kosten bestehen in der Definition von Zielen, der Errichtung von

Anreizsystemen und der Kontrolle der Ergebnisse aus den Handlungen des Agenten. Bonding-Kosten entstehen beim Agenten durch Unterlassung von Aktionen, die nicht die Wohlfahrt des Prinzipals maximieren. Wohlfahrtsverluste (engl. residual loss) entstehen, da der Prinzipal aufgrund von Transaktionskosten das Verhalten des Agenten nicht perfekt an seinen Interessen ausrichten kann.

Eine weitere Frage, die sich im Kontext der Prinzipal-Agenten-Beziehung stellt, ist die Ausgestaltung der Kontrollen zur Ausrichtung des Verhaltens des Agenten an den Interessen des Prinzipals. Mit dieser Frage setzt sich die Theorie der organisatorischen Kontrollen (Organizational Control Theory) auseinander (Ouchi 1979). Unter Kontrollen können alle Einflussbeziehungen in einem Unternehmen verstanden werden (Ouchi 1979, S. 833). Kontrollen oder Kontrollmechanismen können entweder formal oder informal gestaltet sein. Formale Kontrollen wirken durch formale Strukturen und Regeln, wie Anreizsysteme. Informale Kontrollen beziehen sich auf die Werte und Normen von Organisationen (Ouchi 1979, S. 834). Außerdem können Kontrollen in prozessorientierte und ergebnisorientierte Kontrollen unterschieden werden. Ein prozessorientierter Kontrollansatz zielt auf das Monitoring des Agenten ab, wohingegen ein ergebnisorientierter Kontrollansatz, der aufgrund der geringeren Transaktionskosten häufig präferiert wird, in Form von Anreizsystemen gestaltet wird, die eine Angleichung der Interessen des Prinzipals und Agenten bewirken sollen. In diesem Fall werden lediglich das Ergebnis der Handlung und nicht die Handlung selbst kontrolliert (Lange 2008, S. 712).

Die Annahmen der Prinzipal-Agenten-Theorie sind, insbesondere im Rahmen der Corporate Governance Debatte, jedoch nicht ohne Kritik (siehe bspw. Donaldson 1990; Müller 1995). So wird argumentiert, dass Corporate Governance-Mechanismen, die nach der Prinzipal-Agenten-

Theorie abgeleitet werden, bestenfalls ineffektiv und im schlimmsten Fall sogar nachteilig sein können. Die Stewardship-Theorie ist ein alternativer Vorschlag und geht von grundlegend anderen Verhaltensannahmen aus. Insbesondere das unterstellte opportunistische Verhalten der Agenten und die hierdurch notwendige extrinsische Motivation, werden in der Stewardship-Theorie verworfen. Stattdessen wird eine von Vertrauen erfüllte Beziehung zwischen Prinzipal und Steward unterstellt und von einer Zielkonformität zwischen den Beteiligten ausgegangen. Schlussfolgernd existieren somit zwei unterschiedliche theoretische Perspektiven, die zu unterschiedlichen Empfehlungen kommen (Tosi et al. 2003, S. 2055, für eine detaillierte Analyse dieser Problematik siehe Grundei 2008).

3.3.3.2 Anwendung der ökonomischen Theorien in der GRC-Literatur

Die Theorie der rationalen Entscheidung wird sowohl von Al-Omari et al. (2012b) als auch von Bulgurcu et al. (2010) und Hu et al. (2011) zur Untersuchung des Compliance-Verhaltens in Hinblick auf Richtlinien der Informationssicherheit angewendet. Die Anwendung der Theorie erfolgt bei Al-Omari et al. (2012b) und Bulgurcu et al. (2010) durch eine Kombination mit weiteren verhaltenswissenschaftlichen Theorien. Bulgurcu et al. (2010) unterscheiden hierzu den individuellen Nutzen von Compliance (bspw. Belohnungen), die Kosten von Compliance (konkretisiert durch den Arbeitsaufwand) und die Kosten von Non-Compliance (bspw. Sanktionen). Sie stellen damit ebenso wie Hu et al. (2011, S. 56) die Theorie der rationalen Entscheidung ins Zentrum ihres Forschungsmodells und erklären die Entscheidung zu normkonformen Verhalten im Wesentlichen durch ein wirtschaftliches Kalkül.

Pupke (2008, S. 54-80) analysiert mit Hilfe der Transaktionskostenökonomik Koordinationsformen für das Compliance-Management. Er

identifiziert hierbei den „Hybrid Compliance Approach“ als beste Koordinationsform des Compliance-Managements. Dieser ist eine dezentralisierte Koordinationsform und integriert die Compliance-Aktivitäten in die Primärorganisation.[43] Gleichzeitig sollen jedoch alle Aktivitäten und speziell die Implementierung neuer Anforderungen zentral koordiniert werden (Pupke 2008, S. 79).[44] Christiaanse und Hulstijn (2012) untersuchen hingegen nicht die allgemeine Koordination des Compliance-Managements, sondern die Kosten von Kontrollen auf der Grundlage der Transaktionskostentheorie.

Die Prinzipal-Agenten-Theorie wird im Kontext von GRC in einem breiten thematischen Spektrum angewendet. Mossanen (2010, S. 177-180) stellt in diesem Zusammenhang fest, dass im Kontext von Compliance verschiedene hierarchisch angeordnete Prinzipal-Agenten-Beziehungen existieren. Einerseits sind die Stakeholder als Prinzipale zu verstehen, die von Unternehmen (Agenten) die Einhaltung der regulatorischen Vorgaben als Teil der Erfüllung ihrer Interessen erwarten. Interne Prinzipal-Agenten-Beziehungen existieren zwischen Aufsichtsrat und Vorstand sowie zwischen dem Vorstand bzw. Management und den Mitarbeiten. Die Prinzipal-Agenten-Theorie wird von Pupke (2008, S. 53-54) außerdem zur Untersuchung eines optimalen Compliance-Levels aufgegriffen. Im Rahmen dieser Analyse werden auf abstraktem Niveau die Kosten der Implementierung von Compliance-Standards gegen die hiermit verbundene Einsparung von Agenturkosten gestellt.

---

[43] Die Primärorganisation beschreibt die aufbauorganisatorische, hierarchisch angelegte Grundstruktur der Organisation. Ergänzend hierzu kann eine Sekundärorganisation etabliert werden, die hierarchieübergreifend und oftmals bspw. in Form der Projektorganisation zeitlich befristet ist (Bea und Göbel 2006, S. 375-410).

[44] Detaillierte Ausführungen hierzu finden sich in Abschnitt 3.4.2.2.

Liang et al. (2011) beziehen die Agenturproblematik auf die Ausgestaltung der Entscheidungsrechte von Top-Managern. Da auch Top-Manager als Eigennutzenmaximierer verstanden werden, sollten zur Minimierung möglicher negativer Auswirkungen dieser Verfolgung von Eigeninteressen daher Entscheidungsbefugnisse möglichst auf unterschiedliche Entscheidungsträger mit verschiedenen Interessenslagen verteilt werden. Verschiedene Autoren untersuchen zudem das Compliance-Verhalten auf der Grundlage der Prinzipal-Agenten-Theorie und untersuchen Anreizsysteme, Kontroll- und Überwachungsmechanismen sowie Transparenzpflichten (Becker et al. 2011c; Boss et al. 2009; Panitz et al. 2011). Boss et al. (2009) betonen zudem insbesondere die Bedeutung der formalen Spezifikation der Vorgaben. Ali et al. (2009, S. 2-3) greifen darüber hinaus die Agenturtheorie auf allgemeiner Ebene als theoretische Basis zur Untersuchung der Compliance-Kultur im Kontext der IT-Governance auf. Grundei (2006) stellt in seinem Beitrag den reinen Fokus auf die Prinzipal-Agenten-Theorie in Frage. Er untersucht die Beziehung zwischen vertrauens- und kontrollbasierten Ansätzen der Organisationsgestaltung.

Lange (2008) untersucht auf Basis der Prinzipal-Agenten-Theorie unterschiedliche Kontrolltypen im Kontext der Korruptionsbekämpfung. Hierbei wird die Unterscheidung zwischen sozialen bzw. kulturellen und administrativen Kontrollen einerseits sowie die Unterscheidung von prozess- und ergebnisorientierten Kontrollen andererseits entwickelt. Die Kontrollen werden weiterhin den vier Quadraten Autonomiereduzierung (engl. autonomy reduction), Konsequenz-Systeme (engl. consequence systems), umweltbezogene Sanktionierung (engl. environmental sanctioning) und intrinsisch motivierte Kontrollen zugeordnet (Lange 2008, S. 715). Christ et al. (2012) untersuchen bezugnehmend auf die Prinzipal-Agenten-Theorie die Effekte von präven-

tiven und detektiven Kontrollen auf die Motivation von Mitarbeitern. Es wird festgestellt, dass präventive und detektive Kontrollen grundsätzlich ähnliche Auswirkungen auf das Verhalten haben, wobei bei detektiven Kontrollen das Feedback zu Regelverstößen zeitnah erfolgen sollte. Verschiedene Autoren setzen an dieser Thematik an und untersuchen im Speziellen die Ausgestaltung der Kontrollen, die durch die Prinzpal-Agenten-Theorie intendiert werden, auf Basis der Organisational Control Theorie (Boss et al. 2009; Heumann und Wiener 2012; Liang et al. 2013; Lowry und Moody 2013; Wiesche et al. 2012; Wiesche et al. 2011b). Zum einen wird hierbei das Compliance-Verhalten im Kontext der Informationssicherheit untersucht (Boss et al. 2009; Liang et al. 2013; Lowry und Moody 2013). Wichtige Konstrukte sind Belohnung (engl. reward) und Strafe (engl. punishment) sowie das Vorhandensein von formalisierten Kontrollen. Heumann und Wiener (2012) untersuchen den Zusammenhang zwischen formalen und kulturellen Kontrollen, wobei nahegelegt wird, dass formale Kontrollen bspw. im Rahmen von Ergebniskontrollen eine kulturelle Kontrolle durch die Gruppe fördert. Wiesche et al. (2012) untersuchen die Vorbedingungen zur Gestaltung von Kontrollen und berücksichtigen hierbei auch die Rolle der IT. Sie zeigen, dass durch IT neue Möglichkeiten zur Ausgestaltung von Kontrollen entstehen. In einem weiteren Beitrag (Wiesche et al. 2011b), der auf die Organisational Control Theorie Bezug nimmt, wird zudem nahegelegt, dass durch eine Automatisierung von Kontrollen Kosteneinsparungen erzielt werden können.

3.3.4 Verhaltenswissenschaftliche Theorien

3.3.4.1 Darstellung der verhaltenswissenschaftlichen Theorien

Institutionalistische Theorien können in Marko- und Mikroinstitutionalistische Ansätze unterschieden werden (Jörges-Süß und Süß

2004; Walgenbach 2006). Makro-Ansätze betrachten den Einfluss der Umwelt auf Organisationen (Jörges-Süß und Süß 2004; Walgenbach 2006, S. 357). Bei Mikro-Ansätzen werden Unternehmen selbst als Institutionen betrachtet, welche institutionelle Strukturen entwickeln und ihre Umwelt beeinflussen (DiMaggio und Powell 1983; DiMaggio und Powell 1991; Meyer und Rowan 1997). Da die erste Perspektive im Kontext von GRC relevant ist, soll diese im Weiteren betrachtet werden. In der institutionalistischen Theorie kann Institutionalisierung als Prozess oder Zustand verstanden werden (Tolbert und Zucker 1983; Zucker 1983). Als Prozess bezieht sich Institutionalisierung auf die Entwicklung von sozialen Beziehungen und Handlungen zu Selbstverständlichkeiten. Als Zustand bezeichnet Institutionalisierung Situationen, in denen die gesellschaftlichen Vorstellungen die Bedeutung und Möglichkeit von sozialen Handlungen festlegen (Walgenbach 2006, S. 255; DiMaggio und Powell 1991, S. 9). Bezogen auf Unternehmen bedeutet Institutionalisierung, dass bestimmte organisatorische Elemente zu Unternehmen gehören, ohne dass deren Existenz hinterfragt wird (Walgenbach 2006, S. 255; DiMaggio und Powell 1991, S. 9). Hierbei wird argumentiert, dass die Aufbau- und Ablauforganisation von Unternehmen nicht ausschließlich nach Effektivitäts- und Effizienzkriterien ausgewählt wird, sondern dass die Unternehmensumwelt einen erheblichen Einfluss ausübt. Organisationen streben Legitimität formaler Strukturen an, indem sie die Erwartungen verschiedener Anspruchsgruppen erfüllen. Die Legitimität hat somit Bedeutung für die Überlebensfähigkeit von Organisationen (Meyer und Rowan 1997, S. 343; DiMaggio und Powell 1983). Weiterhin wird im Rahmen der institutionalistischen Theorie das Argument vorgebracht, dass Institutionen Handlungsspielräume einschränken und daher Unternehmen, die mit ähnlichen Umwelterwartungen konfrontiert sind, sich einander angleichen. Dies wird als Isomorphismus bezeichnet, wobei Zwang, Nach-

ahmung und normativer Druck eine Rolle spielen (DiMaggio und Powell 1983, S. 150).

Die Diffusionstheorie befasst sich im Kontext der Wirtschaftswissenschaften mit der Verbreitung von Innovationen im Sinne neuer Produkte und Prozesse (Malik 2009, S. 99). Rogers (2003, S. 5) definiert Diffusion als „the process in which an innovation is communicated through certain channels over time among the members of a social system". Der Diffusionsprozess setzt sich dieser Definition folgend aus insgesamt vier Hauptkomponenten zusammen: (1) der Innovation selbst, (2) den Kommunikationskanälen, (3) der Zeitkomponente und (4) dem sozialen System (Rogers 2003, S. 11-35). Der Begriff Innovation wird von Rogers recht breit definiert und umfasst Ideen, Praktiken oder Objekte, die von einem Individuum oder einer anderen Einheit, die die Adoption vollziehen soll, als neu empfunden wird (Rogers 2003, S. 12). Es ist leicht nachzuvollziehen, dass im Rahmen dieser Definition auch bspw. Compliance-Vorgaben als Innovationen angesehen werden können. Nach Rogers (2003, S. 168-194) kann der Diffusionsprozess, der die Adaption von Innovationen im Zeitverlauf beschriebt, mit Hilfe der fünf Stufen Bewusstsein (engl. knowledge), Überzeugung (engl. persuasion), Entscheidung (engl. decision), Implementierung (engl. implementation) und Bestätigung (engl. confirmation) (Übersetzung gemäß Mann 2009, S. 105) beschrieben werden. Personen erhalten in allen Phasen Informationen über die Innovation, die ihre Adoptionsentscheidung beeinflussen.

In den Sozialwissenschaften haben sich in den 1970er Jahren verschiedene Modelle entwickelt, die Verhalten auf der Grundlage von mehreren Komponenten erklären. In der wissenschaftlichen Diskussion haben die Theorie des überlegten Handelns (engl. theory of reasoned action) von Fishbein und Ajzen (1975) sowie dessen Erweiterung zur

Theorie des geplanten Verhaltens (engl. theory of planned behavior) von Ajzen (Ajzen 1985) bzw. Ajzen und Madden (1986) die meiste Aufmerksamkeit erlangt (siehe hierzu auch Frey et al. 2001, S. 366-367). Die Theorie des überlegten Handelns postuliert eine Kausalbeziehung zwischen Meinungen (engl. beliefs), Einstellungen (engl. attitudes), Verhaltensintentionen (engl. intentions) und dem tatsächlich ausgeführten Verhalten. Das tatsächliche Verhalten wird zudem direkt durch die Verhaltensintention beeinflusst. Die Verhaltensintention wird wiederum durch die Einstellung gegenüber dem Verhalten sowie die subjektive Norm determiniert. Die Einstellung erfasst, ob ein Individuum ein bestimmtes Verhalten positiv oder negativ bewertet. Die subjektive Norm ergibt sich aus der subjektiven Wahrnehmung, ob die Ausführung eines bestimmten Verhaltens vom sozialen Umfeld erwartet oder nicht erwartet wird. Normen werden als wahrgenommene soziale Vorschriften verstanden. Die relative Wichtigkeit der Determinanten variiert in Abhängigkeit von der spezifischen Situation. Die Theorie des überlegten Handelns bezieht sich nur auf willentliches Verhalten. Gerade die persönliche Kontrolle über das eigene Verhalten ist jedoch häufig eingeschränkt. Die Theorie des geplanten Verhaltens (Ajzen 1985; Ajzen und Madden 1986) erweitert daher die Theorie des überlegten Handelns um die Komponente der wahrgenommenen Verhaltenskontrolle (engl. perceived behavioral control), die sowohl die Verhaltensintension als auch das tatsächliche Verhalten direkt beeinflusst. Determinanten der wahrgenommenen Verhaltenskontrolle sind Ressourcen, Fähigkeiten und Verhaltensmöglichkeiten.

Das Technology Acceptance Model (TAM) ist eine Adaption der Theory of Reasoned Action und wurde für die Erklärung der Akzeptanz von Informationssystemen entwickelt. Zentral für die Akzeptanz von Informationssystemen sind demnach der wahrgenommene Nutzen (engl.

perceived usefulness) und der wahrgenommene Bedienungskomfort (engl. perceived ease of use). Davies (1986; 1989) bzw. Davis et al. (1989, S. 985-989) definieren den wahrgenommenen Nutzen als den „Grad, zu welchem eine Person glaubt, dass das Verwenden einer Technologie ihre Leistungen bei ihrer Arbeit verbessert“ und den wahrgenommenen Bedienungskomfort als den „Grad, zu welchem eine Person glaubt, dass die Verwendung einer Technologie frei von Aufwand sei“. Beide Konstrukte beeinflussen die Einstellung (engl. behavioral intention) zur Nutzung des Informationssystems. Die Einstellung beeinflusst wiederum die Verhaltensabsicht. Hierdurch kann die tatsächliche Nutzung (engl. actual use) des Informationssystems erklärt werden. Im Jahre 2003 wurde das Modell zur Unified Theory of Acceptance and Use of Technology weiterentwickelt (Venkatesh et al. 2003), die eine Integration der wichtigsten Theorien erreichen soll. Demnach beeinflussen die Aufwandserwartung, die Leistungserwartung und der soziale Einfluss maßgeblich die Verhaltensabsicht. Außerdem haben erleichternde Bedingungen einen direkten Einfluss auf das Nutzungsverhalten.

Die Theorie der Schutzmotivation (engl. protection motivation theory) (Rogers 1983) wurde im Kontext der Gesundheitspsychologie entwickelt um zu erklären unter welchen Bedingungen Individuen gesundheitsschädigendes Verhalten beibehalten bzw. ihr Verhalten hin zu gesundheitsbewussten Verhalten ändern (Frey et al. 2001, S. 386). Die Theorie erklärt gesundheitsbewusstes Verhalten durch die Schutzmotivation, welche durch die Folgen eines nicht gesundheitsbewussten Verhaltens, die Wahrscheinlichkeit der persönlichen Betroffenheit durch die Folgen, das Vorhandensein effektiver Maßnahmen zur Verhinderung der negativen Folgen und durch die intrinsischen und extrinsischen Belohnungen des gesundheitsbewussten Verhaltens beeinflusst

wird. Die Theorie der Schutzmotivation betont ergänzend zur Theorie des geplanten Verhaltens die persönliche Betroffenheit und das gegenseitige Abwägen verschiedener Handlungsalternativen (Frey et al. 2001, S. 387).

Die General Deterrence Theorie (Straub und Welke 1998) erklärt die Funktionsfähigkeit von Gegenmaßnahmen, die von einer Normverletzung abschrecken sollen. Die Theorie besitzt eine weite Verbreitung in der Kriminologie und stellt heraus, dass Individuen durch Sanktionen von einer Absicht zu unsozialem Verhalten abgebracht werden können. Die General Deterrence Theorie betont insbesondere die Bedeutung von Zuverlässigkeit, Härte und Schnelligkeit von Sanktionen. Higgens et al. (2005, S. 169-170) verweisen darüber hinaus auf die Bedeutung sozialer Missbilligung, eigenem Missfallen und Impulsivität hin.

3.3.4.2 Anwendung der verhaltenswissenschaftlichen Theorien in der GRC-Literatur

Die institutionalistische Theorie wird in der ausgewerteten Literatur (Asprion und Knolmayer 2013; Braganza und Desouza 2006; Butler und McGovern 2008; Currie 2008; Hu et al. 2007; Jacobson 2009; Krell et al. 2009; MacLean und Behnam 2010; Yayla 2011) insbesondere zur Analyse der internen und externen institutionellen Einflüsse auf die (IT)-Compliance oder IT-Governance eingesetzt. Insgesamt wird festgestellt, dass verschiedene institutionelle Kräfte bei der Umsetzung von Compliance von Bedeutung sind, wobei sowohl Zwang, Nachahmung als auch normativer Druck von Bedeutung sind (Braganza und Desouza 2006; Butler und McGovern 2008; Currie 2008; Hu et al. 2007; Jacobson 2009). Dieses vielschichtige institutionelle Umfeld führt zu teilweise konfliktären Anforderungen an die Umsetzung von Compliance (Currie 2008). MacLean und Behnam (2010) untersuchen auf der Basis der institutionalistischen Theorie darüber hinaus die Entkopplung von

Compliance-Programmen von den operativen Geschäftsaktivitäten. Hierdurch kann es zum Vortäuschen von Compliance zur Aufrechterhaltung der Legitimität gegenüber externen Institutionen kommen. Asprion und Knolmayer (2013) stellen fest, dass institutionelle Einflüsse einen signifikanten Effekt auf die Assimilation von Compliance-Software haben. Krell et al. (2009) untersuchen die Effekte von regulatorischen Vorgaben, welche als normativer Druck im Sinne der institutionalistischen Theorie verstanden werden, auf den Erfolg der Adaption von Informationssystemen. Es wird behauptet, dass regulatorische Vorgaben sowohl positive als auch negative Effekte auf Erfolgsfaktoren der Adaption von Informationssystemen haben können. Die institutionellen Unterschiede in multinationalen Unternehmen und deren Einfluss auf die Ausgestaltung auf Richtlinien der Informationssicherheit werden von Yayla (2011) untersucht. Es wird argumentiert, dass bei der Ausgestaltung der Richtlinien der institutionelle Kontext berücksichtigt werden sollte. Ist dieser zwischen der Muttergesellschaft und Tochterunternehmen unterschiedlich, wird eine Durchsetzung von einheitlichen Richtlinien erschwert.

In der GRC-Literatur existieren eine Vielzahl von Arbeiten zur Diffusionstheorie (Al-Omari et al. 2012a; Pahnila et al. 2007), zur Theorie des überlegten Handelns (Al-Omari et al. 2012b; Guo und Yuan 2012; Herath und Rao 2009; Lebek et al. 2013; Pahnila et al. 2007; Siponen et al. 2006), zur Theorie des geplanten Verhaltens (Al-Omari et al. 2013; Al-Omari et al. 2012a; Al-Omari et al. 2012b; Aurigemma und Panko 2012; Bulgurcu et al. 2009; Bulgurcu et al. 2010; Herath und Rao 2009; Hu et al. 2012; Lebek et al. 2013; Milicevic und Goeken 2013a; Milicevic und Goeken 2013b; Milicevic und Goeken 2012; Siponen et al. 2006), zum TAM (Al-Omari et al. 2012b; Boss et al. 2009; Cannoy und Salam 2010; Lebek et al. 2013; Xue et al. 2011), zur Theorie der

Schutzmotivation (Herath und Rao 2009; Johnston und Warkentin 2010; Lebek et al. 2013; Pahnila et al. 2007; Vance et al. 2012) und zur General Deterrence Theorie (D' Arcy et al. 2009; Goo et al. 2012; Guo und Yuan 2012; Herath und Rao 2009; Lebek et al. 2013; Pahnila et al. 2007; Siponen et al. 2006; Siponen und Vance 2010; Son 2011). Wie auch an den Literaturverweisen zu erkennen ist, verwenden die Mehrzahl der Arbeiten mehrere theoretische Perspektiven, weshalb nachfolgend keine getrennte Darstellung nach den Theorien erfolgt, sondern eine Zusammenfassung auf der Grundlage der wichtigsten theoretischen Konstrukte vorgenommen wird. Detaillierte Analysen zu den theoretischen Grundlagen der Forschung zum Compliance-Verhalten im Kontext der Informationssicherheit sind in den Literaturreviews von Lebek et al. (2013) sowie Milisevic und Goeken (2012; 2013a; 2013b) zu finden.

Die Arbeiten zum Compliance-Verhalten im Kontext der Informationssicherheit (Abraham 2011; Al-Omari et al. 2013; Al-Omari et al. 2012a; Al-Omari et al. 2012b; Aurigemma und Panko 2012; Boss et al. 2009; Bulgurcu et al. 2009; Bulgurcu et al. 2010; D' Arcy et al. 2009; Goo et al. 2012; Guo und Yuan 2012; Herath und Rao 2009; Hu et al. 2012; Hsu 2009; Hu et al. 2011; Johnston und Warkentin 2010; Johnston et al. 2010; Lebek et al. 2013; Liang et al. 2013; Lowry und Moody 2013; Milicevic und Goeken 2012; Milicevic und Goeken 2013a; Milicevic und Goeken 2013b; Myyry et al. 2009; Pahnila et al. 2007; Puhakainen und Siponen 2010; Siponen et al. 2006; Siponen und Vance 2010; Son 2011; Spears und Barki 2010; Vance et al. 2012; Yayla 2011), die auf verhaltenswissenschaftliche Theorien zurückgreifen, können zum einen die Relevanz der Theorie der überlegten Handelns und des geplanten Verhaltens für das Compliance-Verhalten aufzeigen. Hierbei stehen die Konstrukte Einstellung, subjektive Norm, Verhaltensabsicht

und das tatsächliche Compliance-Verhalten im Zentrum. Neuere Arbeiten versuchen die Determinanten, die dieses Verhalten beeinflussen zu untersuchen. Diese Determinanten bestehen aus Konstrukten der weiteren Theorien wie der Theorie der Schutzmotivation, der General Deterrence Theorie und des Technology Acceptance Models. Sie beinhalten insbesondere Konstrukte der intrinsischen und extrinsischen Motivation für Compliance. Weitere Einflussfaktoren wie das Bewusstsein (Awareness) für Informationssicherheit und Technologie im Allgemeinen sowie die Sichtbarkeit (engl. visibility) der Informationssicherheits-Maßnahmen werden aus der Diffusionstheorie abgeleitet.

3.3.5 Zwischenfazit

In diesem Abschnitt wurden die in der GRC-Literatur verwendeten Theorien identifiziert, grob strukturiert, die relevanten Aspekte anhand der einschlägigen Grundlagenliteratur dargestellt und auf die Anwendungen in der GRC-Literatur eingegangen. Es ist festzustellen, dass bislang keine dominante theoretische Perspektive im Kontext von GRC existiert. Das Kapitel zeigt vielmehr, dass GRC vielfältige Aspekte aufweist, die nicht anhand einer einzigen theoretischen Perspektive erklärt werden können und somit mehrere Theorien eingesetzt werden sollten. Die in diesem Kapitel dargestellten Theorien stellen hierfür eine gute Grundlage dar. Insbesondere ist es möglich, jeder noch zu entwickelnden Anforderungskategorie mindestens eine Theorie zuzuordnen. Da die Theorien bereits zu GRC-bezogenen Fragestellungen eingesetzt wurden, ist auch von einer Relevanz für das strategische GRC-Management auszugehen. Die Vorstrukturierung der Theorien in die Gruppen strategisch, ökonomisch und verhaltenswissenschaftlich sowie

die Darstellung der Anwendungen in der relevanten Literatur ermöglicht eine nachvollziehbare Zuordnung der Theorien zu den noch herzuleitenden Anforderungskategorien.[45]

3.4 Anforderungen für das strategische GRC-Management

3.4.1 Identifikation der Anforderungskategorien

Wie bereits ausgeführt stellen Anforderungen eine Klasse von Zielen dar (Walls et al. 1992, S. 42-43; Fischer et al. 2010, S. 384) und sollten, wie von Walls et al. (1992; 2004) explizit gefordert, auf Grundlage von Theorien begründet werden. Der Begriff Anforderung kann in Anlehnung an den Standardglossar des Institute of Electrical and Electronics Engineers (IEEE) konkretisiert werden (siehe hierzu auch Baskerville und Pries-Heje 2010, S. 262-263 im Kontext der erklärenden Designtheorie). Eine Anforderung ist demnach:

1. „eine Bedingung oder Fähigkeit, die der Anwender benötigt, um ein Problem zu lösen oder ein Ziel zu erreichen;
2. eine Bedingung, die ein System oder eine Systemkomponente erfüllen oder besitzen muss, um einem Vertrag, einer Norm, einer Spezifikation oder einem anderen förmlich auferlegten Dokument zu entsprechen;
3. eine Dokumentation einer Bedingung gemäß (1) und (2)." (Baskerville und Pries-Heje 2010, S. 263).

[45] Siehe hierzu Abschnitt 3.4.1 und insbesondere Tab. 6.

Nachfolgend werden Anforderungskategorien für das strategische GRC-Management in der Literatur identifiziert und dann auf Grundlage relevanter Theorien in konkrete Anforderungen überführt. Im weiteren Text wird zwischen Anforderungskategorien, Unterkategorien und Anforderungen unterschieden. Anforderungskategorien stellen das direkte Ergebnis der Literaturauswertung und des Kodierungsprozesses im Rahmen der qualitativen Inhaltsanalyse dar. Sie identifizieren die relevanten Anforderungsbereiche und basieren auf einer Verdichtung von Unterkategorien. Anforderungen werden auf Basis der theoretischen Untersuchung der Anforderungskategorien formuliert und stellen konkrete Handlungsempfehlungen zur Errichtung, Bewertung und Weiterentwicklung von GRC-bezogenen Management-Ansätzen dar.

Zur Herleitung der Anforderungskategorien wurde methodisch auf die qualitative Inhaltsanalyse zurückgegriffen. Allgemein können quantitative und qualitative Inhaltsanalysen unterschieden werden. Während erstere auf die Überprüfung von Hypothesen abzielen, dienen letztere zur Erschließung des Bedeutungsinhalts von Kommunikationsinhalten bspw. in Form von Texten. Für solche Analysen existiert eine Vielzahl von Verfahren (siehe bspw. Krippendorff und Bock 2009; Mayring 2008), aus denen mit Blick auf das Forschungsziel ein geeignetes auszuwählen ist. Während quantitative Inhaltsanalysen den Vorteil der Exaktheit aufweisen, erscheinen diese jedoch oftmals inhaltsleer. Diesen Nachteil versuchen qualitative Inhaltsanalysen zu beseitigen, sind jedoch oftmals mit dem Vorwurf einer mangelnden Objektivität konfrontiert (Atteslander 2010, S. 195-224). Die Objektivität könnte durch den Einsatz voneinander unabhängiger Forscher im Kodierungsverfahren erhöht werden. Da das vorliegende Forschungsprojekt jedoch ein Promotionsvorhaben ist, stand diese Option nicht zur Verfügung. Im vorliegenden Fall sollen Anforderungen an einen GRC-Management-

Ansatz aus der bestehenden Literatur hergeleitet werden. Hierzu wird ein Kodierungsverfahren eingesetzt, das auch Bestandteil der Grounded Theory ist. Die Grounded Theory verfolgt das Ziel der Bildung von Theorien auf Basis von empirischen Daten und ist den qualitativen Forschungsmethoden zuzuordnen. Sie ist eine anerkannte Forschungsmethode der Organisations- und Managementforschung (siehe hierzu bspw. Goulding 2002, S. 50). Als Daten können Interviews ebenso wie publiziertes Material herangezogen werden.

Bei der Datenanalyse können die drei Kodierungstypen offenes, axiales und selektives Kodieren unterschieden werden. Im Zuge des offenen Kodierens wird der Text „geöffnet". Solche Aussagen, die einander ähneln, werden in sogenannte Kernkategorien (hier als Unterkategorien bezeichnet) zusammengeführt. Das axiale Kodieren entwickelt diese Kategorien weiter. Ziel dieser Analyse ist es durch die Gruppierung eine höhere Abstraktionsebene zu erreichen und die Daten zu reduzieren (hier erfolgt eine Verdichtung in die Anforderungskategorien). Das selektive Kodieren erfordert das gezielte Nachkodieren weiterer Daten (Bohnsack et al. 2006, S. 70-75).

Obwohl die Anwendung der qualitativen Inhaltsanalyse zur Auswertung von transkribierten Interviews dominiert, kann diese allgemein zur Auswertung von Texten, Bildern und Videos herangezogen werden. Zu den auswertbaren Texten gehören Transkripte ebenso wie Zeitungsartikel und wissenschaftliche Publikationen (Atteslander 2010, S. 195-224). In der Wirtschaftsinformatik wird eine ähnliche methodische Vorgehensweise im Kontext des Konzepts der stilisierten Fakten (Houy et al. 2009; Houy et al. 2011) eingesetzt. Hierbei wird die qualitative Inhaltsanalyse als Methode zur Gewinnung von stilisierten Fakten aus wissenschaftlichen Publikationen verwendet. Ähnlich wie in diesem Kontext kann auch für die Entwicklung von Anforderungen für das strategische

GRC-Management argumentiert werden, dass der große Teil des vorhandenen Wissens in Form von publizierten Texten vorliegt. Diese Texte beinhalten sowohl Ergebnisse aus empirischen Forschungsvorhaben als auch konzeptionelle Überlegungen bspw. basierend auf aktuellen regulatorischen Vorgaben. Sie beinhalten somit konsolidierte Expertenauffassungen, die sich aus verschiedenen Quellen nähren und erscheinen daher derzeit als geeignetste Quelle zur Herleitung der Anforderungskategorien. Die Ableitung der Anforderungskategorien geschieht, ähnlich wie die Herleitung stilisierter Fakten, auf der Basis von unterschiedlichen Aussagen, die durch Abstraktion und Konsolidierung verdichtet werden. Jede Anforderungskategorie zeichnet sich durch hinlängliche Repräsentativität und inhaltliche Gemeinsamkeit aus.

Konkret wurde zur Herleitung der Anforderungskategorien an einen GRC-Management-Ansatz wie folgt vorgegangen. Nach intensiver Lektüre der relevanten Arbeiten wurden besonders relevante Textpassagen extrahiert und nach Microsoft Excel™ übernommen. Hier wurden die Textstellen sortiert und in einem ersten Schritt in Unterkategorien kategorisiert. Ergänzend hierzu wurden die Unterkategorien, nach mehrfacher Überarbeitung, in die Anforderungskategorien, die eine höhere Abstraktionsebene darstellen, zusammengeführt. Im Anhang findet sich die Aufstellung der Literaturbelege aller kodierten Textstellen mit einer Zuordnung zu den Kategorien und Unterkategorien (siehe Tab. 64 bis Tab. 68). Tab. 6 zeigt die Anforderungskategorien, Unterkategorien und die Anzahl der kodierten Textstellen je Kategorie und Unterkategorie (in Klammern). Pro Quelle und Unterkategorie wurde nur eine Textstelle kodiert. Die Anzahl der Kodierungen soll als ein Anzeichen über die Stärke der Evidenz der Anforderungen verstanden werden, kann jedoch aufgrund der methodischen Vorgehensweise nicht als exaktes Maß gedeutet werden. Es ist anzumerken, dass durch die

wörtliche Übernahme von Textstellen implizite Annahmen nicht berücksichtigt wurden. Die qualitative Inhaltsanalyse stellt in diesem Zusammenhang auch nur eingeschränkt Interpretationen bei der Kodierung der Textstellen an.

Tab. 6: Kategorien, Unterkategorien, Anzahl Kodierungen (Kod.) und relevante Theorien

Nr.	Anforderungskategorie	Unterkategorie (Anzahl Kodierungen)	Anzahl Kod.	Relevante Theorien
1	Strategische Ausrichtung	GRC als Teil des strategischen Managements (27), GRC als strategische Chance (23), „trade-off" zwischen Geschäfts- und Compliance-Zielen (3), Nutzenpotentiale (28), Orientierung an Stakeholderanforderungen (4)	85	Market-based view, Resource-based view, Stakeholdertheorie
2	Integration	Integration der GRC-Disziplinen (41), Integriertes Management über GRC-Vorgaben oder Risikobereiche (11), Integration von IT-bezogenen und unternehmensweiten Ansätzen (2), Integration in die operativen Geschäftsprozesse (4), Methodische und informationstechnische Integration (8)	66	Transaktionskostenökonomik
3	Geschäftsprozessorientierung	Bedeutung von Geschäftsprozessen für GRC (25), Integration von GPM und GRC-Management (17), Bedeutung der gesamten Enterprise Architecture (1), Bedeutung eines geschäftsprozessorientierten Ansatzes für die Automatisierung der Compliance-Sicherung (5)	48	Transaktionskostenökonomik
4	Management-Systeme	---	12	Transaktionskostenökonomik, Institutionalistische Theorie

Nr.	Anforderungskategorie	Unterkategorie (Anzahl Kodierungen)	Anzahl Kod.	Relevante Theorien
5	Automatisierung	Unterscheidung der Bedeutungsvarianten von IT (5), IT-Unterstützung des GRC-Managements (8), Automatisierung der Compliance-Sicherung (24)	37	Transaktionskostenökonomik, Prinzipal-Agenten-Theorie, Organisational Control Theorie
6	Flexibilität	Relevanz von Flexibilität (16), Trade-off zwischen Flexibilität und Compliance (1), Flexibilität durch serviceorientierte Architekturen (5), Flexibilität durch Cloud-Computing (2)	24	Prinzipal-Agenten-Theorie, Stewardship-Theorie
7	Menschliche Faktoren	Compliance-Verhalten (35), Compliance-Kultur (8), „tone at the top" (16)	59	Theorie des überlegten Handelns, Theorie des geplanten Verhaltens; General Deterrence Theorie, Technology Acceptance Model; Theorie der Schutzmotivation; Theorie der rationalen Entscheidung; Diffusionstheorie, Prinzipal-Agenten-Theorie, Stewardship-Theorie, Organisational Control Theorie

Basierend auf der Identifikation und groben Strukturierung der Theorien in die Gruppen strategisch, ökonomisch und verhaltenswissenschaftlich, konnte eine Zuordnung der Theorien zu den Anforderungskategorien erfolgen. Hierbei wurde jede Theorie aus Tab. 5 mindestens einer Anforderungskategorie zugeordnet. Das Ergebnis dieses Prozesses ist ebenfalls in Tab. 6 wiedergegeben.

Des Weiteren ist folgende Anmerkung zu beachten. Es existieren durchaus Abhängigkeiten zwischen den Anforderungskategorien bzw. Unterkategorien. Deutlich werden diese bspw. bei den Unterkategorien informationstechnische und methodische Integration der Anforde-

rungskategorie Integration, Bedeutung der Geschäftsprozesse für die Automatisierung der Compliance-Sicherung der Anforderungskategorie Geschäftsprozessorientierung und Automatisierung der Compliance-Sicherung der Anforderungskategorie Automatisierung. Obwohl alle diese Unterkategorien einen Bezug zur Automatisierung haben, werden hierbei jedoch unterschiedliche Aspekte betont, die im Nachfolgenden eine separate Analyse rechtfertigen. Auf die Beziehungen der Teilbereiche wird insbesondere im Rahmen der Darstellung der Forschungsagenda detailliert eingegangen.[46]

Im folgenden Abschnitt 3.4.2 werden die Anforderungskategorien dargestellt und die Anforderungen unter Einbeziehung der relevanten Theorien hergeleitet. Die Anforderungen ergeben sich somit sowohl aus der Auswertung der GRC-Literatur als auch aus der Analyse der vorhandenen Literaturergebnisse an Hand der zugeordneten Theorien. Die Anforderungen gehen somit über den bisherigen Stand der Literatur hinaus. Die Zuordnung der Theorien zu den Anforderungskategorien wird im Rahmen dieser Analyse genauer begründet. Zur besseren Lesbarkeit der folgenden Darstellungen werden die Literaturhinweise, die Ergebnis des Kodierungsprozesses sind, nicht direkt angegeben. Es erfolgt im Text stattdessen ein Verweis auf die entsprechende Unterkategorie in Tab. 64 bis Tab. 68, in welchen die Literaturbelege wiedergegeben sind. Zur Veranschaulichung werden weiterhin Beispiele angeführt.

[46] Siehe Abschnitt 3.6.4.

3.4.2 Darstellung und theoretische Analyse der Anforderungskategorien

3.4.2.1 Strategische Ausrichtung

Viele Veröffentlichungen im Kontext der Corporate Governance bzw. der IT-Governance, aber auch Veröffentlichungen zum Risikomanagement verorten die jeweiligen Aufgaben als Teil bzw. mit engem Bezug zum strategischen Management (siehe Literaturverweise zur Unterkategorie „GRC als Teil des strategischen Managements“ in Tab. 64 sowie Definitionen im Abschnitt 2.2). Bspw. fasst die OECD den Aufgabenbereich der Corporate Governance wie folgt zusammen: „Der Corporate-Governance-Rahmen sollte die strategische Ausrichtung des Unternehmens, die effektive Überwachung der Geschäftsführung durch den Board und die Rechenschaftspflicht des Board gegenüber dem Unternehmen und seinen Aktionären gewährleisten." (OECD 2004, S. 27). IT-Governance verfolgt weiterhin eine Ausrichtung der IT an den strategischen Geschäftszielen („Business/IT-Alignment“). Obwohl zwischen Normkonformität und den Geschäftszielen grundsätzlich ein „trade-off“ angenommen wird (siehe Literaturverweise zur Unterkategorie „„trade-off“ zwischen Geschäfts- und Compliance-Zielen“ in Tab. 64), weisen bereits einige Autoren darauf hin, dass GRC auch als eine strategische Chance aufgefasst werden kann (siehe Literaturverweise zur Unterkategorie „GRC als strategische Chance“ in Tab. 64). In diesem Zusammenhang wird oftmals beklagt, dass GRC derzeit in der Praxis überwiegend als Kostenverursacher wahrgenommen wird und die wertbringenden Eigenschaften vernachlässigt werden (Lu et al. 2007, S. 1; Lu et al. 2009, S. 245; Vicente und da Silva 2011a, S. 1). Das strategische Potential von GRC wird insbesondere auch im Kontext von integrierten GRC-Ansätzen betont (PwC 2004, S. 16; PwC 2007, S. 11; Racz et al. 2010b, S. 6; Racz et al. 2010a, S. 4; Schöler und Zink

2008, S. 21-22; Vicente und da Silva 2011a, S. 1). Neben dem strategischen Potential des GRC-Managements werden im Wesentlichen operative Nutzenpotentiale aufgeführt, die sich aus GRC ergeben können (siehe Literaturverweise zur Unterkategorie „Nutzenpotentiale“ in Tab. 64). Außerdem wird eine Ausrichtung von GRC an den Interessen der Stakeholder gefordert (siehe Literaturverweise zur Unterkategorie „Orientierung an Stakeholderanforderungen“ in Tab. 64).

Porters Modell der Wettbewerbsstrategien (Porter 1980; Porter 1985; Porter 1996) ist ebenso wie der Resource-based view (Barney 1991) eine anerkannte Basis zur Erklärung von Wettbewerbsvorteilen. Da GRC, wie dargestellt, oftmals als strategische Chance betrachtet wird und somit ein Beitrag zur Erzeugung von Wettbewerbsvorteilen vermutet wird, ist die Anwendbarkeit dieser Theorien gegeben. Diese Theorien erklären wodurch strategische Wettbewerbsvorteile geschaffen werden können, sagen jedoch wenig über die strategischen Ziele aus. Daher wird die Stakeholdertheorie (Freeman 1984; Mitroff 1983) ergänzend herangezogen, welche sich mit den strategischen Zielen eines Unternehmens auseinandersetzt. Porter betont allgemein, dass Strategien sich in den Aktivitäten eines Unternehmens widerspiegeln müssen (Porter 1996, S. 64). Anders ausgedrückt sollten also alle unternehmerischen Aktivitäten an den strategischen Zielen ausgerichtet werden um einen Wettbewerbsvorteil zu generieren. Die Anforderung der strategischen Ausrichtung zielt auf eine Unterstützung der Unternehmensziele durch das GRC-Management ab, wodurch GRC zur Schaffung von Wettbewerbsvorteilen beitragen könnte.

Krell und Matook (2008; 2009) kommen im Rahmen ihrer Untersuchung zu zwei Erkenntnissen, die hier relevant sind. Zum einen wird der hybride Charakter von Investitionen, die durch GRC induziert sind, betont. Hybrid meint hierbei, dass oftmals eine Kombination von ge-

schäftlichen und GRC-Investitionen stattfindet. GRC muss sich demzufolge zwangsläufig an geschäftlichen Anforderungen orientieren. Zum anderen wird anhand der generischen Wettbewerbsstrategien von Porter (1980; 1985) aufgezeigt, welche strategischen Ziele hierdurch intendiert werden. So ist zu vermuten, dass bei einer Preisführerschaft zusätzliche Kosten von GRC, auch wenn hierdurch ein hohes Compliance-Level bzw. eine verbesserte Risikosituation ermöglicht werden, nicht an den Kunden weitergegeben werden können. Dies liegt in der Tatsache begründet, dass sich Kunden in solchen Märkten am Preis orientieren und nicht an anderen Merkmalen des Produkts. Bei einer Differenzierungsstrategie ist die Situation jedoch eine andere. Hier kann durch einen höheren Compliance-Level, bspw. erzeugt durch die freiwillige Implementierung von Standards, dann ein Wettbewerbsvorteil erwartet werden, wenn dies die Kaufbereitschaft der Kunden beeinflusst. Somit kann zusammenfassend behauptet werden, dass ein GRC-System, das nicht zu den strategischen Zielen des Unternehmens passt, die Überlebensfähigkeit des Unternehmens gefährden kann. Daher sollte GRC an den strategischen Zielen ausgerichtet werden.

Anforderung 1: GRC sollte an den strategischen Zielen des Unternehmens ausgerichtet werden, um die Überlebensfähigkeit des Unternehmens nicht zu gefährden.

Auf Basis des Market-based views konnte zwar die Schlussfolgerung getroffen werden, dass GRC bei Nichtbeachtung der Unternehmensstrategie die Überlebensfähigkeit des Unternehmens beeinträchtigen könnte, hiermit wird jedoch noch nichts darüber ausgesagt, ob ein GRC-System, das an den strategischen Geschäftszielen ausgerichtet ist, auch zur Schaffung langfristiger Wettbewerbsvorteile beitragen kann. Zur Beantwortung dieser Frage wird nachfolgend der Resource-based

view aufgegriffen. Mossanen (2010, S. 180-184) untersucht die der Compliance zugrundliegenden Ressourcen an Hand der von Barney (1991, S. 105-112) aufgestellten Kriterien. Er kommt zu dem Schluss, dass durch Compliance kein strategischer Wettbewerbsvorteil erzielt werden kann. Obwohl GRC nur schwer handelbar sowie übertragbar ist und auch wertvoll im Sinne einer strategischen Relevanz ist, kann jedoch von einer Imitierbarkeit ausgegangen werden. Auch wenn das GRC-Management eine Vielzahl von Ressourcen kombinieren muss und die strategische Bedeutung dieser Ressourcen weitestgehend unerforscht ist, kann vermutet werden, dass in Zukunft etablierte Vorgehensmodelle, Methoden und Werkzeuge für das Management von GRC verfügbar und für Unternehmen zugänglich sein werden. Barney (1991, S. 112-114) analysiert exemplarisch den strategischen Planungsprozess und merkt hierbei an, dass dieser, selbst wenn er zur Identifikation von Gefahren und Chancen im Wettbewerbsumfeld eines Unternehmens beiträgt, nicht die Quelle für einen nachhaltigen Wettbewerbsvorteil sein kann. Der Hauptgrund hierfür liegt in der guten Dokumentation solcher Methoden in Forschung und Praxis, die für alle Unternehmen verfügbar ist. Zusammenfassend scheint GRC zwar von strategischer Relevanz zu sein, der Resource-based view legt jedoch nahe, dass hiermit keine oder bestenfalls kurzfristige Wettbewerbsvorteile verbunden sind, da Konkurrenten ebenfalls effiziente GRC-Management-Ansätze nachahmen können.[47]

---

[47] Es ist auf die Schwierigkeit einer exakten Analyse von Barneys Kriterien hinzuweisen. Diese Kriterien stellen nur ein grobes Gerüst zur Beurteilung der Ressourcen dar. Ob ein Kriterium im konkreten Fall erfüllt ist oder nicht ist anhand dieses Rasters nur schwer zu entscheiden. Barney (1991, S. 107) weist selbst auf diesen Umsatnd hin in dem er im Kontext der Seltenheit anführt: „How rare a [...] resource must be [...] is a difficult question.“. Es könnte gegebenefalls argumen-

In der Literatur wird hinsichtlich der IT/Business Value Debatte (siehe bspw. Carr 2003; Carr 2004; Goeken und Patas 2009, S. 12-13; Seddon 2005) ein etwas anderer Untersuchungsrahmen auf der Grundlage des Resource-based views verfolgt. Hierbei wird in einem ersten Schritt ein Einfluss der IT-Ressourcen auf die Geschäftsprozesse angenommen. Verbesserungen in den Geschäftsprozessen gehen mit operativen Effizienzsteigerungen einher. Die Frage, ob sich diese operativen Verbesserungen auch in finanziellen Messgrößen und letztlich in einen strategischen Wettbewerbsvorteil niederschlagen, wird also separiert (Melville et al. 2004). In der Literatur wird GRC mit einer Vielzahl von potentiellen Nutzeneffekten in Verbindung gebracht, welche unter anderem die Möglichkeit von Prozessverbesserungen oder eine verbesserte Informationsversorgung von Entscheidungsträgern nahelegen. Diese Überlegungen zusammenfassend wird folgende Anforderung aufgestellt.

Anforderung 2: Die das GRC-Management konstituierenden Ressourcen sollten die Erzielung operativer Nutzenpotentiale ermöglichen.[48]

Um die Frage zu prüfen, ob das GRC-Management an den Interessen der Stakeholder ausgerichtet werden sollte, ist das Ziel des GRC-Managements zu bestimmen. In der Literatur sind mit dem Shareholder- und dem Stakeholder-Ansatz zwei mögliche Zielsetzungen zu unterscheiden. Ziel des Shareholder-Ansatzes ist die Maximierung des

---

tiert werden, dass kulturelle Aspekte, denen im Kontext von GRC eine hohe Bedeutung zugestanden wird, nur schwer imitierbar sind.

48 Die Anforderung enthielt ursprünglich den folgenden zusätzlichen Satz: „Die Erzielung dauerhafter Wettbewerbsvorteile durch überlegenes GRC-Management ist dagegen zumindest schwierig." Dieser ist auch in die Delphi-Studie (siehe Abschnitt 4) eingegangen. Dieser Zusatz stellt jedoch keine Anforderung im Sinne der eingeführten Definition dar und wurde daher nachträglich entfernt.

Shareholder-Values oder Unternehmenswertes, der auf Basis diskontierter zukünftiger Zahlungsströme (engl. Cashflows) ermittelt wird. Die Richtlinien der Corporate Governance, sowie regulatorische Vorgaben und Risikomanagement-Rahmenwerke (siehe bspw. COSO 2004) stellen zweifelsfrei die Interessen der Shareholder in den Mittelpunkt. Hierbei wird jedoch nicht unmittelbar die Maximierung des Shareholder-Values verfolgt, sondern Kontroll- und Offenlegungspflichten, die zur Lösung der Agenturproblematik beitragen sollen. Erweitert man die Betrachtungsweise auf alle Stakeholder, so werden unterschiedliche Interessen offenkundig. Diese sind teilweise in GRC-Vorgaben kodifiziert und erstrecken sich bspw. auf die Bereiche Datenschutz, Produktsicherheit oder Umweltschutz. Im GRC-Management stellt sich somit die Frage, zu welchem Grad die Interessen der jeweiligen Stakeholder erfüllt werden sollen. Dies kann bedeuten, dass lediglich die gesetzlichen Mindestanforderungen erfüllt werden sollen, oder dass sogar eine Übererfüllung gesetzlicher Vorgaben im Rahmen der Implementierung von Best Practices und Standards angestrebt wird. Auch das Risikomanagement muss von der Unternehmensstrategie und somit letztlich von den Stakeholderinteressen aus betrachtet werden, um die Aufmerksamkeit auf die wesentlichen Risikobereiche zu lenken. Ein Kernaspekt des Stakeholder-Ansatzes, wie er auch in der weiten Definition von Corporate Governance aufgegriffen wird, ist die Maximierung des kumulierten Nutzens aller Stakeholder. Dies erfordert insbesondere die Berücksichtigung von Zielkonflikten zwischen den Stakeholdern. Im Shareholder-Ansatz ist der spezifische Grad der Erfüllung der Stakeholderinteressen (Umweltschutz, Datenschutz usw.) also allein am Shareholder-Value auszurichten, wohingegen der Stakeholder-Ansatz einen Interessensausgleich anstrebt. Wie die Ausführungen zeigen, nimmt GRC durch die unterschiedlichen Bereiche der GRC-Vorgaben inhärent eine Stakeholder-Perspektive ein, wobei sich

lediglich die Frage stellt, ob sich die Stakeholderinteressen letztlich vollständig der Shareholder-Value-Maximierung unterzuordnen haben. Wird der Shareholder-Value nicht in der kurzfristigen Maximierung der Marktkapitalisierung (im Sinne des Aktienpreises) gesehen, kann der Konflikt zwischen den beiden Ansätzen aufgelöst werden. Einige Autoren (Albach 2001; Danielson et al. 2008) argumentieren, dass der Shareholder-Value aufgrund der Berücksichtigung aller zukünftigen Zahlungsströme inhärent langfristig ausgerichtet ist. Dies bedeutet, dass durch die Maximierung des Shareholder-Values langfristig auch die Interessen der Stakeholder bestmöglich erfüllt werden.

Anforderung 3: GRC sollte an den Stakeholderinteressen ausgerichtet werden. Die Stakeholderinteressen sollten hierbei unter der Prämisse der langfristigen Maximierung des Unternehmenswertes ausbalanciert werden.

3.4.2.2 Integration

Die Integration von GRC wird in der Literatur unter inhaltlichen (siehe Literaturverweise zur Unterkategorie „Integration der GRC-Disziplinen“ und zur Unterkategorie „Integriertes Management über GRC-Vorgaben oder Risikobereiche“ in Tab. 65) und methodischen bzw. informationstechnischen Aspekten (siehe Literaturverweise zur Unterkategorie „Methodische und informationstechnische Integration“ in Tab. 65) diskutiert. Außerdem wird eine Integration der GRC-Aktivitäten in die operativen Geschäftsprozesse gefordert (siehe Literaturverweise zur Unterkategorie „Integration in die operativen Geschäftsprozesse“ in Tab. 65) sowie die Integration von informationstechnischen und unternehmensweiten Ansätzen diskutiert (siehe Literaturverweise zur Unterkategorie „Integration und IT-bezogenen und unternehmensweiten Ansätzen“ in Tab. 65). Die inhaltlichen Aspekte der Integration können in die Forderung eines integrierten Manage-

ments über mehrere GRC-Vorgaben und Risikobereiche (siehe Literaturverweise zur Unterkategorie „Integriertes Management über GRC-Vorgaben oder Risikobereiche“ in Tab. 65) sowie die Forderung der Integration der GRC-Teildisziplinen (siehe Literaturverweise zur Unterkategorie „Integration der GRC-Disziplinen“ in Tab. 65) unterteilt werden.

Die Forderung eines integrierten Managements von GRC wurde bereits vielfach in Wissenschaft und Praxis aufgestellt. Beispielhaft seien Klotz und Dorn (2008) hervorgehoben, welche aufgrund der inhaltlichen Zusammenhänge „eine integrierte Strategie und ein gemeinsames Management“ fordern (Klotz und Dorn 2008, S. 7). In der Literatur (De Haes und Van Grembergen 2006, S. 7; De Haes und Van Grembergen 2008a, S. 447; De Haes und Van Grembergen 2008b, S. 5; De Haes und Van Grembergen 2009, S. 128) wird Compliance, bspw. konkret manifestiert durch den SOX, außerdem als eine Art Treiber für die Governance bzw. das Risikomanagement angesehen, da Risikomanagement bzw. ein internes Kontrollsystem regulatorisch erforderlich ist. Hiermit ist jedoch noch keine konkrete Forderung nach einer Integration der Teildisziplinen von GRC verbunden.

Die Forderung der Integration von GRC liegt, wenn auch überwiegend implizit, in der Auffassung begründet, dass hierdurch eine überlegene Koordinationsform geschaffen werden kann. Theoretisch kann diese Anforderung daher aus der Perspektive der Transaktionskostenökonomik betrachtet werden. Die Transaktionskostenökonomik ist in der Lage verschiedene Managemententscheidungen zu unterstützen. Insbesondere ist sie in der Lage die Auswahl eines effizienten Koordinationsmechanismus für Transaktionen zu unterstützen (Jost 2001, S. 11). Es ist anzumerken, dass ebenfalls die institutionelle Theorie sowie die Kontingenztheorie einen Erklärungsbeitrag zur Anforderungskategorie

„Integration“ leisten könnten. Die Anforderungen betrachten jedoch weniger die Frage, welche Einflussfaktoren die tatsächliche Ausgestaltung von GRC-Management-Systemen beeinflussen, sondern welche Anforderungen bei der Errichtung und Weiterentwicklung von GRC-bezogenen Management-Ansätzen berücksichtigt werden sollten. Es wird somit ein normativer anstelle eines deskriptiven Standpunkts eingenommen. Hierfür ist die Transaktionskostenökonomik geeignet, da diese als ökonomische Theorie Effizienz- und Effektivitätskriterien verfolgt. Die institutionalistische Theorie legt nahe, dass neben diesen Kriterien auch weitere Einflüsse auf reale GRC-Systeme existieren. Diese müssen nicht zwangsläufig einem wirtschaftlichen Kalkül folgen. Die Kontingenztheorie legt zudem nahe, dass in unterschiedlichen Situationen auch unterschiedliche Koordinationsformen überlegen sein können. An dieser Stelle werden jedoch lediglich allgemeine Anforderungen formuliert, die unternehmensspezifisch anzupassen und zu verfeinern sind.

Um an den theoretischen Untersuchungen von Pupke (2008, S. 54-80) ansetzen zu können, soll hier ebenfalls die Vorgehensweise von Picot (1982, S. 273) aufgegriffen werden. Diese gliedert sich in die folgenden Schritte: (1) die Eigenschaften der Transaktionen (hier verstanden als Prozessschritte), die für das GRC-Management erforderlich sind, müssen identifiziert werden; (2) die denkbaren Koordinationsformen sind zu ermitteln und (3) für jede Transaktion ist die Koordinationsform mit minimalen Transaktionskosten auszuwählen.

Zu (1): Die Definition der Transaktionen, die das GRC-Management ausmachen ist derzeit schwierig, da noch kein etablierter Management-Ansatz vorliegt, der eine Beschreibung der Aktivitäten in Form eines integrierten Prozessmodells beinhaltet. Aus diesem Grund wird für die vorliegende Untersuchung eine grobe Unterscheidung in Management-

Aktivitäten sowie operative Normerfüllung und Risikosteuerung vorgenommen. Management kann nach Fayol (1949, S. 3) in die Aktivitäten Planung, Organisation, Führung, Koordination und Kontrolle unterteilt werden. Die operative Normerfüllung und Risikosteuerung beinhaltet die Umsetzung einzelner GRC-Vorgaben und die Ausführung der hierdurch induzierten Maßnahmen sowie die Durchführung der risikosteuernden Maßnahmen. Die Identifikation und Analyse der GRC-Vorgaben und Risiken werden als Management-Aufgabe verstanden. Wie bereits erläutert wurde, ist es Aufgabe der Corporate Governance einen Rahmen für das Compliance- und Risikomanagement zur Verfügung zu stellen. Corporate Governance ist für diese Analyse somit vornehmlich als Management-Aufgabe zu verstehen bzw. dem Management sogar übergeordnet (Racz et al. 2010c, S. 11). Diese Unterscheidung ist in Übereinstimmung mit existierenden Ansätzen. So unterscheidet Pupke (2008, S. 71) die Phasen „Implementation“ und „Sustainment“ im Compliance-Management. Die Phase „Implementation“ enthält hierbei die erstmalige Umsetzung von Compliance-Vorgaben und ist somit als Management-Aktivität zu verstehen. Die Sustainment-Phase stellt die Normkonformität im Regelbetrieb sicher, was den operativen Aufgaben entspricht. Im Prozessmodell für GRC von Racz et al. (2010c, S. 12) lassen sich ebenfalls Management-Aktivitäten (Identifikation und Analyse von Risiken und Compliance-Vorgaben, Monitoring, Kommunikation) von der operativen Normerfüllung und Durchführung der Risikomaßnahmen abgrenzen.

Die Untersuchung der Eigenschaften der Transaktionen orientiert sich an der entsprechenden Analyse von Pupke (2008, S. 72-75) für das Compliance-Management. Außerdem wird die Unterscheidung in Management-Aktivitäten und operative Compliance-Sicherung und Risi-

kosteuerung aufgegriffen. Tab. 7 fasst die Ergebnisse der Analyse für die relevanten Eigenschaften zusammen.

Tab. 7: Analyse der Eigenschaften zu den GRC-Transaktionen

Eigenschaft	Management-Aktivitäten		Operative Normerfüllung und Risikosteuerung	
Transaktions-spezifität	Hoch	Für jede Risikoart und GRC-Vorgabe ist spezifisches Wissen erforderlich und es existiert Umsetzungs-spielraum.	Nied-rig	Es existieren klare Regeln, die jeweils für einzelne Ge-schäftsprozesse die Normerfüllung und Risikosteuerung festlegen.
Unsicherheit	Hoch	Unternehmen sind stetig mit neuen und veränderten Nor-men und Umwelt-bedingungen kon-frontiert.	Nied-rig	Die gegenwärtig gültigen Regeln sind klar definiert. Ände-rungen werden in die Vorgabedokumente integriert und kom-muniziert.
Häufigkeit	Nied-rig	Management-Aktivitäten werden überwiegend zyk-lisch (bspw. jährlich) ausgeführt.	Hoch	Die operativen Akti-vitäten sind inhären-ter Bestandteil jeder Geschäftsprozess-ausführung.
Effiziente Ko-ordina-tionsform	Zentral		Hybrid	

Zu (2) und (3): Um die Transaktionsform, welche die Kosten minimiert, identifizieren zu können, sind zuerst die denkbaren Koordinationsformen zu definieren. Pupke (2008, S. 75-80) unterscheidet hierbei zwei Ebenen. Die erste Ebene beschreibt die Koordinationsformen für die Umsetzung einer einzelnen Compliance-Vorgabe bzw. eines einzelnen Risikobereichs, welche somit zur Untersuchung der Forderung nach einer operativen Integration sowie der methodischen und informationstechnischen Integration herangezogen werden können. Hierbei existieren in Anlehnung an Horvath (2003, S. 77) und Schierenbeck

(2003, S. 127) die zentrale, duale und hybride Koordination als mögliche Koordinationsformen. Die zentrale Koordinationsform bedeutet, dass eine organisatorische Einheit für GRC verantwortlich ist. Dies bedeutet auch, dass die Managementprozesse sowie Methoden und Werkzeuge zentralisiert sind. Im dualen Ansatz werden für GRC Organisationseinheiten der Sekundärorganisation wie bspw. Projektorganisationen einschließlich entsprechender Prozesse, Methoden und Werkzeuge geschaffen. Der hybride Ansatz integriert GRC direkt in die Primärorganisation. Jede der angesprochenen Koordinationsformen hat Vor- und Nachteile. In einer zentralen Organisationseinheit kann spezifisches Wissen für GRC aufgebaut und Entscheidungsprozesse beschleunigt werden. Hierdurch werden jedoch die Geschäftsanforderungen nicht einbezogen. Die duale Form nutzt teilweise Ressourcen der Primärorganisation und kann auch Wissen der Geschäftsanforderungen integrieren, ermöglicht jedoch nicht in gleicher Weise wie bei der zentralen Koordinationsform den Aufbau von spezifischem Wissen. Der hybride Ansatz nutzt vollständig die Ressourcen und organisatorischen Rahmenbedingungen der Primärorganisation. Der Aufbau von spezialisiertem GRC-Wissen gestaltet sich jedoch besonders schwierig. Bezogen auf die Eigenschaften der Transaktion ergeben sich als effiziente Koordinationsformen der zentrale Ansatz für die Management-Aktivitäten und der hybride Ansatz für die operative Normerfüllung und Risikosteuerung (siehe Tab. 7).[49]

[49] Es sei darauf hingewiesen, dass im Kontext der IT-Governance eine ähnliche Debatte geführt wird, die sich mit den „Governance Mechanismen" der IT-Funktion auseinandersetzt. In diesem Zusammenhang wird bspw. eine Unterscheidung in eine zentrale, hybride/federale und dezentrale Organisation getroffen (Brown und Magill 1994; Ein-Dor und Segev 1982; Olson und Chervany 1980; Sambamurthy und Zmud 1999; Zmud 1984). Weill entwickelt diese grundsätzlichen Gover-

Die zweite Ebene unterscheidet Koordinationsformen für das Management mehrerer GRC-Vorgaben bzw. Risikobereiche. Pupke (2008, S. 75-80) unterscheidet hierbei einen integrierten und einen nicht integrierten Ansatz. Diese Ebene korrespondiert mit der Forderung der Integration über GRC-Vorgaben und Risikobereiche. Im Kontext des Gegenstandbereichs dieser Untersuchung wird eine weitere Ebene relevant, welche die Integration der GRC-Disziplinen erfasst. Hierbei ist wiederum ein integrierter und ein nicht integrierter Ansatz denkbar. Erweitert man die Koordinationsformen für das Compliance-Management nach Pupke um die Ebene der Integration der GRC-Disziplinen, ergibt sich das in Tab. 8 dargestellte Bild.

Tab. 8: Mögliche Koordinationsformen des GRC-Managements

	GRC-Vorgaben und Risikobereiche		GRC-Disziplinen	
	Nicht integriert	Integriert	Nicht Integriert	Integriert
Zentral	Es existiert eine zentrale Organisationseinheit je Vorgabe bzw. Risikobereich. Vorgaben werden einzeln umgesetzt.	Es existiert eine zentrale Organisationseinheit und eine Integration über Vorgaben und Risikobereiche.	Es existiert eine zentrale Organisationseinheit für Management- bzw. operative Aktivitäten. Dies ist aber getrennt nach GRC-Disziplinen.	Es existiert eine zentrale Organisationseinheit für Koordination und operative Aktivitäten für alle GRC-Disziplinen.

nance Mechanismen der IT in sechs sogenannte Archetypen weiter. Diese sind „business monarchy", „IT monarchy", „feudal", „federal", „duopoly", und „anarchy" (Weill 2004). Es handelt sich hierbei, wie erwähnt, um Gestaltungsmöglichkeiten für die IT-Funktion und nicht für die IT-Governance selbst.

	GRC-Vorgaben und Risikobereiche		GRC-Disziplinen	
	Nicht integriert	Integriert	Nicht Integriert	Integriert
Dual	Es existiert eine sekundäre Organisations-form für Management- bzw. operative Aktivitäten je Vorgabe und Risikobereich.	Es existiert eine sekundäre Organisationseinheit für Management- bzw. operative Aktivitäten integriert über mehrere GRC-Vorgaben bzw. Risikobereiche.	Es existiert eine sekundäre Organisationseinheit für Management- bzw. operative Aktivitäten je GRC-Disziplin.	Es existiert eine sekundäre Organisationseinheit für Management- bzw. operative Aktivitäten integriert über die GRC-Disziplinen.
Hybrid	Die Management- bzw. operativen Aktivitäten sind in die operativen Geschäftsprozesse integriert aber es existiert keine Verbindung zwischen den Vorgaben bzw. Risikobereichen.	Die Management- bzw. operativen Aktivitäten sind in die operativen Geschäftsprozesse integriert. Außerdem besteht eine Verbindung zwischen den Vorgaben bzw. Risikobereichen.	Die Management- bzw. operativen Aktivitäten sind in die operativen Geschäftsprozesse integriert, wobei keine Verbindung zwischen den Teildisziplinen existiert.	Die Management- bzw. operativen Aktivitäten sind in die operativen Geschäftsprozesse integriert. Außerdem besteht eine Verbindung zwischen den GRC-Teildisziplinen.

Pupke (2008, S. 75-80) hat bereits die integrierte Erfüllung der GRC-Vorgaben als vorteilhaft herausgearbeitet. Diese basiert auf der großen inhaltlichen Nähe der GRC-Vorgaben, durch die Synergieeffekte bei einer Integration realisiert werden können. Zudem zeigen sich methodische Schwächen in siloartigen (nicht integrierten) Ansätzen, die zwar eine adäquate Umsetzung einzelner regulatorischer Vorgaben erlauben, jedoch einen Gesamtüberblick bzgl. des Compliance-Status bzw. der Risikosituation unmöglich machen. Im Risikomanagement beschreibt der Begriff des „Enterprise Risk Management" einen ganzheitlichen Ansatz, der zu einer adäquaten Sicht auf alle Risiken eines Unternehmens beitragen soll (Barateiro et al. 2012, S. 1-2; Oh et al. 2007, S. 420; Hardy und Leonard 2011, S. 795; Zoet et al. 2011, S. 456). Ein nicht integrierter Ansatz kann sowohl zu Lücken bei der Umsetzung als auch zu Doppelarbeiten führen. Auch kann die Governance nur dann ihre

Aufgabe der Unterstützung strategischer Entscheidungen erfüllen, wenn hierfür aus dem Risiko- und Compliance-Management geeignete Informationen zur Verfügung stehen. Sind die Informationen nur silo-artig vorhanden, ist eine adäquate Entscheidungsunterstützung nur eingeschränkt möglich. In der Literatur lassen sich zudem die folgenden Argumente finden.

Allgemeine Vorteile

- Gesamtüberblick bzgl. des Compliance-Status bzw. der Risikosituation
- Verhinderung von Lücken und Doppelarbeiten
- Verbesserte Informationsversorgung für Entscheidungsträger
- Synergien aufgrund allgemeiner Überschneidungen:
- Allgemeine Anforderungen an Vorgabedokumente (bspw. Arbeitsanweisungen), Dokumentationsstandards, Durchführung von Reviews und Audits,
- Einhaltung von Aufbewahrungspflichten (Böhm 2008, S. 23),
- Sicherung des Datenzugriffs (Böhm 2008, S. 23)

Synergien zwischen spezifischen Vorgaben:

- Synergien zwischen Vorgaben in einer Domäne (bspw. SOX und Basel II zur Finanzberichterstattung (Pupke 2008, S. 75), ISO 9001 und Good Manufacturing Practice (GMP) im Qualitätsmanagement),
- Synergien zwischen unternehmensweiten und IT-

bezogenen Vorgaben, bspw. Kontrollen aus SOX und ISO 27001/2

- Überlappung von Vorgaben auf nationaler und internationaler Ebene (Abdullah et al. 2010a) (bspw. SOX und KonTraG)

Abb. 7: Vorteile einer integrierten Erfüllung von GRC-Vorgaben

Die Integration der GRC-Teildisziplinen wird von Pupke (2008) nicht analysiert. Aus der Analyse der Beziehungen von GRC ergeben sich folgende Gründe für eine Integration der GRC-Disziplinen.

- Zusammenhänge bei der Identifikation und Analyse der Compliance-Vorgaben und Risiken sowie Zusammenhänge bei der operativen Compliance-Sicherung und Risikosteuerung (bspw. Zusammenhänge zwischen Risikomanagement und Compliance-Kontrollen in Kontrollmodellen wie COSO (2004) bzw. im IT-Bereich COBIT (ITGI 2007), ITIL (OGC 2007a; OGC 2007b) und ISO 27001/2 (DIN 2008a))
- Non-Compliance als bedeutsame Risikokategorie (Withus 2010, S. 100).
- Governance als Rahmen für Risiko- und Compliance-Management (Racz et al. 2010c, S. 11-12)

Abb. 8: Vorteile einer Integration der GRC-Teildisziplinen

Die vorangegangenen Analysen lassen sich in den folgenden Anforderungen zusammenfassen.

Anforderung 4: Die für GRC relevanten Management-Aktivitäten sollten einem zentralen Ansatz folgen. Die operativen Aktivitäten sind in die Kernprozesse und operativen IT-Systeme zu integrieren.

Anforderung 5: Zur Nutzung von Synergien und Verhinderung von Doppelarbeiten bzw. Lücken sollten GRC-Aktivitäten über verschiedene Bereiche (bspw. Compliance-Vorgaben) als auch über die GRC-Disziplinen integriert werden.

3.4.2.3 Geschäftsprozessorientierung

Ein geschäftsprozessorientierter Ansatz wird in der Literatur aufgrund des direkten Zusammenhangs der Geschäftsprozesse mit dem ökonomischen Ergebnis eines Unternehmens sowie den GRC-Vorgaben und Risiken gefordert (siehe Literaturverweise zur Unterkategorie „Bedeutung von Geschäftsprozessen für GRC" in Tab. 66). Besonders hervorgehoben wird außerdem die Bedeutung eines geschäftsprozessorientierten Ansatzes für die Automatisierung der Compliance-Sicherung (siehe Literaturverweise zur Unterkategorie „Bedeutung eines geschäftsprozessorientierten Ansatzes für die Automatisierung der Compliance-Sicherung" in Tab. 66). Insgesamt wird hierauf aufbauend auch eine Integration von GRC-Management und GPM gefordert, da sich diese beiden Managementkonzepte gegenseitig ergänzen (siehe Literaturverweise zur Unterkategorie „Integration von GPM und GRC-Management" in Tab. 66). Bspw. wird angeführt, dass Geschäftsprozessmodelle zur Identifikation von Risiken bzw. GRC-relevanten Bereichen herangezogen werden können. Außerdem können diese zur Kommunikation von Risiken und Maßnahmen sowie zur Dokumentation für interne und externe Revisionen dienen (Rieke und Winkelmann 2008, S. 347). Erweitert wird diese Sichtweise zudem auf das Enterprise

Architecture Management[50], das für GRC als relevant erachtet wird (siehe Literaturverweise zur Unterkategorie „Bedeutung der gesamten Enterprise Architecture“ in Tab. 66) und wozu insbesondere die Architektur der Informationssysteme und Daten gehört.

Ein Prozess bzw. Geschäftsprozess kann nach Scheer (1998, S. 3) als „eine zusammenhängende Abfolge von Unternehmensverrichtungen zum Zweck einer Leistungserstellung“ verstanden werden. Das GPM nimmt eine ablauforientierte Sichtweise des Unternehmens ein, die auf Nordsieck (1934) und Kosiol (1976) zurückgeführt werden kann. Für das GPM existieren etablierte Vorgehensmodelle (siehe z.B. Allweyer 2005; Becker et al. 2005; Schmelzer und Sesselmann 2013), Methoden (siehe z.B. Ferstl und Sinz 1995; Österle 1995; Keller et al. 1992) und Werkzeuge wie das ARIS Toolset. Geschäftsprozessorientierte Ansätze haben sich in vielen Anwendungsgebieten, wie der Einführung von ERP-Systemen oder dem Qualitätsmanagement, durchgesetzt (Becker et al. 2009, S. 6-17). Betrachtet man das GPM aus der Perspektive der Transaktionskostentheorie, kann als ein wesentliches Ziel des GPM die Senkung von Transaktionskosten genannt werden, die auf der Verbesserung der betrieblichen Abläufe basieren. Aufgrund des Reifegrades und der Verbreitung von Vorgehensmodellen, Methoden und Werkzeugen des GPM, wird zusammenfassend die folgende Anforderung formuliert.

---

[50] Gemäß dem IEEE Standard (IEEE 2000; ISO 2007) kann der Begriff Architektur als „the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution" definiert werden. Der Begriff Enterprise Architecture wird hierauf aufbauend als „fundamental organization of an enterprise embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution” definiert (Stelzer 2010, S. 2). Zur

Anforderung 6: Eine ablauforientierte Sicht sowie Vorgehensmodelle, Methoden und Werkzeuge des Geschäftsprozessmanagements sollten zur Senkung von Transaktionskosten im GRC-Bereich adaptiert werden.

3.4.2.4 Management-Systeme

In der Literatur wird eine Harmonisierung von GRC mit weiteren Management-Systemen gefordert (siehe Literaturverweise zur Anforderungskategorie „Management-Systeme" in Tab. 66). Grundsätzlich existieren im Kontext von GRC Management-Systeme, die unter GRC zu subsumieren sind (bspw. Interne Revision, Datenschutz, Qualitätsmanagement) und sonstige, die im Kontext von GRC relevant sind (bspw. Controlling, IT-Management) (Bhimani 2009; Klotz 2009, S. 13-16).

Konkret weisen einige Autoren auf den Zusammenhang von GRC und Controlling hin (Bhimani 2009, S. 2, Isensee 2008, S. 161, von Werder und Grundei 2006, S. 19-20) oder betonen den Beitrag der Internen Revision für die IT-Compliance (Lohre 2009). Im Kontext von GRC ist zudem insbesondere das gleichzeitige Zusammenspiel verschiedener Beteiligter oder Management-Systeme bedeutsam. Braganza und Franken (2007) untersuchen in diesem Zusammenhang die Beziehungen zwischen dem Chief Information Officer (CIO), dem Chief Financial Officer (CFO), dem Chief Executive Officer (CEO) und dem Auditor aus dem Blickwinkel der Einflussnahme des CIO. Maheshwari et al. (2009) gehen auf die Beziehung von CIO und CFO bei der Implementierung von Kontrollen ein. Klotz (Klotz 2009, S. 13-16) beschreibt die

---

Enterprise Architecture gehören somit neben den Geschäftsprozessen und der Organisationsstruktur bspw. auch die Ziele und die Informationssysteme.

Beteiligten und Interessengruppen im Kontext der IT-Compliance. Neben der IT-Abteilung sowie den an IT-Compliance beteiligten Fachabteilungen wird die Rechtsabteilung, der Datenschutzbeauftragte, das IT-Risikomanagement sowie die IT-Revision, das Controlling, der Einkauf und externe Wirtschaftsprüfer angeführt. Diese Einschätzung wird auch in weiteren Arbeiten geteilt, wobei schwerpunktmäßig die Bedeutung von internen und externen Aufsichtsorganen, also bspw. interne Revision und Wirtschaftsprüfern, sowohl für allgemeine als auch IT-bezogene Fragestellungen betont werden (Caron et al. 2013, S. 7; Chang et al. 2013, S. 2; Grünninger und Jantz 2013, S. 135; Leon et al. 2012, S. 453; van der Veen et al. 2011, S. 270).

Die angeführten Literaturbelege zeigen, dass GRC im Kontext mehrerer Management-Systeme relevant ist. Hierbei stellt sich die Frage, wie die Aufgaben abgestimmt und koordiniert werden können, was wiederum die Anwendbarkeit der Transaktionskostentheorie begründet. Grundsätzlich ist festzustellen, dass durch die Abstimmung und Koordination der Management-Systeme Transaktionskosten entstehen. Die genannten Management-Systeme können jedoch aus verschiedenen Gründen nicht in das GRC-Management integriert werden. Zum einen erfordern diese Aufgaben eigene fachliche Fähigkeiten und sind aus Komplexitätsgründen nur schwer zusammenzufassen. Außerdem sind institutionelle Überlegungen anzuführen. Unternehmen versuchen demnach den Anforderungen unterschiedlicher Gruppen gerecht zu werden. Da die Umsetzung dieser Anforderungen häufig lediglich symbolisch stattfindet (siehe im Kontext von Compliance MacLean und Behnam 2010 bzw. im Kontext des Risikomanagements Wiesche et al. 2013), liegt die Implementierung separater Management-Systeme wie bspw. für Umweltschutz, Datensicherheit usw. nahe. Weitere für GRC-relevante Aufgabenbereiche wie das Qualitätsmanagement oder die

interne Revision verlangen aufgrund ihrer Aufgabenstellung eigenständige Organisationseinheiten (DIN 2008b; IIA 2009). Es ist daher zu erwarten, dass weiter für Teilaufgaben von GRC eigenständige Organisationseinheiten erhalten bleiben. Dies erfordert geeignete Vorgehensweisen, Methoden und Werkzeuge für die Abstimmung dieser Management-Systeme mit GRC. Folgende Anforderung fasst diese Analyse zusammen.

Anforderung 7: Zur Harmonisierung der Management-Systeme im Kontext von GRC sollten geeignete Vorgehensweisen, Methoden und Werkzeuge entwickelt werden.

3.4.2.5 Automatisierung

Die IT kann sowohl als Gegenstand als auch als Unterstützer von GRC angesehen werden (siehe Literaturverweise zur Unterkategorie „Unterscheidung der Bedeutungsvarianten von IT“ in Tab. 67), wobei ein GRC-Management-Ansatz beide Perspektiven berücksichtigen sollte. Aus Sicht der IT als Unterstützer von GRC ist die Forderung der Automatisierung der Compliance-Sicherung und Risikosteuerung relevant (siehe Literaturverweise zur Unterkategorie „Automatisierung der Compliance-Sicherung“ in Tab. 67). Außerdem wird eine IT-seitige Unterstützung der Management-Aufgaben von GRC gefordert (siehe Literaturverweise zur Unterkategorie „IT-Unterstützung des GRC-Managements“ in Tab. 67). Die Automatisierung der Compliance-Sicherung, wird als ein zentrales Mittel zur Reduzierung des manuellen Aufwandes bspw. bei der Durchführung von internen Kontrollen angesehen (Awad et al. 2008, S. 1; Cannon und Byers 2006, S. 33-34; Sackmann 2008c, S. 39; Schultz 2013, S. 123; Turetken et al. 2012, S. 29) und soll außerdem die Wahrscheinlichkeit menschlicher Fehler senken. Des Weiteren wird argumentiert, dass die Compliance-Sicherung und

Risikosteuerung durch Automatisierung „beschleunigt, reproduzierbar und nachvollziehbar“ (Kranawetter 2009, Prologue) wird. Eine Voraussetzung hierfür ist eine gewisse Standardisierung der Kontrollen sowie deren Formalisierung (El Kharbili und Pulvermüller 2009, S. 61; Menzies et al. 2008, S. 141; Pohlman 2008, S. 41).

Des Weiteren wurde die IT bereits im Rahmen der Analyse der Integration von GRC berücksichtigt. Hierbei wurde analysiert, ob eine Integration der für GRC relevanten Informationssysteme sinnvoll ist. Zur Analyse der Automatisierung ist zum einen die Transaktionskostentheorie relevant, da die IT einen Einfluss auf die Transaktionskosten hat (Picot 1982, S. 271-273). Bei der operativen Compliance-Sicherung und Risikosteuerung sind die Gesamtkosten im Sinne von Produktionskosten und Transaktionskosten relevant (Jost 2001, S. 18-22). Als Produktionskosten können im Kontext von GRC die Kosten für die operative Ausführung der GRC-Kontrollen verstanden werden. Die Automatisierung kann zum einen zur Senkung dieser Produktionskosten beitragen, da die Kosten der automatisierten Ausführung wohl geringer als die hohen Arbeitskosten bei einer manuellen Ausführung sind. Dies gilt insbesondere für Kontrollen, die stark repetitiv sind und daher die Implementierungskosten der Kontrollen in IT nur geringen Einfluss auf die Gesamtkosten haben. Des Weiteren können jedoch auch Transaktionskosten eingespart werden. Zum einen sind hierbei die Effekte, die durch Qualitätsverbesserung der Kontrollen bspw. durch Vermeidung menschlicher Fehler entstehen, zu nennen. Zum anderen ermöglicht der IT-Einsatz neue Koordinationsformen für GRC. So können den beteiligten Mitarbeitern relevante Informationen bedarfsgerecht zur Verfügung gestellt werden, wobei ein signifikanter Effekt auf Abstimmungs- und Informationssuchkosten zu erwarten ist. Die Automatisierung kann somit auch die Rolle eines Enablers für das gesamte GRC-

Management einnehmen. Die Forderung der Integration der IT-bezogenen Vorarbeiten in eine ganzheitliche GRC-Management-Konzeption, wird zusätzlich dadurch gestützt, dass der Wertbeitrag von IT langfristig signifikant steigt, wenn ihr Einsatz durch geeignete Organisationskonzepte wie das GPM komplementär unterstützt wird (Brynjolfsson und Hitt 2003; Tallon et al. 2000). Dies bedeutet, dass insbesondere der intelligente Einsatz der Automatisierung entscheidend ist.

Zum anderen sind die Prinzipal-Agenten-Theorie im Allgemeinen und die Kontrolltheorie im Speziellen relevant, da diese eine Grundlage für die Analyse bietet, welche Kontrolltypen eine Automatisierung ermöglichen. Die Automatisierung der Compliance-Sicherung ist ein vielbeachteter Forschungsbereich (El Kharbili et al. 2008a, Rinderle-Ma et al. 2008). Die Automatisierungsmethoden lassen sich in die Ansätze „compliance by design" und „compliance by detection" gliedern. Ersterer ist dem prozessorientieren Kontrollansatz zuzuordnen und beinhaltet einen präventiven Ansatz, in welchem Fehlverhalten technisch nicht möglich ist (Sackmann 2008c, S. 43; Sadiq et al. 2007).[51] „Compliance by detection" ist dem ergebnisorientierten Kontrollansatz zuzuordnen und stellt somit einen reaktiven Ansatz dar, der Fehlverhalten durch Kontrollen nachträglich identifiziert (Agrawal et al. 2006). Es wird deutlich, dass die Automatisierung lediglich einige, der von Lange (2008, S. 711) angeführten Kontrolltypen abdeckt. So können informelle Kontrollen, welche durch Werte und Normen wirken nicht automatisiert und bestenfalls durch geeignete IT unterstützt werden. Für Anreizsys-

[51] Eine detaillierte Darstellung der Automatisierungsmethoden findet in Abschnitt 3.5.7.2 statt in welchem der Forschungsstand zur Anforderungskategorie „Automatisierung" aufgearbeitet wird. Die angeführten Literaturbelege stellen lediglich Beispiele dar.

teme erscheint eine Automatisierung der Aufdeckung von Fehlverhalten geradezu notwendig (Sackmann 2008c, S. 44), da für ihre Wirksamkeit eine hohe Aufdeckungswahrscheinlichkeit sowie eine zeitnahe Aufdeckung notwendig sind (vergleiche auch General Deterrence Theorie nach Straub und Welke 1998). Dies zeigt, dass eine wechselseitige Beziehung zwischen der Automatisierung und organisatorischen Maßnahmen besteht. Die folgenden Anforderungen fassen die angestellten Überlegungen zusammen.

Anforderung 8: Die IT sollte als Enabler für das GRC-Management eingesetzt und durch geeignete Organisationskonzepte unterstützt werden.

Anforderung 9: Kontrollen sollten zur Erhöhung der Wirksamkeit von organisatorischen Maßnahmen der Compliance-Sicherung und Risikosteuerung sowie aus Gründen der Kostensenkung weitestgehend automatisiert werden. Gleichzeitig sollten automatisierte Kontrollen durch organisatorische Maßnahmen komplementär unterstützt werden.

3.4.2.6 Flexibilität

In der Literatur wird insbesondere die Flexibilisierung der Geschäftsprozesse und IT-Systeme als Herausforderung für GRC darstellt (siehe Literaturverweise zur Unterkategorie „Relevanz von Flexibilität“ in Tab. 67). Bspw. sind die Auswirkungen von Änderungen der GRC-Vorgaben auf bestehende Geschäftsprozesse zu analysieren. Umgekehrt müssen die Auswirkungen von Prozessänderungen auf die Compliance betrachtet werden (Müller 2007, S. 109). Außerdem besteht die Notwendigkeit, die Geschäftsrisiken genau zu überwachen, da die Risikovermeidung zum Entwurfszeitpunkt der Geschäftsprozesse bei sich ständig ändernden Prozessabläufen und unterstützender IT nur noch begrenzt möglich ist (Sackmann 2008b, S. 1138). Eine Berücksichtigung der Flexibilität wird insbesondere auch vor dem Hintergrund neuer IT-

Trends, die eine flexibilitätssteigernde Wirkung haben sollen, gefordert. In der GRC-Literatur werden insbesondere serviceorientierte Architekturen (SOA) (siehe Literaturverweise zur Unterkategorie „Flexibilität durch serviceorientierte Architekturen“ in Tab. 67) und Cloud-Computing (siehe Literaturverweise zur Unterkategorie „Flexibilität durch Cloud-Computing“ in Tab. 67) diskutiert. Grundei (2006) (Unterkategorie „Trade-off zwischen Flexibilität und Compliance“) betrachtet zudem die Beziehung zwischen vertrauens- und kontrollbasierten Ansätzen im Organizational Design. Vertrauensbasierte Organisationskonzepte werden als ein Instrument der Flexibilitätssteigerung angesehen.

Flexibilisierung ist ein Bereich, der bereits seit Jahren ausgiebig thematisiert wird. Entwicklungen wie Internationalisierung, kurze Produktlebenszyklen, sinkende Losgrößen und wachsende Kundenanforderungen erfordern eine Erhöhung der Flexibilität (Warnecke 1997; Westkämper 1997). Der Begriff des „Real-Time-Enterprise“ wurde im Kontext des GPM geprägt und rückt auch die Bedeutung der IT für die Flexibilisierung des Unternehmens in den Blickpunkt (Scheer 2003; Kuhlin und Thielmann 2005). Flexibilität wird daher auch in der Wirtschaftsinformatik- und Information Systems-Forschung thematisiert (siehe bspw. Byrd und Turner 2000; Byrd und Turner 2001; Melarkode und Fromm-Poulsen 2004; Nissen und Mladin 2009; Sambamurthy et al. 2003). Der Begriff Flexibilität ist facettenreich und gleichzeitig in eine Reihe weitere Begrifflichkeiten einzureihen, die nur schwer voneinander abzugrenzen sind. Zu nennen sind bspw. die Begriffe Anpassungsfähigkeit, Agilität und Elastizität (Burmann 2005, S. 31; Termer und Nissen 2014). Zentral für die Flexibilität eines Unternehmens oder der Informationsverarbeitung ist die Möglichkeit der schnellen Reakti-

on auf geänderte geschäftliche Anforderungen (Nissen 2008; Nissen und Mladin 2009).

Grundei (2006) diskutiert die Beziehung zwischen vertrauens- und kontrollbasierten Ansätzen im Organizational Design. Bei der Analyse der Beziehung geht Grundei von der Annahme aus, dass Unternehmen beide Fähigkeiten benötigen, sie müssen sich also sowohl an neue Marktbedürfnisse flexibel anpassen können, als auch die Normkonformität sicherstellen. Kontrollbasierte Ansätze gehen auf agenturtheoretische Überlegungen zurück. Das Prinzipal-Agenten-Problem lässt sich hierbei bspw. auf dezentrale Unternehmensstrukturen zurückführen, wobei sichergestellt werden muss, dass die Mitarbeiter konform zu den relevanten Normen handeln. Da die Prinzipal-Agenten-Theorie grundsätzlich opportunistisches Verhalten unterstellt, werden Kontrollmechanismen in Form von Überwachung und Anreizsystemen vorgeschlagen, um konformes Verhalten zu erreichen. Vertrauensbasierte Ansätze gehen auf die Stewardship-Theorie zurück, die grundsätzlich unterstellt, dass die Akteure im Interesse der Organisation handeln. Kontrollmechanismen werden hierdurch überflüssig. Gerade durch Konzepte, die auf einer solchen Verhaltensannahme aufbauen, kann jedoch eine Flexibilitätssteigerung erreicht werden. In Beiträgen zur prozessorientierten Organisationsgestaltung wird diese Erhöhung des Handlungsspielraums und der Verantwortung von Mitarbeitern ebenfalls als zentrales Gestaltungsmerkmal beschrieben um eine Flexibilitätssteigerung herbeizuführen. Namentlich sind Job Enlargement, Job Enrichment und Empowerment zu nennen (siehe bspw. Schmelzer und Sesselmann 2013, S. 209). Hingegen werden in Arbeiten zu GRC kontrollbasierte Ansätze auf Basis der Prinzipal-Agenten-Theorie favorisiert.

Des Weiteren ist Flexibilität im Kontext der IT relevant. Obwohl die IT auf der einen Seite als Enabler des GRC-Managements angesehen werden kann, ist die IT jedoch auch ein zentraler Gegenstand von GRC. Im Kontext der IT existieren vielfältige Compliance-Vorgaben als auch Anforderungen aus Governance und Risikomanagement. Wenn Kontrollen im Rahmen von operativen Informationssystemen ausgeführt werden müssen, ist vor dem Produktivbetrieb des neuen Systems bzw. der neuen Funktionalität sicherzustellen, dass neben den funktionalen Benutzeranforderungen auch diese Kontrollen wie spezifiziert umgesetzt wurden. Hiermit wird deutlich, dass neue geschäftliche Anforderungen aufgrund höherer Aufwände langsamer umgesetzt werden könnten. Zusätzlich zu diesem grundsätzlichen Konflikt zwischen Flexibilität und GRC im Kontext der IT entstehen weitere Herausforderungen, wenn bestimmte IT-bezogene Ansätze, wie bspw. SOA oder Cloud-Computing, zur Steigerung der IT-Flexibilität betrachtet werden.[52]

Es erscheint notwendig, dass Unternehmen den beschriebenen „tradeoff" zwischen GRC und Flexibilität bewusst bei Entscheidungen, durch Abwägung des Non-Compliance-Risikos, berücksichtigen. Dieser Konflikt lässt sich in den allgemeinen Konflikt zwischen GRC und den Geschäftszielen eingliedern (Böhm et al. 2009, S. 7; Grundei 2006, S.

[52] SOA werden auf eine Vielzahl von Werten und Prinzipien zurückgeführt (Arsanjani et al. 2009). Hier sind insbesondere zwei Eigenschaften von Bedeutung. Erstens werden Services nicht exklusiv für einen Prozess verwendet. Zweitens erfolgt die Orchestrierung der Services dynamisch und kontextspezifisch für die jeweilige Geschäftsanforderung. Der Begriff Cloud-Computing wird in der Literatur auf drei Ansätze zurückgeführt. Hierzu gehören Software as a Service (SaaS), wobei es sich um das Angebot von Anwendungssystemen handelt, Platform as a Service (PaaS), was bspw. Entwicklerplattformen sind und Infrastructure as a Service (IaaS), welches im Wesentlichen Computerhardware und Speicherplatz zur Verfügung stellt (Mei et al. 2008; Weinhardt et al. 2009).

43).[53] Zur Lösung des Zielkonflikts sind unterschiedliche Vorschläge gemacht worden. Sowohl Böhm et al. (2009) für die IT-Abteilung als auch Grundei (2006) für die Organisationsgestaltung schlagen ein situationsspezifisches Ausbalancieren des Zielkonflikts vor, wobei die spezifischen strategischen Aspekte ebenso wie die GRC-Situation zu analysieren sind.

Anforderung 10: Die Herausforderung flexibler Geschäftsprozesse und IT-Systeme ist in dem Konflikt zwischen strategischer Zielerreichung und regulatorischen GRC-Erfordernissen begründet. Dieser Zielkonflikt sollte situationsspezifisch ausbalanciert werden.

3.4.2.7 Menschliche Faktoren

In der Literatur werden mehrere Faktoren gefordert, die sich mit der Motivation der Mitarbeiter im Kontext des strategischen GRC-Managements auseinandersetzen. Hierbei wird die Berücksichtigung des Verhaltens der beteiligten Mitarbeiter (siehe Literaturverweise zur Unterkategorie „Compliance-Verhalten" in Tab. 68), die Berücksichtigung der GRC-bezogenen Kultur (siehe Literaturverweise zur Unterkategorie „Compliance-Kultur" in Tab. 68) sowie die Etablierung einer effizienten Unternehmenskommunikation im Sinne eines „tone at the top" (siehe Literaturverweise zur Unterkategorie „tone at the top" in Tab. 68) gefordert.

Die Determinanten für das Compliance-Verhalten, die wie bereits angesprochen im Kontext der Informationssicherheit diskutiert werden (Abraham 2011; Al-Omari et al. 2013; Al-Omari et al. 2012a; Al-Omari et al. 2012b; Aurigemma und Panko 2012; Boss et al. 2009; Bulgurcu et

[53] Siehe hierzu auch Abschnitt 3.4.2.1.

al. 2009; Bulgurcu et al. 2010; D' Arcy et al. 2009; Goo et al. 2012; Guo und Yuan 2012; Herath und Rao 2009; Hu et al. 2012; Hsu 2009; Hu et al. 2011; Johnston und Warkentin 2010; Johnston et al. 2010; Lebek et al. 2013; Liang et al. 2013; Lowry und Moody 2013; Milicevic und Goeken 2012; Milicevic und Goeken 2013a; Milicevic und Goeken 2013b; Myyry et al. 2009; Pahnila et al. 2007; Puhakainen und Siponen 2010; Siponen et al. 2006; Siponen und Vance 2010; Son 2011; Spears und Barki 2010; Vance et al. 2012; Yayla 2011), ergeben sich aus den verhaltenswissenschaftlichen Theorien und beinhalten die Einstellung, die subjektive Norm, die Verhaltensabsicht und das tatsächliche Compliance-Verhalten. Diese werden wiederum von der intrinsischen und extrinsischen Motivation sowie der Awareness für Compliance beeinflusst. Der Kodierungsprozess beinhaltete keine detaillierte Auswertung der Determinanten zum Compliance-Verhalten, vielmehr war es das Ziel besonders wichtige Aspekte zu erfassen. Eine Analyse der Theorien und Konstrukte zeigt ein weit detailreicheres Bild.[54]

Vergleicht man die Erkenntnisse, die auf der Grundlage der verhaltenswissenschaftlichen Theorien zum Compliance-Verhalten gewonnen wurden mit den theoretischen Aussagen der Organisational Control Theorie wird deutlich, dass GRC nicht auf die Automatisierung von präventiven und detektiven Kontrollen reduziert werden kann. Vielmehr sind solche prozessorientierten Kontrollen einerseits durch ergebnisorientierte Kontrollen in Form von Anreizsystemen zu ergänzen. Andererseits sollten jedoch auch soziale bzw. kulturelle Kontrollen im Sinne der Organisational Control Theorie nicht vernachlässigt werden.

[54] Eine detailliertere Aufarbeitung des Forschungsstandes zu theoretischen und empirischen Erkenntnissen im Kontext des Compliance-Verhaltens findet sich in Abschnitt 3.5.9.

Lange (2008) weist zu Recht auf die Bedeutung der Beziehung der Kontrollen zueinander hin. So ist zu vermuten, dass die Kombination der Kontrollen nicht in beliebiger Weise erfolgen kann, sondern dass konfliktäre Konstellationen entstehen können.[55] Des Weiteren ist zu vermuten, dass der Kontrollansatz nicht unabhängig von der jeweiligen Situation aufgesetzt werden kann, sondern dass hierbei ebenfalls Abhängigkeiten bestehen. Aus der Analyse wird folgende Anforderung geschlussfolgert.

Anforderung 11: Die Determinanten des Compliance-Verhaltens erfordern die Berücksichtigung vielfältiger Kontrollformen. Der gewählte Kontrollansatz sollte die Beziehung der Kontrollen zueinander ebenso wie situationsspezifische Aspekte berücksichtigen.

3.4.3 Zwischenfazit

In Abschnitt 3.4.2 wurden die Anforderungskategorien sowie die im Rahmen der Kodierung identifizierten Unterkategorien dargestellt und anhand der relevanten Theorien zu Anforderungen in Form von konkreten Handlungsempfehlungen weiterentwickelt. Diese sind in Tab. 9 zusammengefasst. Es konnte gezeigt werden, dass ein strategischer GRC-Management-Ansatz vielfältigen Anforderungen genügen sollte.

[55] Im Rahmen der Diskussion der Beziehung von Prinzipal-Agenten- und Stewardship-Theorie (Grundei 2008) wird darauf hingewiesen, dass ein von Misstrauen geprägtes Handeln gerade opportunistisches Verhalten der Mitarbeiter erzeugen kann. Mitarbeiter könnten gerade in einem System, dass anstrebt Compliance sehr rigide, bspw. durch einen verpflichtenden IT-gestützen Prozess, durchzusetzen, versuchen diesen zu umgehen um ihren Eigennutzen, durch das Einsparen von eigenem Aufwand zu erhöhen. Kampagnen, die versuchen ein Bewusstsein für Compliance-Aspekte zu schaffen, könnten hierdurch zudem ins Leere laufen.

Die Integration stellt hierbei einen wichtigen Aspekt dar, ermöglicht an sich jedoch noch keinen adäquaten GRC-Management-Ansatz.

Die Anforderungskategorien stellen eine erste inhaltliche Strukturierung des Themengebietes strategisches GRC-Management dar. Die Anforderungen haben normativen Charakter und sollen außerdem die theoretischen Erkenntnisse für weitere Forschungsvorhaben verdichten und speziell als Ausgangspunkt zur Entwicklung von Lösungskomponenten für das strategische GRC-Management dienen. Die Anforderungen können ähnlich wie Hypothesen in Anlehnung an Atteslander (2010, S. 22) als „Erklärungsversuche der ungeklärten Umwelt" verstanden werden, haben somit vorläufigen Charakter und sollen weitere Forschung leiten.

Tab. 9: Anforderungen an das strategische GRC-Management

Nr.	Anforderungs-kategorie	Anforderung
1	Strategische Ausrichtung	1. GRC sollte an den strategischen Zielen des Unternehmens ausgerichtet werden, um die Überlebensfähigkeit des Unternehmens nicht zu gefährden.
		2. Die das GRC-Management konstituierenden Ressourcen sollten die Erzielung operativer Nutzenpotentiale ermöglichen.
		3. GRC sollte an den Stakeholderinteressen ausgerichtet werden. Die Stakeholderinteressen sollten hierbei unter der Prämisse der langfristigen Maximierung des Unternehmenswertes ausbalanciert werden.
2	Integration	4. Die für GRC relevanten Management-Aktivitäten sollten einem zentralen Ansatz folgen. Die operativen Aktivitäten sind in die Kernprozesse und operativen IT-Systeme zu integrieren.

Nr.	Anforderungs-kategorie	Anforderung
		5. Zur Nutzung von Synergien und Verhinderung von Doppelarbeiten bzw. Lücken sollten GRC-Aktivitäten über verschiedene Bereiche (bspw. Compliance-Vorgaben) als auch über die GRC-Disziplinen integriert werden.
3	Geschäftspro-zess-orientierung	6. Eine ablauforientierte Sicht sowie Vorgehens-modelle, Methoden und Werkzeuge des Ge-schäftsprozessmanagements sollten zur Senkung von Transaktionskosten im GRC-Bereich adap-tiert werden.
4	Management-Systeme	7. Zur Harmonisierung der Management-Systeme im Kontext von GRC sollten geeignete Vorge-hensweisen, Methoden und Werkzeuge entwickelt werden.
5	Automatisie-rung	8. Die IT sollte als Enabler für das GRC-Management eingesetzt und durch geeignete Organisationskonzepte unterstützt werden.
		9. Kontrollen sollten zur Erhöhung der Wirk-samkeit von organisatorischen Maßnahmen der Compliance-Sicherung und Risikosteuerung so-wie aus Gründen der Kostensenkung weitestge-hend automatisiert werden. Gleichzeitig sollten automatisierte Kontrollen durch organisatorische Maßnahmen komplementär unterstützt werden.
6	Flexibilität	10. Die Herausforderung flexibler Geschäftspro-zesse und IT-Systeme ist in dem Konflikt zwi-schen strategischer Zielerreichung und regulatori-schen GRC-Erfordernissen begründet. Dieser Zielkonflikt sollte situationsspezifisch ausbalan-ciert werden.
7	Menschliche Faktoren	11. Die Determinanten des Compliance-Verhaltens erfordern die Berücksichtigung vielfäl-tiger Kontrollformen. Der gewählte Kontrollan-satz sollte die Beziehung der Kontrollen zueinan-der ebenso wie situationsspezifische Aspekte berücksichtigen.

Im Rahmen der Darstellung und Diskussion der Anforderungen wurden im Wesentlichen Ergebnisse zum Forschungsziel „Beschreiben und Erklären“ verwendet. Jedoch war es nicht das Ziel den Forschungsstand systematisch aufzuarbeiten und gegebenenfalls vorhanden Forschungsbedarf zu identifizieren. Im folgenden Abschnitt 3.5 wird die Perspektive gewechselt. Es wird das Ziel verfolgt, den Forschungsstand im Hinblick auf die Anforderungen kritisch zu analysieren und offenen Forschungsbedarf zu identifizieren.

3.5 Forschungsstand und weiterer Forschungsbedarf

3.5.1 Strukturierung der Diskussion des Forschungsstandes

Zur Strukturierung des Forschungstandes können die Anforderungskategorien für einen strategischen GRC-Management-Ansatz sowie die dazugehörigen Unterkategorien herangezogen werden, da diese die benötigten Fähigkeiten und zu erfüllenden Bedingungen an einen solchen Ansatz widerspiegeln. Des Weiteren sind die folgenden Überlegungen relevant.

Es soll eine Unterscheidung in die Forschungsziele „Beschreiben und Erklären“ sowie „Gestalten“ vorgenommen werden. Heinrich et al. (2007, S. 18) führt als Aufgaben von Wissenschaft Beschreibung, Erklärung, Prognose und Gestaltung ein. Als Kernaufgaben werden Erklärung und Gestaltung hervorgehoben. Es wird außerdem betont, dass die Beschreibung von Phänomenen als Voraussetzung für ihre Erklärung angesehen werden kann. In der Wirtschaftsinformatik- und Information Systems-Forschung lässt sich, wie bereits einleitend ausge-

führt[56], die verhaltenswissenschaftliche von der gestaltungsorientierten Forschungsausrichtung unterscheiden. Verhaltenswissenschaftliche Forschung kann den Aufgaben „Beschreiben und Erklären" zugeordnet werden. Gestaltungsorientierte Forschung erfüllt hingegen die Aufgabe „Gestalten" (siehe zur Zuordnung Lange 2005, S. 10). Es ist außerdem darauf zu verweisen, dass die gestaltungorientierte Forschung oftmals einen zweistufigen Forschungsaufbau verwendet (Lange 2005, S. 11). Hierbei werden die beiden Kernaktivitäten „Entwicklung" und „Evaluierung" voneinander unterschieden (March und Smith 1995; Peffers et al. 2006; Österle et al. 2010). Es kann zudem argumentiert werden, dass gestaltungsorientierte Forschung auf Erkenntnissen zum Forschungsziel „Beschreiben und Erklären" aufbauen sollte. Gleichzeitig bieten gestaltungsorientierte Forschungsergebnisse wiederum Ansatzpunkte für Forschung zum Forschungsziel „Beschreiben und Erklären" (Hevner et al. 2004, S. 79-80).

Um eine strukturierte Aufarbeitung der Arbeiten zur gestaltungsorientierten Forschung im Kontext von GRC zu ermöglichen, wird eine Strukturierung anhand der unterschiedlichen Artefakte vorgeschlagen. Wie einleitend ausgeführt, können als Artefakte (begriffliche) Konstrukte, Modelle, Methoden und Instanzen unterschieden werden (Hevner et al. 2004, S. 78-79).[57] Diese von Hevner et al. (2004) gewählte Abgrenzung und Strukturierung ist durchaus nicht ohne Kritik (Zelewski 2007). Zum einen könnten Theorien auch als Artefakte angesehen werden. Andererseits sind Modelle eine Art von Theorien im

[56] Siehe Abschnitt 1.3.

[57] Die Definition der Begriffe Kontrukt, Modell, Methode und Instanz basierend auf Hevner et al. (2004, S. 78-79) ist in Abschnitt 1.3 enthalten.

Kleinen. Letztlich besteht ein Abgrenzungsproblem zwischen dem Begriff Artefakt und den in der Wissensbasis genannten Begriffen wie Instrument oder Methodologie, woraus sich ein Konkretisierungsbedarf ergibt. Um eine solche Konkretisierung vornehmen zu können, ist ein Verständnis darüber notwendig, welche Artefakte für das GRC-Management relevant sind. Hierfür sind der Management-Begriff sowie der Begriff des Konzepts relevant. Konzepte unterscheiden insbesondere zwischen Ziel-Modellen und Vorgehensweisen zur Erreichen dieser Ziele.[58] In der Wirtschaftsinformatik-Forschung existiert zudem der Ansatz des Methoden-Engineerings. Demnach bestehen Methoden aus Aktivitäten, Techniken, Ergebnissen und Rollen. Eine Aktivität bezeichnet hierbei eine Ausführung, die Techniken einsetzt und Ergebnisse erzielt. Hierbei legen Techniken fest, wie eine Aktivität ausgeführt wird. Rollen beschreiben, durch wen eine Aktivität ausgeführt wird. Eine Methode muss außerdem die Abfolge der Aktivitäten spezifizieren (siehe hierzu bspw. Börner und Goeken 2009, S. 4; Heym 1993). Zusammenfassend sind aus gestaltungsorientierter Sicht folgende Artefakte im Kontext eines GRC-Management-Ansatzes relevant.

- (Ziel-)Modell bspw. in Form eines Referenzmodells
- Vorgehensweise bestehend aus Management-Aktivitäten und Rollenmodell
- Methoden für einzelne Management-Aktivitäten
- Werkzeuge (bspw. Informationssysteme) zur Unterstützung

[58] Siehe Abschnitt 2.8.

Zur Diskussion der Methoden im Kontext der Anforderungen wird zwischen Management-Methoden, Methoden zur Modellierung von GRC-Informationen und Methoden zur Automatisierung der Compliance-Sicherung und Risikosteuerung (im Weiteren als Automatisierungsmethoden bezeichnet) unterschieden. Automatisierungsmethoden werden in der Literatur (Sackmann 2008c, S. 43; Sadiq et al. 2007) einheitlich in die Ansätze „compliance by design" und „compliance by detection" unterschieden. Werkzeuge werden im weiteren Verlauf den Automatisierungsmethoden zugeordnet. Eine Übersicht der Methoden, die in der GRC-Literatur zu finden sind, ist in Tab. 69 enthalten. Die oben genannten Kategorien Zielmodell und Vorgehensweisen werden in sogenannte Management-Ansätze zusammengefasst.

Im Hinblick auf die Entwicklung eines Management-Ansatzes für GRC sind Arbeiten, die sich mit GRC-Management-Ansätzen befassen von besonderer Bedeutung. Zum einen kann durch die Analyse der existierenden Ansätze gezeigt werden, dass bislang kein Ansatz alle Anforderungen erfüllt. Dies stellt die Forschungslücke für die Entwicklung eines neuen Ansatzes dar. Zum anderen können diese Vorarbeiten in besonderer Weise zur Entwicklung eines neuen Ansatzes beitragen. Die anhand der Literatursuche identifizierten Management-Ansätze für GRC sind in Tab. 10 überblicksartig wiedergegeben. Einige Arbeiten die Management-Ansätze darstellen wurden nicht weiter betrachtet, da diese nicht ausreichend dokumentiert sind bzw. lediglich von geringer Relevanz für ein strategisches und integriertes GRC-Management sind

(Deloitte 2008, DIN 2008a; DIN 2008b; Gill und Purushottam 2008; Krey 2012; Krey et al. 2012[59]).

Um eine bessere Strukturierung zu ermöglichen, wird die Diskussion der Management-Ansätze im Anschluss zuerst vorgenommen, bevor der Forschungsstand im Allgemeinen zu den Anforderungskategorien dargestellt und hinsichtlich des weiteren Forschungsbedarfs analysiert wird.

Tab. 10: Management-Ansätze für GRC aus der Literatur

Bezeichnung	Kurzbeschreibung	Quellen
Böhm	Böhm beschreibt Gestaltungsgrundätze für IT-Compliance durch welche mehr Wertbeitrag durch den IT-Einsatz erzielt werden soll.	Böhm 2008
COSO	Das COSO beschreibt sowohl ein Rahmenwerk für die Umsetzung eines internen Kontrollsystems als auch für die Umsetzung eines unternehmensweiten Risikomanagements.	COSO 1994; COSO 2004

[59] Krey et al. (Krey 2012; Krey et al. 2012) geben zwar an einen Ansatz für IT-Governance, Risk und Compliance im Krankenhaus entwickeln zu wollen, die Publikationen beziehen sich jedoch lediglich auf die Entwicklung von Anforderungen für einen solchen Ansatz und die Grundlegung des forschungsmethodischen Ansatzes, der für die Entwicklung des Ansatzes herangezogen werden soll. Die Dokumentation des Ansatzes selbst ist nicht ausreichend genug, um in der folgenden Diskussion Berücksichtigung zu finden. Neben einem kurzen Literaturüberblick zu den GRC-Teilbereichen entwickelt Krey et al. (Krey 2012; Krey et al. 2012) Eigenschaften und Anforderungen an eine Methode zur Umsetzung von IT Governance, Risk und Compliance im Krankenhaus. Als Eigenschaften, die relevant für eine solche Methode sind, werden die Autonomie einzelner Organisationseinheiten von Krankenhäusern genannt, die Vielfalt und Komplexität von IT-GRC und die Rolle der IT in Krankenhäusern. Die Anforderungen bleiben insgesamt recht allgemein und stellen stärker auf formale Aspekte ab als auf inhaltliche Anforderungen. So wird neben der Verwendung von bestehenden Best Practices (wie bspw. COBIT (ITGI 2007)) sowie Methoden und Werkzeugen bspw. eine adäquate Berücksichtigung von Machtstrukturen und Entscheidungswegen in Krankenhäusern gefordert. Des Weiteren wird die Entwicklung der Anforderungen nur auf einem hohen Abstraktionsniveau beschrieben, womit die Herleitung der konkreten Anforderungen nicht nachvollziehbar begründet ist.

Bezeichnung	Kurzbeschreibung	Quellen
El Kharbili et al.	El Kharbili et al. entwickeln einen geschäftsprozessorientierten Ansatz für das Compliance-Management unter Berücksichtigung beider Ansätze zur Automatisierung von Compliance. Der Ansatz basiert auf semantisch beschriebenen Policies in Form von Ontologien.	El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b; El Kharbili et al. 2008c
Corporate Governance of Information Technology	Die ISO/IEC 38500 ist ein Standard zur „Corporate governance of information technology". Hierunter wird ein System verstanden, welches den gegenwärtigen und zukünftigen Einsatz der IT steuert und kontrolliert.	ISO 2008
Integrated Enterprise Balancing (IEB)	Das „Integrated Enterprise Balancing" (IEB) verfolgt die Zielsetzung der Unterstützung des wertorientierten Managements sowie der regulatorischen Anforderungen an Transparenz und Finanzberichterstattung durch integrierte Ertrags- und Risikogrößen.	Faisst und Buhl 2005; Fill et al. 2007
Menzies / PwC	Die Darstellung dieses Ansatzes ist in den einzelnen Veröffentlichungen uneinheitlich. Menzies (2006) beschreibt im Kern das GRC-Stufenmodell. Demnach soll ausgehend von der projektbasierten Umsetzung einzelner Anforderungen („Compliance"), die Nachhaltigkeit im Regelbetrieb sichergestellt werden („Transformation & Optimierung"). Letztlich findet die Integration von GRC und somit eine Optimierung des GRC-Ansatzes statt („Integration & Optimierung"). Stufenübergreifend soll die Optimierung des internen Kontrollsystems und der Geschäftsprozesse ermöglicht werden („Compliance-Driven Optimization").	PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012
OCEG	Die OCEG bietet nach eigener Aussage einen vollständigen Ansatz für ein GRC-System. Im Kern steht hierbei das OCEG Capability Model, welches aus den Elementen Context & Culture, Organize & Oversee, Assess & Align, Prevent & Promote, Detect and Discern, Inform & Integrate, Respond & Resolve sowie Monitor & Measure besteht.	OCEG 2009
Pupke	Pupke identifiziert auf der Grundlage einer Transaktionskostenanalyse den „Hybrid Compliance Approach" als beste Koordinationsform des Compliance-Managements. Dieser ist eine dezentralisierte Koordinationsform und integriert die Compliance-Aktivitäten in die Primärorganisation.	Pupke 2008
IDW	Das IDW beschreibt im Rahmen eines Prüfungsstandards für Compliance-Management-Systeme grundsätzliche Elemente solcher Management-Ansätze.	IDW 2010; Withus 2010
Racz et al.	Racz et al. entwickeln ein Prozessmodell für IT-GRC indem sie einzelne Prozessschritte bestehender Ansätze für die Teildisziplinen einander zuordnen.	Racz et al. 2010b; Racz et al. 2010c; Racz et al. 2011b

Bezeichnung	Kurzbeschreibung	Quellen
Rath und Sponholz	Rath und Sponholz formulieren einen IT-Compliance-Management-Ansatz, der die drei Hauptbereiche Organisation, Prozess und Werkzeuge unterscheidet.	Rath und Sponholz 2009, S. 117-153
Sackmann et al.	Sackmann et al. entwickeln ein Rahmenwerk für die Automatisierung von Compliance, wobei Risikoaspekte integriert werden sollen. Dieses beinhaltet eine geschäftsprozessorientierte Methode, die die Ansätze „compliance by design“ und „compliance by detection“ in einer mehrstufigen Vorgehensweise berücksichtigt	Sackmann 2008c; Sackmann 2009; Sackmann und Kähmer 2008; Sackmann et al. 2008
COBIT	Die Version 4.1 der Control Objectives for Information and Related Technology (COBIT 4.1) stellt ein Best Practice-Rahmenwerk für IT-Governance dar. Im Kern beschreibt COBIT insgesamt 34 IT-Prozesse, denen Kontrollziele (engl. Control Objectives) zugeordnet sind.	ITGI 2007
Vicente und da Silva	Vicente und da Silva entwickeln zum einen ein konzeptionelles Modell für GRC auf Basis der Analyse der GRC-Teildisziplinen, das die für GRC relevanten Informationen beinhalten soll. Diese Informationen werden in einem zweiten Schritt dem Prozessmodell von Racz et al. (2011b; 2010c) zugeordnet.	Vicente und da Silva 2011a; Vicente und da Silva 2011b
Hauschka und Vetter	Vetter beschreibt aufbauend auf den Überlegungen von Hauschka ein Vorgehensmodell für Compliance, welches auf den fünf Aktivitäten Risikoanalyse, Commitment, Kommunikation, Organisation und Dokumentation basiert.	Hauschka 2007, S. 19-21; Wecker und van Laak 2008, S. 41-47

3.5.2 Untersuchung von GRC-bezogenen Management-Ansätzen hinsichtlich der Berücksichtigung der Anforderungen

3.5.2.1 Strategische Ausrichtung

Obwohl strategische Aspekte in einigen Management-Ansätzen angesprochen werden, ist die strategische Ausrichtung im Sinne der Anforderungskategorie bestenfalls teilweise berücksichtig. In den Rahmenwerken der COSO (1994; 2004) dient Risikomanagement der Erhöhung der Sicherheit bzgl. der Erreichung der strategischen Ziele. Das heißt

Risikoanalysen (auch im Hinblick auf Compliance-Risiken) sind auf der Grundlage der strategischen Bedeutung durchzuführen. Der Zielkonflikt zwischen Compliance und dem strategischen Zielerreichungsgrad wird jedoch ebenso wenig berücksichtigt wie die Verfolgung von Nutzenpotentialen. Im Rahmen des ISO Standards für „Corporate Governance of IT" (ISO 2008) wird das Prinzip „Strategy" eingeführt. Dieses beinhaltet die Forderung der Ausrichtung der IT an den Geschäftszielen (Business/IT-Alignment) und nicht die Ausrichtung von GRC an den Geschäftszielen. Des Weiteren wird das Begriffspaar „Performance" und „Conformance" eingeführt. Auf den hiermit verbundenen Zielkonflikt wird jedoch nicht eingegangen. Ebenso wie der ISO Standard zur IT-Governance thematisiert auch COBIT (ITGI 2007) im Wesentlichen das Business/IT-Alignment.

Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012) sprechen verschiedene Aspekte im Kontext der Anforderungskategorie strategische Ausrichtung an. Menzies (2006) versteht die Verfolgung von Nutzenpotentialen als Teil der sogenannten Compliance-Driven Optimization, jedoch ist hierfür keine systematische Methode definiert. Ebenfalls wird die Methode der Stakeholderanalyse betrachtet. Hiermit sollen die Erwartungen der Stakeholder erkannt und durch Priorisierung hinsichtlich ihrer Relevanz gebündelt werden. Auf die methodischen Aspekte und die Adaption für das GRC-Management wird jedoch kaum eingegangen (Menzies 2006, S. 360).

Die OCEG (2009) berücksichtigt die strategische Ausrichtung in zweifacher Weise. Erstens wird versucht die Ergebnisse der Monitoring-Aktivitäten für die Erstellung eines Verbesserungsplans und somit zur Weiterentwicklung des GRC-Managements einzusetzen (siehe Aktivität „M3 Systemic improvement"). Die Ausrichtung von GRC an den strategischen Zielen bleibt jedoch unbeachtet. Zweitens wird eine Analyse

der Stakeholder vorgeschlagen. Hierbei wird neben der Kommunikation mit den Stakeholdern die Bedeutung von Organisationen, die für GRC relevante Best Practices oder Standards herausgeben, betont (siehe Aktivität „P7 Stakeholder Relations & Requirements“).

Pupke (2008) geht auf die strategische Bedeutung von GRC in Form des Zielkonflikts zwischen Geschäfts- und GRC-Zielen ein und stellt die Bedeutung von Compliance als Unterstützer der Geschäftsstrategie heraus. Systematische Methoden zur Verwirklichung von Nutzenpotentialen werden jedoch nicht vorgestellt. Das IDW (IDW 2010; Withus 2010) stellt fest, dass die Compliance-Ziele aus den Unternehmenszielen abzuleiten sind. Eine Methode hierfür wird jedoch ebenfalls nicht beschrieben. Der „trade-off“ zwischen Unternehmens- und Compliance-Zielen wird wie die Verfolgung von Nutzenpotentialen nicht betrachtet. Vicente und da Silva (2011a; 2011b) erwähnen an mehreren Stellen die Bedeutung der Berücksichtigung strategischer Aspekte und integrieren die Elemente „strategy“ und „key objectives“ in ihr konzeptionelles Modell, jedoch bleiben die Hinweise wie eine strategische Ausrichtung von GRC stattfinden kann recht unkonkret. So soll, gemäß dem Modell, Risikomanagement mit den „key objectives“ abgestimmt und die Strategie in den Policies umgesetzt werden.

Die weiteren Ansätze erfüllen die Anforderungskategorie weitestgehend nicht. Böhm (Böhm 2008, S. 21-22) nennt zwar Strategie als einen der Gestaltungsgrundsätze von IT-Compliance, jedoch meint er damit die Strategie der IT-Compliance, im Sinne einer geplanten Vorgehensweise, die auch zukünftige Entwicklungen berücksichtigt. Racz et al. (2010b; 2010c) fordert in seiner Definition die Berücksichtigung strategischer Aspekte, integriert solche jedoch nicht in sein Prozessmodell. In den Ansätzen von El Kharbili et al. (El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b; El Kharbili et al. 2008c), dem Integrated Enter-

prise Balancing (IEB) (Faisst und Buhl 2005; Fill et al. 2007), Rath und Sponholz (2009), Sackmann et al. (Sackmann 2008c; Sackmann 2009; Sackmann und Kähmer 2008; Sackmann et al. 2008) und Hauschka und Vetter (Hauschka 2007, S. 19-21; Wecker und van Laak 2008, S. 41-47) werden strategische Aspekte nicht explizit erwähnt.

3.5.2.2 Integration

Integrierte Ansätze für das Management von GRC lassen sich bei Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012), bei der OCEG (2009), bei Racz et al. (2010b; 2010c; 2011b) sowie Vicente und da Silva (Vicente und da Silva 2011a; Vicente und da Silva 2011b) finden. Bei Menzies (2006) wird die Phase „Integration & Optimierung" als Teil des GRC-Stufenmodells dargestellt. Die Integration von GRC soll mit Hilfe einer Methodik für Optimierungsprojekte durchgeführt werden. Im Wesentlichen zeigt der Ansatz, wie nach der Umsetzung eines internen Kontrollsystems das Compliance-System hin zu einem umfassenden Ansatz für GRC weiterentwickelt werden kann. Im Kern der Integration von GRC steht die sogenannte Corporate Rule Base, die alle Compliance-Kontrollen strukturiert in einer Datenbank abbilden soll. Eine Verbindung zu Governance- und Risikomanagement-Aspekten wird jedoch nur eingeschränkt hergestellt. Auch ein Prozessmodell zum integrierten Management von GRC wird nicht dargestellt.

Die OCEG (2009) stellt das GRC Capability Model vor, das aus neun Kategorien und 29 Sub-Elementen besteht, für die wiederum jeweils Aktivitäten gelistet werden.[60] Somit stellt es sehr detailliert mögliche

[60] Siehe Abschnitt 2.6.

GRC-Aktivitäten dar, jedoch ist unklar, wie innerhalb der Aktivitäten eine Integration stattfindet. Explizit wird zwar die Komponente „Integrate and Inform“ eingeführt. Diese bezieht sich jedoch lediglich auf ein harmonisiertes Dokumentations- und Kommunikationskonzept. Racz et al. (2011b; 2010c) entwickeln ein Prozessmodell für „IT GRC“, das auf einem Mapping von ausgewählten Ansätzen aus den GRC-Teildisziplinen beruht, namentlich der Standard für „IT Governance of IT“ der ISO (2008), der Ansatz zum Risikomanagement des COSO (2004) und der IT-Compliance-Management-Ansatz von Rath und Sponholz (2009). Obwohl das Prozessmodell auf einem hohen Abstraktionsniveau die Beziehungen von GRC und die Möglichkeit einer integrierten Vorgehensweise aufzeigt, sind auch verschiedene Schwachstellen erkennbar. Zum einen erscheint die Auswahl der Ansätze recht willkürlich. So wird bspw. COBIT für die IT-Governance nicht verwendet. Außerdem wird lediglich der Prozess dargestellt und es werden diesem keine Rollen bzw. unterstützende Methoden und Werkzeuge zugeordnet. Darüber hinaus ist die Beschränkung auf IT-GRC unklar, da einerseits bspw. der Ansatz der COSO unternehmensweit konzipiert ist und andererseits im Risikomanagement auch separate IT-bezogene Ansätze aufgrund der ähnlichen methodischen Vorgehensweise in Frage gestellt werden. Letztlich werden bei der Entwicklung des Prozessmodells bestehende Ansätze zwar in der Auswahl evaluiert, jedoch dann unreflektiert übernommen. In wie fern diese Ansätze den aktuellen Anforderungen von GRC entsprechen, wird nicht betrachtet.

Vicente und da Silva (2011a; 2011b) entwickeln auf der Grundlage einer Analyse der Begriffe Governance, Risiko- und Compliance-Management zuerst separate konzeptionelle Modelle für die GRC-Teildisziplinen, die dann zu einem GRC-Modell integriert werden. Den Autoren folgend enthält dieses Modell die für GRC relevanten Infor-

mationen bzw. Konzepte[61]. In einem weiteren Schritt wird das Prozessmodell von Racz et al. (2011b; 2010c) mit ausgewählten Elementen dieses Modells erweitert. Weiterhin werden mögliche GRC-bezogene Akteure im Sinne eines Rollenmodells eingeführt, ohne eine Zuordnung zu den Prozessschritten vorzunehmen. Hinsichtlich des Integrationsaspekts kann der Ansatz von Vicente und da Silva somit als derjenige mit dem größten Reifegrad bezeichnet werden. Wie die Autoren selbst einräumen, handelt es sich dabei um einen Ansatz auf hohem Abstraktionsniveau, der zur Anwendung in der Praxis weiter verfeinert und erweitert werden muss.

Weitere Management-Ansätze integrieren GRC nur teilweise (Böhm (2008, S. 22-23), COSO (1994; 2004), IDW (IDW 2010; Withus 2010), Corporate Governance of Information Technology (ISO 2008), IEB (Faisst und Buhl 2005; Fill et al. 2007)) oder gar nicht (El Kharbili et al. (El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b; El Kharbili et al. 2008c), Pupke (2008), Rath und Sponholz (2009), Sackmann et al. (Sackmann 2008c; Sackmann 2009; Sackmann und Kähmer 2008; Sackmann et al. 2008), COBIT (ITGI 2007), Hauschka und Vetter (Hauschka 2007, S. 19-21; Wecker und van Laak 2008, S. 41-47)).

Arbeiten, die die GRC-Disziplinen teilweise integrieren, subsumieren entweder Compliance unter Risikomanagement (COSO (1994; 2004), IDW (IDW 2010; Withus 2010)) oder IT-Compliance unter IT-Governance (Corporate Governance of Information Technology (ISO 2008)). Das IEB (Faisst und Buhl 2005, S. 404) integriert Compliance- und Risikoaspekte im Kontext des wertorientierten Managements.

[61] Eine detailliertere Analyse des Modells von Vicente und da Silva findet sich in Abschnitt 5.3.1.1.

Böhm (2008, S. 22-23) verweist zwar auf die Zusammenhänge von Compliance mit Governance und Risikomanagement, stellt jedoch keinen integrierten Management-Ansatz für GRC dar. Zur integrierten Erfüllung von mehreren Compliance-Vorgaben schlägt Böhm jedoch einen konkreten Ansatz vor, der einen Anforderungskatalog mit einer Zuordnung von Kontrollzielen zu Compliance-Vorgaben beinhaltet. Er fordert außerdem eine Integration der IT-Kontrollen, die sich aus den Kontrollzielen herleiten, und den operativen IT-Prozessen. Letztlich fordert er auch die Etablierung eines zentralen Compliance-Office. Hauschka und Vetter (Hauschka 2007, S. 19-21; Wecker und van Laak 2008, S. 41-47) sehen lediglich das Management der Compliance-Risiken als Kernaufgabe des Compliance-Managements. Eine integrierte Erfüllung von mehreren GRC-Vorgaben wird auch im Rahmen des Ansatzes der COSO (1994; 2004) thematisiert, die zur Errichtung eines unternehmensweiten, und somit über mehrere Risikobereiche harmonisierten Risikomanagements bzw. eines internen Kontrollsystems dienen. Des Weiteren sollen hiermit mehrere normative Vorgaben wie das KonTraG oder der SOX erfüllt werden. Zudem wird in diesen Rahmenwerken ebenso wie in den Best Practices zur IT-Governance allgemein auf die Einhaltung von Vorgaben verwiesen (COSO 1994, S. 13; COSO 2004, S. 3; ISO 2008, S. 2; ITGI 2007, S. 7). Das Institut für Wirtschaftsprüfer stellt mit seinem Prüfungsstandard für Compliance-Management-Systeme einen Rahmen bereit, der auf verschiedene Rechtsgebiete als auch Geschäftsbereiche und operative Prozesse angewendet werden kann (IDW 2010, S. 16). Alle diese Hinweise bleiben recht allgemein, und es wird nicht aufgezeigt, wie verschiedene GRC-Vorgaben in einem integrierten Konzept erfüllt werden können. Auch konkrete Hinweise für die Harmonisierung der Risikobereiche bspw. hinsichtlich des Informationsaustauschs werden nicht gegeben.

3.5.2.3 Geschäftsprozessorientierung

Von der OCEG (2009), Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012) und Pupke (2008) wird zwar eine Integration von GRC in die operativen Geschäftsprozesse (operative Integration) gefordert. Eine Verbindung zum GPM wird jedoch nicht hergestellt. Hauschka und Vetter (Hauschka 2007, S. 19-21; Wecker und van Laak 2008, S. 41-47) sowie das IDW (IDW 2010; Withus 2010) berücksichtigen ebenso nicht die Möglichkeiten der Geschäftsprozessorientierung. Böhm (2008) stellt in seinem Ansatz für das IT-Compliance-Management ebenfalls keine Verbindung zu Vorgehensweisen, Methoden oder Werkzeugen des GPM her. Es wird lediglich unkonkret auf die Bedeutung eines Modells für die IT-Prozesse hingewiesen. Racz et al. (2010c; 2011b) sowie Rath und Sponholz (2009) und COBIT (ITGI 2007) stellen zwar die Beschreibung des Management-Prozesses in den Mittelpunkt ihrer Ansätze, eine Verbindung zu Methoden und Werkzeugen sowie dem GPM als Ganzes wird jedoch ebenfalls nicht hergestellt. Andere Arbeiten (COSO 1994; COSO 2004; ISO 2008) lassen durch eine vielfältige Verwendung des Begriffs Prozess (bzw. process) eine gewisse geschäftsprozessorientierte Sichtweise vermuten, jedoch wird hierbei keine Verbindung zur Geschäftsprozessorientierung hergestellt.

Der Ansatz von Vicente und da Silva (2011a; 2011b) basiert auf ArchiMate, einer offenen und unabhängigen Enterprise Architecture-Sprache (The Open Group 2013), womit auch eine Modellierung von Geschäftsprozessen unterstützt wird. Die Autoren wenden ArchiMate jedoch lediglich auf die Entwicklung des eigenen GRC-Ansatzes an, wobei unter anderem der GRC-Managementprozess modelliert wird. Im Rahmen des entwickelten konzeptionellen Modells wird außerdem der Begriff „process“ verwendet und mit Zielen sowie Risiken in Ver-

bindung gesetzt. Eine Anwendung von Methoden des GPM innerhalb des Management-Ansatzes für Fragestellungen von GRC findet jedoch nicht statt. Sackmann et al. (Sackmann 2008c; Sackmann 2009; Sackmann und Kähmer 2008; Sackmann et al. 2008) entwickeln einen mehrstufigen Ansatz mit dessen Hilfe ausgehend von normativen Texten automatisierte Compliance-Kontrollen entwickelt werden können. Hierbei wird immer wieder auf die Bedeutung der Geschäftsprozesse für die Compliance verwiesen. In wie weit Ergebnisse des GPM bzw. Methoden und Tools des GPM diesen Ansatz ergänzen können wird nicht expliziert.

Das IEB (Faisst und Buhl 2005; Fill et al. 2007) und El Kharbili et al. (El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b; El Kharbili et al. 2008c) stellen eine weitergehende Verbindung zum GPM her. Die von Fill et al. (2007) vorgestellte Modellierungsmethode für das IEB ermöglicht eine Integration in das GPM. Die Autoren entwickeln eine formale Modellierungssprache zur integrierten Berücksichtigung von Informationen aus den Bereichen Return, Risk, Regulation und Reporting (4R) bei der Prozessmodellierung. Der Ansatz von El Kharbili et al. (El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b; El Kharbili et al. 2008c) basiert auf semantisch beschriebenen Policies in Form von Ontologien. Voraussetzung für die Anwendung ist ein vollständig semantisch beschriebenes Unternehmensmodell, wobei Ontologien zur formalen Beschreibung für Geschäftsprozesse ebenso wie für Compliance-Vorgaben existieren müssen.

3.5.2.4 Management-Systeme

Ein Teil der identifizierten Management-Ansätze bezieht sich explizit auf die IT als Gegenstand von GRC (Böhm (2008), Corporate Governance of Information Technology (ISO 2008), Racz et al. (2010b; 2010c; 2011b), Rath und Sponholz (2009, S. 117-153), COBIT (ITGI

2007)). Es wird hierbei jedoch nicht thematisiert, wie die jeweiligen Ansätze in die Prozesse und Organisationsstrukturen des IT-Managements eingebunden werden können. Der ISO-Standard „Corporate Governance of Information Technology“ (ISO 2008) berücksichtigt ebenso wie Hauschka und Vetter (Hauschka 2007, S. 19-21; Wecker und van Laak 2008, S. 41-47), Pupke (2008), Racz et al. (2010b; 2010c; 2011b), Rath und Sponholz (2009) sowie Sackmann et al. (Sackmann 2008c; Sackmann 2009; Sackmann und Kähmer 2008; Sackmann et al. 2008) nicht die Bedeutung weiterer Management-Systeme im Kontext von GRC. Böhm (2008, S. 25) weist zwar darauf hin, dass die IT-Compliance in der Lage sein könnte andere Management-Systeme wie das IT-Sicherheitsmanagement oder die Interne Revision zu entlasten. Wie die Aufgabenteilung konkret aussehen könnte und welche Abstimmungsbedarfe hierdurch entstehen, wird jedoch nicht ausgeführt. Das IEB (Faisst und Buhl 2005; Fill et al. 2007) betont die Bedeutung weiterer Management-Systeme in Form des wertorientierten Managements. Dieses stellt jedoch mehr eine spezielle Zielfunktion der Unternehmensführung als ein Management-System dar. El Kharbili et al. (El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b; El Kharbili et al. 2008c) berücksichtigt neben dem GPM keine weiteren Management-Systeme.

Die weiteren Management-Ansätze berücksichtigen die Aspekte der Anforderungskategorie zumindest teilweise. Die COSO (1994; 2004), das IDW (IDW 2010; Withus 2010), die OCEG (2009, S. 19-20), Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012), COBIT (ITGI 2007) sowie Vicente und da Silva (2011a; 2011b) betonen explizit die Bedeutung einer unabhängigen internen Stelle zur Prüfung des GRC-Managements, wobei teilweise die Interne Revision als geeignet für diese Aufgabe angeführt wird. Es bleibt je-

doch unklar, wie sich genau die Aufgaben und Verantwortlichkeiten zwischen GRC und einer solchen unabhängigen Stelle aufteilen lassen. COBIT (ITGI 2007) fordert darüber hinaus die Etablierung eines Qualitätsmanagement-Systems (QMS, siehe PO8 Manage Quality). Vicente und da Silva (2011b, 202) berücksichtigen vier sogenannte „main functionalities" von GRC-bezogenen Informationssystemen. Zu diesen gehören in Anlehnung an Racz et al. (2011c) „Audit Management", „Policy Management", „Issues Management" und „Risk Management". Daher sind Aspekte des Audit Management auch im GRC-Modell der Autoren enthalten. Weitere Aspekte werden jedoch nicht diskutiert.

3.5.2.5 Automatisierung

Die Ansätze des COSO (1994; 2004) sowie des IDW (IDW 2010; Withus 2010) bzw. von Hauschka und Vetter (Hauschka 2007, S. 19-21; Wecker und van Laak 2008, S. 41-47) berücksichtigen die Anforderungskategorie Automatisierung nicht. Der Ansatz zur Corporate Governance of Information Technology (ISO 2008) sowie Rath und Sponholz (2009) betrachten zwar explizit die IT als Gegenstand von Compliance, die Automatisierung der Compliance-Sicherung und Risikosteuerung wird jedoch ebenfalls nicht betrachtet.

COBIT (ITGI 2007), Pupke (2008), Racz et al. (2010b; 2010c; 2011b) und die OCEG (2009) betonen zwar die Bedeutung der Automatisierung der Compliance-Sicherung und Risikosteuerung, die Automatisierungsmethoden selbst werden jedoch nicht thematisiert. Stattdessen findet im Ansatz der OCEG eine Zuordnung von sogenannten „Technology Modules" zu den einzelnen Aktivitäten des Modells statt. Böhm (2008, S. 25-26) beschreibt mit „Anforderungen formalisieren", „Deckungslücken identifizieren", „Bewertung unterstützen", „Behebung überwachen" „Umsetzung automatisieren" und „Nachweise erbringen", die möglichen Einsatzgebiete für eine Toolunterstützung im Be-

reich IT-Compliance. Es wird dabei deutlich, dass neben der automatisierten Umsetzung der Compliance-Sicherung auch eine Unterstützung von Management-Aspekten der IT-Compliance gefordert wird. Konkrete Hinweise wie eine solche IT-Unterstützung aussehen kann, werden jedoch nicht gegeben. Das IEB (Faisst und Buhl 2005; Fill et al. 2007) ist ein Konzept für die Entwicklung von integrierten Ertrags- und Risikodatenbanken, beinhaltet jedoch keine Methode zur Automatisierung der Compliance-Sicherung und Risikosteuerung. Die IT wird hierbei als Unterstützer von Managementaufgaben hervorgehoben. Der von Vicente und da Silva (2011a; 2011b) entwickelte Ansatz thematisiert ebenfalls nicht konkret die Automatisierung. Das entwickelte konzeptionelle Modell könnte jedoch als Ausgangspunkt für die Entwicklung eines Informationssystems für das GRC-Management dienen, wobei die Autoren selbst darauf hinweisen, dass die Ebenen der Informationssystems- und Technologie-Architektur nicht beachtet wurden (Vicente und da Silva 2011a, S. 6).

Die Ansätze von El Kharbili et al. (El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b; El Kharbili et al. 2008c) und Sackmann et al. (Sackmann 2008c; Sackmann 2009; Sackmann und Kähmer 2008; Sackmann et al. 2008) werden zwar in dieser Analyse aufgrund ihrer inhaltlichen Breite als Management-Ansätze aufgefasst, stellen jedoch im Kern Rahmenwerke zur Automatisierung der Compliance-Sicherung unter Berücksichtigung der Ansätze „compliance by design“ und „compliance by detection“ dar. Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012) betrachten sowohl die Management-Unterstützung als auch die Automatisierung der Compliance-Sicherung und stellen weiterhin fest, dass bereits geeignete Technologie zur Unterstützung von GRC in Unternehmen existiert, diese jedoch nur unzureichend auf GRC-bezogene Problemstellungen ange-

wendet wird. Hierzu werden insbesondere Anwendungen im Bereich des Reporting und des GPM gezählt. PwC unterscheidet im Rahmen der entwickelten Referenzarchitektur für GRC zwischen den fünf Ebenen „User Interaction“, „GRC-Modules“ wie bspw. Reporting und Dashboards, „Repository & Processing“, wozu ein Datenrepository ebenso wie die Modellierung der Geschäftsprozesse und sogenannten Geschäftsregeln gehört, „Connectivity“ und „Sources“ zu den auch Enterprise Resource Planning (ERP) Systeme gehören (PwC 2004, S. 32-35).

3.5.2.6 Flexibilität

Flexible Geschäftsprozesse und IT-Systeme werden in den meisten Management-Ansätzen nicht berücksichtigt (COSO (1994; 2004), El Kharbili et al. (El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b; El Kharbili et al. 2008c), Corporate Governance of Information Technology (ISO 2008), IEB (Faisst und Buhl 2005; Fill et al. 2007), Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012), IDW (IDW 2010; Withus 2010), Pupke (2008), Racz et al. (2010b; 2010c; 2011b), Rath und Sponholz (2009, S. 117-153), Vicente und da Silva (2011a; 2011b), Hauschka und Vetter (Hauschka 2007, S. 19-21; Wecker und van Laak 2008, S. 41-47)).

Einige Ansätze berücksichtigen den Aspekt zumindest teilweise. Böhm (2008, S. 21) berücksichtigt bspw. nicht explizit Aspekte der Flexibilisierung, führt jedoch den Begriff der Zukunftsfähigkeit ein, der die Möglichkeit zur Aufnahme zukünftiger Vorgaben meint. COBIT (ITGI 2007) fordert zwar Flexibilität von den IT-Prozessen, dies wird jedoch nicht auf das Kontrollmodell bzw. auf das GRC-Management bezogen. Ebenso werden flexible Geschäftsprozesse und IT-Systeme von Sackmann (2008c, S. 40) als Herausforderung explizit benannt, es wird jedoch in der weiteren Darstellung nicht klar, wie diese Herausforderung

berücksichtigt wird. Ob eine höhere Flexibilität bei der Anpassung der automatisierten Kontrollen wie in vergleichbaren Ansätzen vorliegt, wird nicht überprüft und ist somit unklar (Sackmann 2008c; Sackmann 2009; Sackmann und Kähmer 2008; Sackmann et al. 2008). Die OCEG (2009, S. 17-18) fordert von einem GRC-Management-System „responsive" zu sein und meint hiermit schnell auf geänderte Bedingungen reagieren zu können. Änderungen können sich der OCEG folgend sowohl aus geänderten GRC-Vorgaben als auch aus geschäftlichen Initiativen wie M&A-Aktivitäten ergeben. Im Rahmen des Prozessmodells wird Flexibilität in der Komponente „Monitor & Measure" und hier im Rahmen der Aktivität „M1 Context Monitoring" thematisiert. Hierbei wird eine kontinuierliche Überwachung des GRC-Umfeldes gefordert. Auftretende Änderungen müssen weiterhin auf ihre Relevanz für das GRC-Management-System überprüft werden.

3.5.2.7 Menschliche Faktoren

Böhm (2008), El Kahribili et al. (El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b, El Kharbili et al. 2008c) und Sackmann et al. (Sackmann 2008c; Sackmann 2009; Sackmann und Kähmer 2008; Sackmann et al. 2008) berücksichtigen menschliche Faktoren nicht. Im ISO-Standard „Corporate Governance of Information Technology" (ISO 2008) werden verhaltensspezifische Aspekte zwar bei der Ausgestaltung der IT, jedoch nicht bei der Regeleinhaltung, berücksichtigt. Das IEB (Faisst und Buhl 2005; Fill et al. 2007) berücksichtigt kulturelle Aspekte zwar bei der Implementierungsvorgehensweise (dargestellt in Gericke et al. 2009a), bei der Methode selbst werden diese Aspekte jedoch nicht thematisiert.

Ansätze, die die Anforderungskategorie teilweise erfüllen, berücksichtigen lediglich Einzelaspekte. In verschiedenen Ansätzen wird die Bedeutung von kulturellen Aspekten sowie die Berücksichtigung von Infor-

mation und Kommunikation und hierbei insbesondere die Bedeutung des „tone at the top“ berücksichtigt (COSO (1994; 2004), Corporate Governance of Information Technology (ISO 2008); IDW (IDW 2010; Withus 2010), Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012), Pupke (2008), Racz et al. (2010b; 2010c; 2011b), Rath und Sponholz (2009), COBIT (ITGI 2007)). Einen weiteren in den Ansätzen berücksichtigten Aspekt stellen Schulungsmaßnahmen dar (Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012), Rath und Sponholz (2009), COBIT (ITGI 2007)). Vicente und da Silva (2011a; 2011b) berücksichtigen einen Teil dieser Aspekte in ihrem konzeptionellen Modell mit den Elementen „Code of Conduct“, „Culture“ und „Policies“. Hauschka und Vetter (Hauschka 2007, S. 19-21; Wecker und van Laak 2008, S. 41-47) betonen die Bedeutung der Unterstützung der Geschäftsführung und der Kommunikation der Compliance-Vorgaben, jedoch werden aufgrund der niedrigen Detailebene, in welcher der Ansatz dargestellt ist, kaum konkrete Hinweise gegeben.

Am umfangreichsten werden menschliche Faktoren im GRC-Management-Ansatz der OCEG (2009) berücksichtigt. Folgende Prozesse schlagen hierbei vielfältige Beeinflussungsmöglichkeiten von Verhaltensdeterminanten vor: Context and Culture (C3 Culture, C4 Values and Objectives), Prevent & Promote (P1 Codes of Conduct, P2 Policies, P4 Awareness & Education, P5 Human Capital Incentives), Inform & Integrate (I2 Int. & Ext. Communication) und Respond & Resolve (R5 Remediation & Discipline). Der Ansatz beinhaltet somit eine Darstellung von vielfältigen Anknüpfungspunkten zur Berücksichtigung von menschlichen Faktoren im GRC-Management. Anzumerken ist jedoch, dass keine Zurückführung der vielfältigen Aktivitäten auf ein allgemeines Modell zum Compliance-Verhalten stattfindet. Hierdurch

ist die Konsistenz und Vollständigkeit des Ansatzes nur schwer nachzuvollziehen.

3.5.2.8 Zusammenfassung der Diskussion der Management-Ansätze

Tab. 11 und Tab. 12 fassen die Bewertung der Management-Ansätze anhand der Anforderungen zusammen. (+) bedeutet, dass die Anforderung überwiegend erfüllt ist. (o) und (-) bedeuten, dass die Anforderung teilweise oder überwiegend nicht erfüllt ist. Es sei darauf hingewiesen, dass die zuvor entwickelten Anforderungen im Detail eine Vielzahl von verschiedenen Aspekten aufweisen. So ist für die Integration nicht nur eine Integration der GRC-Disziplinen (inklusive zentraler Organisation und einheitlicher Methoden und Informationssysteme) relevant, sondern ebenso eine integrierte Bearbeitung der verschiedenen GRC-Vorgaben und Risikobereiche sowie die Integration der operativen Normerfüllung und Risikosteuerung in die operativen Geschäftsprozesse. Eine vollständige Erfüllung einer Anforderung durch einen Management-Ansatz ist daher nur schwierig möglich, weshalb die höchste Einstufung (+) eine überwiegende Erfüllung reflektieren soll. In diesem Zusammenhang ist auch anzumerken, dass die Ansätze gegenseitig voneinander „lernen“ können, da unterschiedliche Aspekte mit einem unterschiedlichen Detailgrad bearbeitet werden. Als Beispiel sei der Ansatz von Böhm (2008) genannt, der zwar nur kurz auf die Integration der GRC-Disziplinen hinweist, jedoch recht detailliert eine integrierte Normerfüllung darstellt.

Insgesamt wurden mit den Ansätzen von Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012), der OCEG (2009), Racz et al. (2010b; 2010c; 2011b) und Vicente und da Silva (2011a; 2011b) vier Ansätze vorgestellt, die nach eigenen Angaben eine Integration von GRC anstreben. Keiner dieser Ansätze zeigt je-

doch eine zumindest überwiegende Erfüllung der anderen Anforderungen. Racz et al. (2010b; 2010c; 2011b) sowie die OCEG (2009) thematisieren im Wesentlichen den Management-Prozess, wohingegen Vicente und da Silva (2011a; 2011b) im Kern auf die für GRC relevanten Informationen abzielen. Menzies (2006) zeigt, wie aufbauend auf einem Projekt zur Umsetzung der Vorgaben aus dem Sarbanes-Oxley-Act, ein GRC-Ansatz verwirklicht werden kann.

Insgesamt weisen die Management-Ansätze ein recht hohes Abstraktionsniveau auf. Eine Ausnahme bilden die Ansätze von Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012) sowie der OCEG (2009). Insbesondere der letztere Ansatz liefert eine detaillierte Auflistung von GRC-bezogenen Aktivitäten, wird jedoch in der Literatur von Racz et al. (2010b; 2010c; 2011b), wie bereits ausgeführt, kritisiert. Konkrete Methoden für Teilbereiche im Bereich Geschäftsprozessorientierung, die zwar teilweise in der Literatur für GRC bereits adaptiert wurden, werden zudem weder bei diesem noch den weiteren Ansätzen integriert.

Insgesamt ist festzuhalten, dass alle Ansätze wertvolle Hinweise für ein strategisches GRC-Management liefern. Hierbei zeigt sich jedoch auch, dass sich bislang noch kein Ansatz durchgesetzt hat. Zur Weiterentwicklung der Ansätze ist es notwendig die Ziele und Anwendungsmöglichkeiten, bspw. in Form der hier dargestellten Anforderungen, offen zu legen. Außerdem sollten vorhandene Methoden insbesondere im Bereich der Geschäftsprozessorientierung oder der Automatisierung stärker in die Management-Ansätze integriert werden.

Tab. 11: Bewertung der GRC-Management-Ansätze anhand der Anforderungen (1 von 2)

	Strategische Ausrichtung	Integration	Geschäftsprozess-orientierung
Böhm	(-)	IT-Compliance (o)	(-)
COSO	(o)	Compliance als Teil des Risikomanagements (o)	(o)
El Kharbili et al.	(-)	Compliance (-)	(+)
Corporate Governance of Information Technology	(o)	Compliance als Teil der IT-Governance (o)	(o)
IEB	(-)	Compliance- und Risikomanagement (o)	(+)
Menzies / PwC	(o)	GRC (+)	(o)
OCEG	(o)	GRC (+)	(o)
Pupke	(o)	Compliance (-)	(o)
IDW	(o)	Compliance als Teil des Risikomanagements (o)	(-)
Racz et al.	(-)	GRC (+)	(o)
Rath und Sponholz	(-)	IT-Compliance (-)	(o)
Sackmann et al.	(-)	Compliance (-)	(o)
COBIT	(o)	IT-Governance (-)	(o)
Vicente und da Silva	(o)	GRC (+)	(o)
Hauschka und Vetter	(-)	Compliance (-)	(-)

Tab. 12: Bewertung der GRC-Management-Ansätze anhand der Anforderungen (2 von 2)

	Management-Systeme	Automatisierung	Flexibilität	Menschliche Faktoren
Böhm	(-)	(o)	(o)	(-)
COSO	(o)	(-)	(-)	(o)
El Kharbili et al.	(-)	(+)	(-)	(-)
Corporate Governance of Information Technology	(-)	(-)	(-)	(-)
IEB	(-)	(o)	(-)	(-)
PwC	(o)	(+)	(-)	(o)
OCEG	(o)	(o)	(o)	(+)
Pupke	(-)	(o)	(-)	(o)
IDW	(o)	(-)	(-)	(o)
Racz et al.	(-)	(o)	(-)	(o)
Rath und Sponholz	(-)	(-)	(-)	(o)
Sackmann et al.	(-)	(+)	(o)	(-)
COBIT	(o)	(o)	(o)	(o)
Vicente und da Silva	(o)	(o)	(-)	(o)
Hauschka und Vetter	(-)	(-)	(-)	(o)

3.5.3 Forschungsstand: Strategische Ausrichtung

3.5.3.1 Forschungsziel: Beschreiben und Erklären

Obwohl die strategische Ausrichtung in einer Vielzahl von Arbeiten gefordert wird, beruht diese Forderung jedoch überwiegend auf heuristischen Überlegungen bzw. die Arbeiten vertiefen diese Forderung nicht weiter (siehe Literaturverweise zur Unterkategorie „GRC als strategische Chance“ in Tab. 64). Es existieren einige Arbeiten im Kontext der IT-Governance, die bspw. die Verbindung von IT-Governance und

dem Wertbeitrag der IT bzw. dem Unternehmenswert untersuchen (Haghjoo 2012; Lazic et al. 2011; Liang et al. 2011; Musson und Jordan 2006; Urbach et al. 2013). Teilweise werden hierbei auch theoriebasierte Ansätze auf Grundlage des Resouce-based view (Lazic et al. 2011) und der Prinzipal-Agenten-Theorie (Liang et al. 2011) eingesetzt. Im Kontext von Compliance setzten Krell und Matook (2008; 2009), Kwon und Johnson (2013) sowie Mossanen (2010) gezielt Theorien ein um den strategischen Beitrag zu analysieren. Hoyt und Liebenberg (2011) messen den Einfluss von Enterprise Risk Management auf den Unternehmenswert mit Hilfe von Tobin's Q, einem Standardnäherungsverfahren für den Unternehmenswert. Insgesamt ist festzuhalten, dass die Besonderheiten von integrierten GRC-Management-Ansätzen auf die strategische Bedeutung kaum betrachtet werden, sondern lediglich Teilaspekte analysiert werden, die sich aufgrund der unterschiedlichen Forschungsansätze nur schwer zusammenführen lassen. Der Fokus ist außerdem einseitig auf die Untersuchung des Einflusses von GRC auf strategische Ziele bzw. den Unternehmenswert ausgerichtet. Die Frage, welche Auswirkungen die Strategie auf die Ausgestaltung des GRC-Managements hat und wie die Erfüllung von GRC-Vorgaben mit den strategischen Zielen abgestimmt werden könnte, wird bestenfalls am Rand thematisiert. Um weitere Erkenntnisse über die strategische Bedeutung von GRC zu erhalten, sind detaillierte theoretische Untersuchungen wünschenswert. Da in diesen Zusammenhang der Market- und der Resource-based view anwendbar sind, können folgende Forschungsbereiche identifiziert werden. Aufbauend auf den generischen Wettbewerbsstrategien von Porter (1980; 1985) kann untersucht werden, welchen strategischen Beitrag GRC in Abhängigkeit von der gewählten Strategie leisten kann, wobei Fokus, Kostenführerschaft und Diversifikation zu unterscheiden sind (siehe Forschungsbedarf 1.1.1 in Tab. 15). Der Resource-based view legt eine Untersuchung der Res-

sourcen von GRC auf ihre strategische Bedeutung (siehe Forschungsbedarf 1.1.2 in Tab. 15) nahe.

Die Verbindung von GRC mit verschiedenen Nutzenpotentialen (siehe Literaturverweise zur Unterkategorie „Nutzenpotentiale“ in Tab. 64) basiert ebenso größtenteils auf heuristischen Überlegungen. Ausnahmen bilden hierbei die Arbeiten von Wiesche et al. (Krcmar et al. 2011; Wiesche et al. 2011b) und Urbach et al. (2013), welche empirische Forschungsansätze verwenden. Des Weiteren beziehen sich diese potentiellen Nutzeneffekte auf unterschiedliche Aspekte. Hierzu gehören mögliche Nutzenpotentiale, die sich bereits aus separaten Ansätzen bzw. einer Verbesserung dieser Ansätze ergeben und sich somit auf Nutzenpotentiale bzgl. IT-Governance (Baumöl 2012, S. 12; Haghjoo 2012, S. 3; Lazic et al. 2011, S. 6; Urbach et al. 2013, S. 8-9), Nutzenpotentiale bzgl. Risikomanagement (Fill 2012; Hoyt und Liebenberg 2011, S. 795-796; Oh et al. 2007, S. 425) und Nutzenpotentiale bzgl. Compliance (Böhm 2008, S. 26-27; Damianides 2004, S. 39; Gill und Purushottam 2008, S. 45, Isensee 2008, S. 162; Klotz 2009, S. 17-19; Li et al. 2012, S. 180; Volonio et al. 2004, S. 222; Walser et al. 2007, S. 53-58; Weidlich et al. 2011, S. 1009) beziehen. Des Weiteren existieren auch Publikationen die Nutzenpotentiale im Kontext einer Integration von GRC thematisieren (Hardy und Leonard 2011, S. 8; Kranawetter 2009, S. 25; Krcmar et al. 2011, S. 8; OCEG 2009, Intro S. 16; Puspasari et al. 2011, S. 312; PwC 2004, S. 16; PwC 2007, S. 11; Racz et al. 2010b, S. 6; Racz et al. 2010a, S. 4-5; SAP 2009, S. 4; Schöler und Zink 2008, S. 21-22; Spanaki und Papazafeiropoulou 2013, S. 2; Tüllner 2012; van der Veen et al. 2011; Wiesche et al. 2011b, S. 8). Wieder andere Autoren schränken ihre Betrachtung auf Nutzenpotentiale, die durch den Einsatz von IT im Kontext von GRC entstehen können ein (Krcmar et al. 2011, S. 8; Li et al. 2012, S. 180; Racz et al. 2010a, S. 5; Walser et al. 2007, S. 53-58;

Wiesche et al. 2011b, S. 8). Durch den unterschiedlichen Fokus wird eine Synthese der Arbeiten erschwert.

Die im Kontext der Analyse des strategischen Beitrags und der Nutzenpotentiale von GRC verwendeten Konzeptualisierungen sind unterschiedlich und es werden unterschiedliche Begriffe wie „Business Performance" (Lazic et al. 2011), „Business Value" (Haghjoo 2012), „Organizational Performance" (Liang et al. 2011) oder einfach „Benefits" (Musson und Jordan 2006) bzw. „Impact" oder „Impact Factor" (Urbach et al. 2013) verwendet. Neben den bereits angesprochenen Arbeiten, welche die Verbindung von GRC und dem Unternehmenswert untersuchen, setzen sich lediglich Böhm (2008) und Walser et al. (2007) mit den theoretischen Grundlagen von Nutzenpotentialen im Kontext von GRC auseinander. Böhm (2008) unterscheidet im Kontext von Compliance zwischen Wertbeitrag und Performance der IT. Demzufolge bedeutet Wertbeitrag „mit der IT das „Richtige" für das Unternehmen zu tun, und Performance, dies „bestmöglich" zu leisten." (Böhm 2008, S. 15). Performance ist somit eine notwendige, aber nicht hinreichende Bedingung für Wertbeitrag. Compliance-Investitionen sind mit Einbußen in Leistungsfähigkeit und Flexibilität verbunden (Performance). Der Wertbeitrag der IT steigt hingegen durch Investitionen in Compliance, da ohne Compliance in der IT auch die Compliance des Gesamtunternehmens (Corporate Compliance) gefährdet ist. Ist die Compliance jedoch einmal hergestellt, können weitere Compliance-Investitionen den Wertbeitrag der IT reduzieren, da das Compliance-Niveau nicht weiter gesteigert, jedoch durch weitere Kontrollen die Unterstützung der Geschäftsanforderungen beeinträchtigt wird. Böhm formuliert einen weiteren Aspekt, der hier relevant ist. Compliance kann demzufolge als „Treiber" für geschäftliche Verbesserungen auftreten. So wird durch Compliance bspw. die Standardisierung der IT-

Prozesse sowie die Konsolidierung und Dokumentation der Anwendungssysteme vorangetrieben. Walser et al. (2007, S. 56-57) betrachten die Rentabilität von Compliance im Sinne einer Kosten-Nutzen-Betrachtung. Hierbei werden die Kosten von Compliance, die Kosten von Non-Compliance und der Nutzen von Compliance unterschieden. Im Kontext des Nutzens von Compliance spielen den Autoren folgend im Wesentlichen qualitative Nutzenpotentiale, wie Prozessoptimierung oder Kundenloyalität eine Rolle. Als Ergebnis der Kosten-Nutzen-Betrachtung wird ein negativer Return on Investment festgestellt, was ebenfalls auf den trade-off zwischen GRC und strategischer Zielerreichung hinweist. In der Literatur hat sich bislang noch kein einheitlicher Begriff hinsichtlich der Nutzenpotentiale im Kontext von GRC herausgebildet. Die Arbeiten betrachten unterschiedliche Aspekte und erfordern daher eine Konsolidierung auf Basis einheitlicher Begrifflichkeiten.

Im Kontext der Unterkategorie Nutzenpotentiale ergeben sich aus Sicht des Forschungsziels „Beschreiben und Erklären" somit weitere offene Forschungsfragen. Erstens ist die Untersuchung der theoretischen Grundlagen von Nutzenpotentialen durch GRC erforderlich (siehe Forschungsbedarf 1.1.3 in Tab. 15). Hierzu gehört die Definition der grundlegenden Begriffe um ein einheitliches Verständnis über den Forschungsstand herbeizuführen, wobei die betriebswirtschaftlichen Begriffe Nutzen und Wertbeitrag relevant erscheinen (siehe bspw. Bartsch und Schlagwein 2010, S. 238; Harbrecht 1993, S. 271, Kluckhohn 1962, S. 395). Zweitens stellt sich in diesem Zusammenhang die Frage wie die Nutzenpotentiale strukturiert werden können. Aus den oben angeführten Definitionen wird bereits deutlich, dass Nutzenpotentiale analog zum Wertbeitrag inhärent subjektiv sind (Bartsch und Schlagwein 2010, S. 238; Kluckhohn 1962, S. 395). Tallon et al. (2000) weisen im Kontext des Wertbeitrags von IT darauf hin, dass dieser aufgrund

abweichender Zielsetzungen von verschiedenen Beteiligten im Unternehmen unterschiedlich wahrgenommen wird. Da sich der Wertbeitrag an der Unterstützung der Zielerreichung der Beteiligten Interessensgruppen bemisst, liegt es nahe, diese Zielsetzungen bei der Strukturierung der Nutzenpotentiale aufzugreifen. Drittens sollte das Verhältnis von Nutzenpotentialen zu Wettbewerbsvorteilen analysiert werden. Wie bereits angeführt wurde, werden bspw. von Melville et al. (2004) im Kontext des IT/Business Value operative Performanceverbesserungen von der Frage nach einem nachhaltigen strategischen Wettbewerbsvorteil getrennt. Die Analyse der Grundlagen der Nutzenpotentiale ermöglicht die empirische Exploration und Validierung der Nutzenpotentiale (siehe Forschungsbedarf 1.1.4 in Tab. 15).

Der Zielkonflikt oder „trade-off" zwischen Geschäfts- und GRC-Zielen wird in der Literatur bislang, zumindest aus strategischer Perspektive, kaum untersucht. Unbeachtet bleibt derzeit die Frage, welche konkreten Aspekte bspw. im IT-Management oder in der Organisationsgestaltung konfliktär sind. So wird lediglich darauf hingewiesen, dass der Zeitaufwand bei der Änderung oder Neuimplementierung dadurch steigt, dass ebenfalls Kontrollen implementiert und getestet werden müssen (Böhm et al. 2009, S. 12). Es ist zu vermuten, dass eine Vielzahl solcher Konflikte bestehen. Außerdem wird noch nicht der Nutzen dieser Maßnahmen im Rahmen einer Risikominimierung berücksichtigt. Ein Verständnis der konkreten Konflikte sowie der hiermit verbundenen Kosten und Nutzeneffekte ist die Grundlage um eine systematische Methode zu entwickeln, die in der Lage ist, eine Ausbalancierung von GRC und strategischer Zielerreichung zu ermöglichen. Der Zielkonflikt ist zum einen im engen Zusammenhang mit der strategischen Bedeutung zu sehen und kann, soweit der Handlungsspielraum nicht durch verpflichtende Vorgaben eingeschränkt ist, ebenfalls im Kontext der

Untersuchung der strategischen Bedeutung erfolgen. Des Weiteren wird die Bedeutung des Zielkonflikts im Rahmen der Anforderungskategorie Flexibilität in Abschnitt 3.5.8 untersucht.

Im Rahmen der Forderung nach einer Orientierung des GRC-Managements an den Interessen der Stakeholder (Menzies 2006, S. 2; OCEG 2009, Intro S. 6) gibt es kaum konkrete Forschungsergebnisse. Die Autoren sind sich einig, dass als Ausgangspunk für die Analyse der GRC-Vorgaben die Interessen der Stakeholder dienen können. Auch wird das Akzeptieren von (Rest-)Risiken letztlich durch die Stakeholder beeinflusst. Bislang existieren jedoch keine Untersuchungen, welche Stakeholder für bestimmte GRC-Vorgaben oder GRC-Bereiche relevant sind. Daher sollte dieses Thema in weiteren Forschungsarbeiten aufgegriffen werden (siehe Forschungsbedarf 1.1.5 in Tab. 15).

3.5.3.2 Forschungsziel: Gestalten

Aus gestaltungsorientierter Sicht findet die strategische Ausrichtung bislang wenig Beachtung. Wie gezeigt, erfüllt derzeit keiner der Management-Ansätze die strategische Ausrichtung im Sinne der Anforderungskategorie. Management-Methoden im Kontext von GRC, die sich mit dem Reporting und damit auch der Steuerung von Compliance auseinandersetzen (Faisst und Buhl 2005; Fill et al. 2007; Gericke et al. 2009a; Goeken und Knackstedt 2008; Goeken und Knackstedt 2009; Panitz et al. 2010) und somit im Kontext der strategischen Ausrichtung von Interesse sein könnten, fokussieren mehr auf die Erfassung des Risiko- und Compliance-Status sowie die Kommunikation zu den Stakeholdern, als auf die Berücksichtigung von GRC im strategischen Planungsprozess. Auch die von Böhm et al. (2009) und Grundei (2006) dargestellten Methoden zum Ausbalancieren von GRC und strategischer Zielerreichung betrachten die Thematik nur sehr grundlegend

und geben erste Hinweise, wie die konkrete Situation bei dieser Aufgabe berücksichtigt werden könnte.

Wie die Arbeiten von Krell und Matook (2008; 2009) im Kontext von verpflichtenden IT-Investitionen zeigen, könnten strategische Planungsmethoden methodisch die Ausrichtung des GRC-Managements unterstützen. Diese wurden bislang jedoch noch nicht für das strategische GRC-Management adaptiert, weswegen dies einen weiteren Forschungsbedarf darstellt (siehe Forschungsbedarf 1.2.1 in Tab. 15). Hinsichtlich der strategischen Planungsmethoden kann eine Unterscheidung zwischen formalen (Lorange 1980), informalen (Leontiadis und Tezel 1980), emergenten (Mintzberg 1978; Mintzberg und McHugh 1985) und autonomen (Burgelman 1983) Methoden getroffen werden. Eine analoge Unterscheidung lässt sich auch in der strategischen Planung von Informationssystemen finden (Gartner 2008; Lederer und Salmela 1996; McFarlan et al. 1983). Obwohl zur Vorteilhaftigkeit formaler strategischer Planungsmethoden unterschiedliche Ergebnisse existieren (Pearce et al. 1987; Armstrong 1982) und Unternehmen auch eigenentwickelte Methoden einsetzen können, haben sich in der Forschung standardisierte Planungsmethoden entwickelt (siehe bspw. Krell und Matook 2009, S. 36). Strategische Planungsmethoden für das strategische GRC-Management müssen nicht die strategischen Ziele des Unternehmens an sich formulieren, sondern sicherstellen, dass das GRC-Management an den Unternehmenszielen ausgerichtet werden kann. Dies legt die grundsätzliche Anwendbarkeit von Methoden der strategischen Planung von Informationssystemen nahe, die analog hierzu eine Ausrichtung des IT-Einsatzes an den strategischen Unternehmenszielen ermöglichen sollen. Zu beachten ist außerdem, dass eine Vielzahl von Investitionen in GRC mit Investitionen in IT einhergeht. Krell und Matook (2009, S. 36) nennen folgende Standardmethoden:

business cases (Ward und Peppard 2002), internal contractual arrangements (Feeny und Willcocks 1998), IT balanced scorecards (Teubner 2007), importance–performance portfolios (Ward und Peppard 2002), information engineering (Lederer und Sethi 1988) und post-implementation reviews (Piccoli und Ives 2005).

Böhm et al. (2009) schlagen eine Ausbalancierung von GRC und Geschäftszielen an der spezifischen Unternehmenssituation vor. Methodisch wird hierbei auf das IT Strategic Impact Grid von Nolan und McFarlan (2005) zurückgegriffen, das auch auf einzelne Unternehmensbereiche, Prozesse oder Leistungen der IT angewendet werden kann. Um der Frage wie vertrauens- und kontrollbasierte Ansätze sich vereinbaren lassen nachzugehen, greift Grundei (2006) auf Poole und Van de Ven (1989) zurück. Diese unterscheiden allgemein die vier Möglichkeiten „opposition", „spatial separation", „temporal separation" und „synthesis" um einem Spannungsverhältnis zwischen theoretischen Konzepten zu begegnen. Als Lösungsversuch greift Grundei die Synthese auf, wobei wiederum situationsspezifische Faktoren in der Unternehmensumwelt als Ausgangspunkt dienen. Beide Ansätze bleiben insgesamt recht abstrakt. Vielversprechend erscheint daher eine Berücksichtigung des „trade-offs" zwischen GRC und strategischer Zielerreichung in den strategischen Planungsmethoden (siehe Forschungsbedarf 1.2.2 in Tab. 15).

Bzgl. der Unterstützung der Stakeholderorientierung beschreibt Menzies (2006, S. 360) explizit den Einsatz der Stakeholderanalyse im Kontext des strategischen GRC-Managements. Hiermit sollen die Erwartungen der Stakeholder erkannt und durch Priorisierung hinsichtlich ihrer Relevanz gebündelt werden. Auf die methodischen Aspekte und die Adaption für das GRC-Management wird jedoch kaum eingegangen. Außerdem stellt die Stakeholderanalyse die Grundlage zum Aufbau

der sogenannten „Corporate Rule Base“ dar, in welcher ausgehend von den Stakeholdern die Compliance-Vorgaben und Risiken systematisch erfasst werden sollen. Die Analyse der Stakeholder erfolgt im Rahmen des strategischen Managements in der sogenannten Umweltanalyse. Hiermit wird die Frage gestellt, welche Merkmale der Umwelt und insbesondere der Stakeholder für die Wahl und Umsetzung der Wettbewerbsstrategie relevant sind (Bea und Haas 2005, S. 86-89). Sie ist somit der Festlegung von Wettbewerbsstrategien vorgelagert. Zur Durchführung der Stakeholderanalyse existieren vielfältige methodische Empfehlungen (Janisch 1992). Für die einzelnen Aufgaben der Stakeholderanalyse können fallspezifisch unterschiedliche Methoden, wie heuristische Suchstrategien oder Expertenbefragungen angewendet werden (Hügens und Zelewski 2006, S. 369-372). Aus der Abwesenheit von methodisch fundierten Arbeiten zur Stakeholderanalyse im Kontext des strategischen GRC-Managements ergibt sich aus gestaltungsorientierter Sicht der Forschungsbedarf der Adaption der Stakeholderanalyse für das strategische GRC-Management (siehe Forschungsbedarf 1.2.3 in Tab. 15).

3.5.4 Forschungsstand: Integration

3.5.4.1 Forschungsziel: Beschreiben und Erklären

Im Rahmen der Analyse der Anforderungskategorie Integration wurde aufbauend auf den Erkenntnissen von Pupke (2008) und mit Hilfe der Transaktionskostentheorie die mögliche Vorteilhaftigkeit der Integration von GRC aufgezeigt. Die Analyse bleibt jedoch bewusst auf einem recht hohen Abstraktionsniveau und untersucht nicht konkrete Aspekte der Vereinheitlichung von Vorgehensweisen, Methoden und Werkzeugen der GRC-Disziplinen. Zur weiteren Analyse sind detailliertere Einteilungen für die möglichen Koordinationsformen erforderlich. Im

Kontext der IT-Governance werden die sogenannten Archetypen „Business monarchy“, „IT monarchy“, „Feudal“, „Federal“, „IT duopoly“ und „Anarchy“ (Weill und Ross 2004, S. 12) unterschieden. Eine solche Detaillierung würde empirische Untersuchungen zur Vorteilhaftigkeit des Koordinierungsansatzes ermöglichen (siehe Forschungsbedarf 2.1.1 in Tab. 15). Ein weiterer Aspekt der in diesem Zusammenhang relevant ist, ist die Untersuchung der Integration des GRC-Managements in die operativen Geschäftsprozesse. Diese sollte sich auf unterschiedliche Dimensionen oder Rahmenwerke beziehen. Bspw. wird im Kontext von internen Kontrollsystemen zwischen Kontrollen auf unterschiedlichen Ebenen wie unternehmensweiten Kontrollen (engl. company level controls) und Prozesskontrollen (engl. process level controls) unterschieden (Menzies 2006, S. 21 und S. 228, siehe Forschungsbedarf 2.1.3 in Tab. 15).

Für die Integration von GRC ist eine einheitliche Terminologie notwendig. Die Terminologie ist für jeden Forschungsbereich von grundlegender Bedeutung um die relevanten Begriffe zu definieren, ihre Bedeutung abzugrenzen und Zusammenhänge aufzuzeigen. Hierdurch können Unklarheiten in der wissenschaftlichen Diskussion beseitigt und ein einheitliches Verständnis des Themengebiets in der Praxis herbeigeführt werden (siehe auch Schryen 2010, S. 228). Definitionen und Abgrenzungen zu GRC lassen sich in vielen Beiträgen finden, wobei natürlichsprachliche Ansätze (Hardy und Leonard 2011; Klotz 2009; Klotz und Dorn 2008; Krey 2010; Krey 2012; Krey et al. 2012; Menzies 2006; OCEG 2009; Puspasari et al. 2011; PwC 2004; PwC 2007; Racz et al. 2010b; SAP 2009; Schöler und Zink 2008; Tarantino 2007; Teubner und Feller 2008) ebenso wie schematische Darstellungen (Klotz 2009, S. 8-11; Klotz und Dorn 2008, S. 6-10; Kranawetter 2009, S. 24; Puspasari et al. 2011, S. 312; Racz et al. 2010b; SAP 2009, S. 8; Schöler

und Zink 2008, S. 17-18) und Datenmodelle (Puspasari et al. 2011; Vicente und da Silva 2011a; Vicente und da Silva 2011b) zur Untersuchung und Darstellung der Beziehungen von GRC eingesetzt werden.[62] Racz et al. (2010b) liefern eine Definition für GRC und erheben empirisch den aktuellen Stand der Integration hinsichtlich Organisation, Prozessen und Softwarewerkzeugen in der Praxis. Rückschlüsse auf die Vorteilhaftigkeit einer Integration können hieraus nur begrenzt gezogen werden. Wie die Diskussion der Begrifflichkeiten gezeigt hat[63], hat sich hinsichtlich der Terminologie in Forschung und Praxis noch kein einheitliches Verständnis durchgesetzt. Ebenfalls muss festgestellt werden, dass GRC noch überwiegend als Schlagwort für ein neues Themengebiet verwendet wird. So verwenden Krcmar et al. (2011) sowie Spanaki und Papazafeiropoulou (2013) GRC als Obergriff für eine Klasse von Informationssystemen, jedoch wird hierbei nicht deutlich, wie sich solche Informationssysteme von anderen nicht integrierten Informationssystemen zu Compliance oder Risikomanagement abgrenzen.

Racz et al. (2010a, S. 4) unterscheiden die Dimensionen Strategie, Prozesse, organisatorische Struktur und Technologie um den Stand von GRC in der Praxis zu erheben. Viele Organisationen sind dieser Studie folgend noch unentschlossen bzgl. der Bedeutung von GRC. Am weitesten fortgeschritten ist die Etablierung einer zentralen Stelle für GRC in der Praxis. Die Integration von Prozessen und Informationssystemen steht hingegen noch am Anfang. Racz et al. (2011a) stellen anhand einer empirischen Erhebung fest, dass sich die Integration von GRC

[62] Eine detailliertere Auseinandersetzung mit diesen Arbeiten findet im Rahmen der Entwicklung des eigenen Datenmodells für ein strategisches GRC-Management in Abschnitt 5.3.1.1 statt.

[63] Siehe Abschnitte 2.5 und 2.6.

auf eine Vielzahl von Aspekten, die sowohl die Konzept- als auch die Technologieebene betreffen, erstreckt. Teilweise wird IT-Risiko- und Compliance-Management zentralisiert und mit unternehmensweiten Ansätzen verbunden.[64] Sowohl die Diskussionen zur Terminologie in der Literatur als auch die Erhebung des Standes zu GRC in der Praxis zeigen, dass Forschungsbedarf hinsichtlich der Integration der GRC-Teildisziplinen besteht. Hierbei sollte insbesondere eine Untersuchung von Überschneidungen und Synergieeffekten sowie Inkonsistenzen zwischen den GRC-Disziplinen stattfinden (siehe Forschungsbedarf 2.1.2 in Tab. 15).

Zur integrierten Erfüllung verschiedener GRC-Vorgaben wird die gleichzeitige Berücksichtigung mehrerer Best Practices bzw. Standards in der Literatur aufgegriffen. Alter und Goeken (2009) schlagen Metamodelle zur Analyse, Vergleich und Integration der Komponenten und Strukturen von Referenzmodellen wie ITIL (OGC 2007a; OGC 2007b) und COBIT (ITGI 2007) vor. Krey et al. (2011) entwickeln ein Schema zur Klassifikation von Best Practice-Ansätzen im Kontext von GRC. Walser und Goeken (2011) untersuchen die Möglichkeiten und Grenzen eines multiplen Einsatzes von IT-Governance- und IT-Management-Techniken, wozu auch Best Practice-Ansätze wie ITIL und COBIT gehören und diskutieren hierzu unterschiedliche Strukturierungsmöglichkeiten. Die Arbeiten zeigen, dass weitere Untersuchungen notwendig sind, die Überscheidungen und Synergieeffekte sowie

[64] Krey (2010) stellt die Ergebnisse einer Studie zum aktuellen Stand von IT-Governance im Schweizer Krankenhaussektor in den Bereichen Business-IT-Alignment, Leistungsmessung, Ressourcenmanagement, Risikomanagement und Compliance dar. Die Studie verwendet zwar „Governance, Risk and Compliance“ im Titel untersucht jedoch nicht die Integrationsaspekte von GRC.

Inkonsistenzen von GRC-Vorgaben betrachten (siehe Forschungsbedarf 2.1.5 in Tab. 15) sowie die Grenzen einer integrierten Normerfüllung analysieren (siehe Forschungsbedarf 2.1.6 in Tab. 16). Des Weiteren erscheint aufgrund der gleichzeitigen Verwendung mehrerer Best Practices ein strukturierter Vergleich dieser vor dem Hintergrund von Überschneidungen und Synergien sinnvoll (siehe Forschungsbedarf 2.1.8 in Tab. 16). Letztlich könnte die Analyse zur Identifikation von „Basiskontrollen", die für jedes GRC-System relevant sind, führen (siehe Forschungsbedarf 2.1.7 in Tab. 16).

Neben diesen Bereichen wird hinsichtlich der Integration in der Literatur auch der Zusammenhang von IT-bezogenen und unternehmensweiten Ansätzen im Kontext von GRC thematisiert. Wolf und Goeken (2010, S. 239) gehen der Frage nach, welche Kriterien das IT-Risikomanagement erfüllen muss, um adäquate Informationen für das unternehmensweite Risikomanagement bereitstellen zu können. Anhand dieser Kriterien wird gezeigt, dass IT-Risikomanagement-Ansätze derzeit nur unzureichende Informationen für das unternehmensweite Risikomanagement liefern. Wolf und Goeken (2011) untersuchen darüber hinaus die Integration von IT- und unternehmensweitem Risikomanagement auf Basis einer ontologischen Darstellung der Ansätze. Durch die Abbildung der Ansätze und ihrer Schnittstellen soll ein zutreffendes Bild der Gesamtrisikosituation von Unternehmen ermöglicht werden. Racz et al. (2010d, S. 6) untersuchen die Beziehung von unternehmensweitem und IT-Risikomanagement anhand der Rahmenwerke der COSO (2004) und der Information Systems Audit and Control Association (ISACA) (ISACA 2009) für unternehmensweites bzw. IT-Risikomanagement. Hierbei werden separate Ansätze aufgrund der ähnlichen methodischen Vorgehensweise in Frage gestellt. Insgesamt ist die Beziehung von einem unternehmensweiten GRC-Management

und IT-bezogenen Aspekten des GRC-Managements wenig untersucht. Eine genaue Trennung dieser Bereiche erscheint zudem vor dem Hintergrund, dass IT fast alle Geschäftsprozesse unterstützt, überaus schwierig. Eine Untersuchung der Integration von IT-bezogenen und unternehmensweiten Ansätzen für GRC ist daher notwendig (siehe Forschungsbedarf 2.1.4 in Tab. 15).

Aus Sicht der informationstechnischen Integration stellt der Beitrag von Racz et al. (2011c) die bisher einzige Arbeit dar, die versucht, den Softwaremarkt sowie die Anforderungen in der Praxis aus der Perspektive eines integrierten GRC-Managements zu untersuchen.[65] Eine Untersuchung von Nutzenpotentialen und Schwachstellen von Software, die ein integriertes Management von GRC ermöglicht, wird hierbei jedoch nicht vorgenommen und stellt daher einen Forschungsbedarf dar (siehe Forschungsbedarf 2.1.9 in Tab. 16).

3.5.4.2 Forschungsziel: Gestalten[66]

Wie im Rahmen der Analyse der Management-Ansätze gezeigt, existieren Ansätze, die eine Integration von GRC verfolgen (Menzies / PwC (PwC 2004; PwC 2007; Menzies 2006; Menzies et al. 2008; Tüllner 2012), OCEG (2009), Racz et al. (2010b; 2010c; 2011b) und Vicente und da Silva (2011a; 2011b)), jedoch die genannten Schwächen aufweisen. Aus Sicht der Integration von GRC lässt sich konstatieren, dass die

[65] Siehe ebenso Abschnitt 3.5.2.5.

[66] Dieser Abschnitt ist anhand der Unterkategorien zur Anforderungskategorie Integration (siehe Tab. 6) strukturiert und greift zudem die Unterteilung der relevanten Artefakte für das strategische GRC-Management auf (siehe Abschnitt 3.5.1). Management-Methoden, Methoden zur Modellierung von GRC-Informationen und Methoden zur Automatisierung der Compliance-Sicherung und Risikosteuerung sind der Unterkategorie methodische und informationstechnische Integration zuzuordnen.

überwiegende Zahl der gestaltungsorientierten Publikationen sich entweder auf einzelne GRC-Vorgaben bzw. GRC-Bereiche wie die Informationssicherheit (Gehrke und Thams 2010; Goeken und Knackstedt 2008; Kronschnabl 2010; Md Khan 2007; Puhakainen und Siponen 2010; Setiono et al. 2006), das interne Kontrollsystem (Chang et al. 2013; Guan und Levitan 2012; Sackmann et al. 2013) oder ausschließlich auf Aspekte des Risiko- (Marinos et al. 2009; Pauli et al. 2010; Sackmann 2008a; Sackmann et al. 2009; Sienou et al. 2008), des Compliance-Managements (Delbaere und Ferreira 2007; Damianides 2004; Isensee 2008; Lohre 2009; Loosli 2008; Lu et al. 2009; Paine et al. 2005; Panitz et al. 2010; Schaad et al. 2009; Silveira et al. 2009; von Werder und Grundei 2006) oder der IT-Governance (Deutscher und Felden 2010) beziehen. Methoden, die explizit eine Integration ermöglichen, existieren kaum. Gericke et al. (2009a; 2009b) verwenden explizit den Begriff GRC im Kontext einer Management-Methode und stellen eine Methode zur Einführung von GRC-Informationssystemen vor. Das GRC Capability Modell (OCEG 2009) stellt in der Komponente „Integrate and Inform“ auf die Notwendigkeit einer abgestimmten Dokumentation und Kommunikation unterstützt durch eine einheitliche Terminologie ab. Van der Veen et al. (2011, S. 267-268), Tüllner (2012) und Menzies (2006, S. 354) beschreiben Projektvorgehensweisen zur Integration der Teilbereiche von GRC. Unterstützt wird das Vorgehen von Menzies durch die sogenannte Corporate Rule Base (Menzies 2006, S. 362-366). Obwohl diese demnach eine Schlüsselmethode für ein integriertes GRC-Management darstellt, werden die Zusammenhänge von GRC nur unzureichend deutlich. Das dargestellte Beispiel eines initialen Aufbaus einer Corporate Rule Base stellt die Erfassung der Compliance-Vorgaben ausgehend von den Stakeholdern und eine Zuordnung dieser Vorgaben zu den betroffenen organisatorischen Gestaltungselementen (Geschäftsprozesse, Organisationseinheiten) dar. Die

Berücksichtigung von Governance-Aspekten und insbesondere der Zusammenhang zu den Risiken werden nicht berücksichtigt.

Aus gestaltungsorientierter Sicht ergibt sich somit hinsichtlich der Integration der GRC-Teildisziplinen der folgende Forschungsbedarf. Zum einen ist die Referenzmodellierung in der Lage, zur Auflösung der Probleme der uneinheitlichen Terminologie und mangelnden Abgrenzung von GRC und der unzureichenden Erfassung der relevanten Beziehungen zwischen den GRC-Teilbereichen beizutragen, die zum Forschungsziel „Beschreiben und Erklären" dargestellt wurde. In diesem Sinne besteht der Bedarf der konzeptionellen Modellierung der Elemente und Beziehungen von GRC (siehe Forschungsbedarf 2.2.1 in Tab. 15). Zum anderen besteht die Notwendigkeit der Weiterentwicklung der existierenden Management-Ansätze (siehe Forschungsbedarf 2.2.5 in Tab. 15). Diese bezieht sich auf die Weiterentwicklung existierender Prozessmodelle für ein integriertes Management von GRC (siehe Forschungsbedarf 2.2.2 in Tab. 15), die Entwicklung einer Aufbauorganisation für das strategische GRC-Management (siehe Forschungsbedarf 2.2.3 in Tab. 15), sowie die Integration von GRC in Methodensysteme der Referenzmodellierung (bspw. Architektur integrierter Informationssysteme (ARIS), Multi-Perspective Enterprise Modeling (MEMO) (siehe Forschungsbedarf 2.2.4 in Tab. 15). Außerdem besteht ein Defizit hinsichtlich der Evaluierung der Vorschläge für die Integration der GRC-Disziplinen (siehe Forschungsbedarf 2.2.5 in Tab. 15), die unter anderem in den Management-Ansätzen enthalten sind.

Des Weiteren wird auch eine integrierte Erfüllung von mehreren GRC-Vorgaben bzw. eine Harmonisierung von Risikobereichen in den Management-Ansätzen im Kontext von Best Practices (COSO 1994, S. 13; COSO 2004, S. 3; ISO 2008, S. 2; IDW 2010; Regierungskommission DCGK 2010, S. 1; ITGI 2007, S. 7) sowie von Böhm (2008) verfolgt.

Überwiegend weisen die Autoren jedoch lediglich auf potentielle Möglichkeiten der integrierten Erfüllung von GRC-Vorgaben hin (Abdullah et al. 2010b, S. 550; Menzies 2006, S. 63-64; Mossanen et al. 2010, S. 180-181; Racz et al. 2010a, S. 1). Nur Haworth und Pietron (2006) zeigen konkret, wie aufbauend auf den zehn Kontrollkategorien der ISO 17799 zur Informationssicherheit SOX-Compliance erreicht werden kann. Sie stellen somit die methodische Grundlage zum Aufbau eines integrierten Kontrollmodells für Informationssicherheit und SOX-Compliance bereit. Die Integration von Risikobereichen im Rahmen eines unternehmensweiten Risikomanagements wird zwar gefordert (Barateiro et al. 2012, S. 1-2; Oh et al. 2007, S. 420; Hoyt und Liebenberg 2011, S. 795; Zoet et al. 2011, S. 456), jedoch nur unzureichend durch Methoden unterstützt. Aufgrund der Überschneidungen zwischen den GRC-Vorgaben erscheint es insbesondere vielversprechend, allgemeine und branchenspezifische Kontrollreferenzmodelle zu entwickeln, die Referenzprozesse zur Umsetzung von GRC-Vorgaben enthalten (siehe Forschungsbedarf 2.2.6 in Tab. 15). Solche Kontrollmodelle müssten eine Übersetzung der normativen Vorgaben in konkrete Kontrollen beinhalten, wobei Standards und Best Practices berücksichtigt werden sollten. In diesem Kontext wäre auch eine Methode zur Ableitung von unternehmensspezifischen Kontrollen aus regulatorischen Vorgaben (z.B. Gesetzen) von großer Bedeutung (siehe Forschungsbedarf 2.2.10 in Tab. 16).

Es existieren vielfältige Management-Methoden mit unterschiedlichen Schwerpunkten im Kontext von GRC. Zum einen sei auf das große Methodenspektrum des Risikomanagements verwiesen (Prokein 2008; Strohmeier 2007; Wolf 2003). Aus Sicht der Integration von GRC können diese Methoden insoweit auch für die Compliance-Sicherung eingesetzt werden, wie sich Compliance-Vorgaben auf die Etablierung

eines Risikomanagement-Systems bzw. internen Kontrollsystems beziehen (Accorsi et al. 2008; Bai et al. 2007; Bai et al. 2012; Barateiro et al. 2012; Setiono et al. 2006). Aus Sicht der Integration sollten solche Ansätze zudem adaptiert werden, um eine Normerfüllung unter Berücksichtigung des Compliance-Risikos zu ermöglichen (siehe Forschungsbedarf 2.2.9 in Tab. 16).

Weitere Schwerpunkte bilden Kennzahlensysteme bzw. das Berichtswesen im Kontext von GRC (Delbaere und Ferreira 2007; Faisst und Buhl 2005; Fill et al. 2007; Gericke et al. 2009a; Goeken und Knackstedt 2008; Goeken und Knackstedt 2009; Panitz et al. 2010). Racz et al. (2010a, S. 5) stellen in diesem Zusammenhang fest, dass in der Praxis zwar ein Bedarf an einem integrierten GRC-Reporting besteht, existierende Lösungen diesen derzeit jedoch nur unzureichend erfüllen. Ebenfalls stellen van der Veen et al. (2011) die Bedeutung einer integrierten Berichterstattung für GRC heraus, ohne konkrete Gestaltungsempfehlungen zu geben. Ein Ansatz, der durch eine gemeinsame Datengrundlage versucht Aspekte der GRC-Teildisziplinen zu verbinden, ist das IEB (Faisst und Buhl 2005, Fill et al. 2007, Goeken und Knackstedt 2009). Das IEB verspricht integrierte Ertrags- und Risikoinformation unter Berücksichtigung regulatorischer Vorgaben. Im Zentrum des IEB (siehe hierzu Fill et al. 2007) steht die Entwicklung einer Datengrundlage für ein integriertes Ertrags- und Risikomanagement. Diese Datengrundlage soll darüber hinaus zur Erfüllung von regulatorischen Anforderungen (wie bspw. aus dem KonTraG) dienen. Konzeptionell unterstützen die entwickelten Methoden ein Reporting der Ertrags- und Risikosituation auf mehreren Hierarchieebenen bis hin zur Gesamtorganisation. Das Konzept dient somit zwar zur Erfüllung konkreter Compliance-Vorgaben und liefert einen methodischen Beitrag für das Risikomanagement im Kontext der wertorientierten Unternehmensfüh-

rung. Ein Überblick über den Status der Erfüllung aller Compliance-Vorgaben und dessen Integration zum Risikomanagement wird jedoch nicht gegeben. Daher besteht der Bedarf zur Entwicklung integrierter Steuerungssysteme für GRC (siehe Forschungsbedarf 2.2.7 in Tab. 16). Wie Panitz et al. (2010) ausführen, zeigt die Balanced Scorecard hierfür vielversprechende Ansatzpunkte.

Zudem werden in verschiedenen Publikationen Reifegradmodelle für GRC oder Teilbereiche von GRC vorgeschlagen (Kranawetter 2009; ITGI 2007; Menzies 2006; Crawford und Crawford 2013[67]; Rath und Sponholz 2009; SAP 2009; Schöler und Zink 2008). Soweit die in den Publikationen dargestellten Management-Ansätze selbst auf eine Integration von GRC abzielen, ist eine solche auch Gegenstand des Reifegradmodells (Kranawetter 2009; Crawford und Crawford 2013; SAP 2009, Schöler und Zink 2008). Es ist jedoch darauf hinzuweisen, dass lediglich in den Ansätzen der SAP (SAP 2009, Schöler und Zink 2008) der Reifegrad hinsichtlich der Integration gemessen wird und nicht auf das GRC-Management als Ganzes abgestellt wird. So beschreibt die SAP (2009) ein Reifegradmodell, das aus den vier Phasen „Blissful Unawareness", „Reactive, Fragmented Implementation", „Consolidation und Operational Excellence" besteht. Hierbei werden die verschiedenen Phasen der Integration von GRC nachvollzogen. Ausgehend von einem Ad-hoc Ansatz (Blissful Unawareness), wird auf der Grundlage von funktionsübergreifenden Teams und einem Inventory für GRC-Projekte (Reactive, Fragmented Implementation) ein integriertes GRC-Framework aufgebaut und die einzelnen GRC-Initiativen priorisiert

[67] In einer Zusatzpublikation zum sogenannten GRC Redbook (OCEG 2009), welches das GRC Capability Modell beschreibt, wird ein Reifegradmodell auf der Grundlage des Capability Modells vorgeschlagen (Crawford und Crawford 2013).

(Consolidation). In der Operational Excellence Phase werden dann Möglichkeiten für geschäftliche Verbesserungen systematisch identifiziert, und es findet eine kontinuierliche Verbesserung statt. Da die Reifegradmodelle auf den GRC-Management-Ansätzen selbst beruhen, existieren hier die gleichen Probleme wie bei den Management-Ansätzen selbst.

Bei den Methoden zur Modellierung von GRC-Informationen lassen sich zwei Bereiche unterscheiden. Zum einen existieren Methoden, welche durch die Modellierung von zusätzlichen Informationen in Geschäftsprozessmodellen im Wesentlichen Informationszwecke erfüllen sollen (siehe Tab. 69). In der Literatur finden sich solche Methoden vornehmlich zu den GRC-Teilbereichen und sind entweder auf das Risikomanagement oder auf Compliance-Aspekte beschränkt. Lediglich Bellamy et al. (2007) verfolgt eine integrierte Visualisierung von Risiko- und Compliance-Informationen, wobei eine Anwendung zum SOX dargestellt wird. Somit ergibt sich der Bedarf, bestehende Methoden um alle Aspekte von GRC zu erweitern, um einen integrierten Ansatz zu unterstützen (siehe Forschungsbedarf 2.2.8 in Tab. 16).

Die Automatisierungsmethoden (siehe Tab. 69), beschäftigen sich ebenfalls weitgehend mit Einzelaspekten aus Risiko- und Compliance-Management und betrachten die Integration somit kaum. Trotzdem sind die Automatisierungsmethoden so allgemein gehalten, dass jegliche Form von Regeln oder Kontrollen automatisiert werden können. Diese können neben Compliance-Vorgaben auch aus dem Risikomanagement oder der Corporate Governance stammen. Somit erscheinen die existierenden Methoden durchaus geeignet einen integrierten GRC-Management-Ansatz zu unterstützen. Die Frage, wie ein integriertes Kontrollmodell aufgebaut werden kann, wird jedoch nicht angesprochen. Insbesondere praxisbezogene Veröffentlichungen zu kommerzi-

ellen Softwareprodukten verwenden zwar GRC als Schlagwort (Götz et al. 2008; Pohlman 2008; PwC 2004; PwC 2007; SAP 2009; Schöler und Zink 2008), jedoch dient dies mehr zur Zusammenfassung unterschiedlicher für GRC relevanter Funktionalitäten als das hierdurch ein integrierter Management-Ansatz für GRC unterstützt würde.[68] Puspasari et al. (2011) entwickeln ein Modell für ein IT-GRC-Informationssystem mit Schwerpunkt auf IT-Risikomanagement in Banken, das jedoch auch nur eingeschränkt die Integration von GRC unterstützt.[69] Die OCEG integriert die informationstechnische Unterstützung in ihren integrierten GRC-Ansatz (OCEG 2009). Hierbei werden mit jeder Aktivität sogenannte Technology Modules bestehend aus „Business Applications", „GRC Core Applications" und „Infrastructure" verknüpft. Insgesamt bleibt der Ansatz mit Business Applications wie Corporate Performance Management oder Infrastructure-Komponenten wie Identity and Access Management jedoch recht generisch. Obwohl die einzelnen Komponenten in den unterschiedlichen Aktivitäten wiederverwendet werden, ist kaum zu erkennen, wie eine Integration im Sinne der Anforderungskategorie unterstützt wird. Der Wiederverwendungsgedanke wird auch von RedMonk (2008) aufgegriffen, wobei sonst keine Integration unterstützt wird. Aus gestaltungsorientierter Sicht existieren folgende Ansatzpunkte um den derzeitigen Forschungsstand hinsichtlich der informationstechnischen Integration zu erweitern. Es besteht der Forschungsbedarf zur Entwicklung eines Referenzmodells für GRC-Software (siehe Forschungsbedarf 2.2.11 in Tab. 16). Ein solches Modell könnte zur Entwicklung einer IT-Unterstützung für ein inte-

[68] Siehe Abschnitt 3.5.2.5.

[69] Das Modell wird ausführlicher im Rahmen der Entwicklung des datenseitigen Modells für das strategische GRC-Management betrachtet (siehe Abschnitt 5.3.1.1).

griertes GRC-Management führen (siehe Forschungsbedarf 2.2.12 in Tab. 16).

3.5.5 Forschungsstand: Geschäftsprozessorientierung

3.5.5.1 Forschungsziel: Beschreiben und Erklären

Zur Geschäftsprozessorientierung im Kontext des strategischen GRC-Managements existiert lediglich eine Veröffentlichung, die das Forschungsziel „Beschreiben und Erklären" verfolgt. Ly et al. (2012) leiten grundsätzliche Anforderungen an GPM-Systeme zur Unterstützung von Geschäftsprozess-Compliance her. Hierbei wird eine formale Spezifikation der Restriktionen (engl. „constraints")[70], eine geeignete Organisation der Restriktionen, die Unterstützung verschiedener Abstraktionsebenen, die Unterstützung der Compliance über den gesamten Prozesslebenszyklus, also unter anderem eine Kombination der Ansätze „compliance by design" und „compliance by detection", die Unterstützung von prozessübergreifenden Szenarien, die Bereitstellung von verständlichem Feedback für die Endanwender, die flexible Handhabung der Restriktionen und die Bereitstellung einer Nachvollziehbarkeit zwischen Compliance-Prüfungen sowie deren Ergebnissen gefordert. Ly et al. (2012) geben somit Hinweise wie das GPM und GPM-bezogene Informationssysteme hinsichtlich einer Unterstützung von Compliance erweitert werden können.

Die Analyse der Anforderung legt insbesondere auf Grundlage der Transaktionskostentheorie verschiedene Ansatzpunkte zur erklärungs-

[70] Mit dem Begriff „semantic constraint" werden im Rahmen des Beitrags konkrete Compliance-Vorgaben bezeichnet, wie sie sich bspw. in Geschäftsregeln (engl. „business rules") und Richtlinien wiederfinden (Ly et al. 2012).

orientierten Forschung in diesem Bereich nahe (siehe Forschungsbedarf 3.1.1 in Tab. 16). Hierbei sollten sowohl die Transaktions- als auch die Produktionskosten, wie bspw. die Kosten der Durchführung von Kontrollen, von GRC betrachtet werden. Zu fragen wäre außerdem, welche Kontextfaktoren die Vorteilhaftigkeit eines geschäftsprozessorientieren Ansatzes beeinflussen (siehe Forschungsbedarf 3.1.2 in Tab. 16). Des Weiteren kann empirische Forschung helfen, geschäftsprozessorientierte Ansätze und Methoden im Kontext von GRC zu evaluieren bzw. den aktuellen Stand von geschäftsprozessorientierten Ansätzen und Methoden in der Praxis zu erfassen und zu bewerten. Letztlich würde dies zu einer Untersuchung der Integration von GPM und GRC-Management führen (siehe Forschungsbedarf 3.1.3 in Tab. 16), für die Ly et al. (2012) einen ersten Schritt gemacht haben.

3.5.5.2 Forschungsziel: Gestalten

Aus gestaltungsorientierter Sicht wird die Geschäftsprozessorientierung im Kontext von GRC auf den verschiedenen Ebenen des GPM diskutiert, wobei bereits eine Vielzahl an Publikationen existiert. Auf der Management-Ebene wird versucht, im Kontext von GRC eine ablauforientierte Sichtweise einzunehmen. Hierauf aufbauend wird aufgrund der Bedeutung der Geschäftsprozesse für die Compliance-Sicherung und Risikosteuerung versucht, die unterschiedlichen Management-Ansätze zusammenzuführen. Marianos et al. (2009) und Sackmann (2008b; 2009) nehmen eine ablauforientierte Sichtweise auf das IT-Risikomanagement ein. Sienou et al. (2008) schlagen eine Integration von Geschäftsprozess- und Risikomanagement auf der Grundlage eines vereinheitlichten Metamodells vor. Barateiro et al. (2012) erweitern die Sichtweise indem die Beziehung zwischen Risikomanagement und dem Enterprise-Architecture-Management behandelt wird. Ebenfalls auf der Basis von Metamodellen schlägt Karagiannis (2008) einen Ansatz zur

Integration von Geschäftsprozess- und Compliance-Management vor. Weitere Arbeiten (DIN 2008a; DIN 2008b) beschreiben geschäftsprozessorientierte Ansätze für das Qualitätsmanagement. Obwohl diese Arbeiten der gestaltungsorientierten Forschung zuzuordnen sind, stellen sie trotzdem einen Ausgangspunkt zur Untersuchung der Beziehung von Geschäftsprozess- und GRC-Management dar, was bereits im Forschungsziel „Beschreiben und Erklären" als Forschungsbedarf identifiziert wurde.

Auf methodischer Ebene wird die Modellierung von GRC-Informationen (Risiken und Kontrollen) in Geschäftsprozessmodellen vorgeschlagen bzw. es werden Methoden zur Spezifikation von Risiken und Kontrollen entworfen und mit Geschäftsprozessen bzw. Geschäftsprozessmodellen in Beziehung gesetzt (Awad et al. 2008; Awad et al. 2009; Bai et al. 2007; Bai et al. 2012; Bräuer et al. 2013; Elgammal et al. 2010b; Fill 2012; Guan und Levitan 2012; El Kharbili et al. 2008b; El Kharbili et al. 2008c; El Kharbili und Pulvermüller 2009; Liu et al. 2007; Lu et al. 2007; Lohmann 2013; Lohmann 2011; Ly et al. 2012; zur Muehlen und Rosemann 2005; Namiri und Stojanovic 2007a; Namiri und Stojanovic 2007b; Namiri und Stojanovic 2008; Sadiq et al. 2007; Schumm et al. 2010; Schultz 2013; Sienou et al. 2008; Strecker et al. 2011; Turetken et al. 2011; Turetken et al. 2012; Rieke und Winkelmann 2008; Weiss und Winkelmann 2011; Weidlich et al. 2010). Hierbei werden sowohl semi-formale Ansätze (Hengmith 2008; zur Muehlen und Rosemann 2005; Schultz 2013; Sienou et al. 2008; Rieke und Winkelmann 2008), welche bspw. die Erweiterung der ereignisgesteuerten Prozesskette (EPK) um Informationen des Risikomanagements thematisieren, als auch formale Ansätze (Awad et al. 2008; Awad et al. 2009; Bai et al. 2007; Bai et al. 2012; Bräuer et al. 2013; Elgammal et al. 2010b; Fill 2012; Guan und Levitan 2012; El Kharbili et al. 2008b; El

Kharbili et al. 2008c; El Kharbili und Pulvermüller 2009; Liu et al. 2007; Lu et al. 2007; Lohmann 2013; Lohmann 2011; Ly et al. 2012; Namiri und Stojanovic 2007a; Namiri und Stojanovic 2007b; Namiri und Stojanovic 2008; Sadiq et al. 2007; Schumm et al. 2010; Turetken et al. 2011; Turetken et al. 2012; Weiss und Winkelmann 2011; Weidlich et al. 2010) verfolgt.

Letztere Ansätze stehen in einem engen Zusammenhang mit der Automatisierung der Compliance-Sicherung und Risikosteuerung auf Basis der Geschäftsprozessmodellierung (Awad et al. 2008; Awad et al. 2009; Bräuer et al. 2013; Elgammal et al. 2010b; El Kharbili et al. 2008b; El Kharbili et al. 2008c; El Kharbili und Pulvermüller 2009; Lu et al. 2007; Liu et al. 2007; Lohmann 2013; Lohmann 2011; Ly et al. 2012; Namiri und Stojanovic 2007a; Namiri und Stojanovic 2007b; Namiri und Stojanovic 2008; Sadiq et al. 2007; Schumm et al. 2010; Turetken et al. 2011; Turetken et al. 2012; Weidlich et al. 2010). Um diese zu erreichen werden Sprachen wie die Business Process Execution Language (El Kharbili et al. 2008b; El Kharbili et al. 2008c; El Kharbili und Pulvermüller 2009; Schumm et al. 2010; Liu et al. 2007) eingesetzt, die auch zur Automatisierung der Geschäftsprozesse selbst dienen kann. Informationssysteme des GPM werden in den Arbeiten kaum explizit thematisiert. Beispielsweise thematisieren Karagiannis (2008) und Fill (2012) die Umsetzung des Metamodells in der Plattform ADOxx®. Caron et al. (2013) sowie Werner et al. (2012; 2013) greifen zwar ebenfalls einen geschäftsprozessorientierten Ansatz auf, nähern sich der Thematik jedoch nicht auf der Grundlage der Geschäftsprozessmodellierung, sondern auf Basis des Business-Process-Mining-Ansatzes. Dieser Ansatz ermöglicht eine Analyse von Geschäftsprozessen, was wie Werner et al. (2012; 2013) feststellen, ebenfalls eine zweckmäßige Modellierung der Geschäftsprozesse notwendig macht. Solche Ansätze

ermöglichen somit eine automatisierte Analyse der Compliance von Geschäftsprozessen und sind im Automatisierungsansatz „compliance by detection“ zu verorten. Weitere Arbeiten greifen konkrete Modellierungsprobleme bspw. im Kontext des Qualitätsmanagement-Standards ISO 9001 (Kim et al. 2007) und zur Compliance im Finanzdienstleistungssektor (Becker et al. 2011a) auf.

Insgesamt wird in den Publikationen eine Vielzahl von methodischen Herangehensweisen und unterschiedliche Aspekte von GRC thematisiert. Hierbei werden an den Reifegrad des GPM der jeweiligen Organisation, die den Ansatz in der Praxis umsetzen möchte, hohe Anforderungen gestellt. So ist für den Ansatz von El Kharbili et al. (El Kharbili et al. 2008b; El Kharbili et al. 2008c; El Kharbili und Pulvermüller 2009) eine vollständige semantische Modellierung der Geschäftsprozesse notwendig, die in der Praxis wohl nur selten gegeben ist. Des Weiteren wird in wenigen Arbeiten eine empirische Evaluierung (Bai et al. 2007; Bai et al. 2012; Fill 2012; Karagiannis 2008; Schultz 2013; Turetken et al. 2011; Turetken et al. 2012; Weiss und Winkelmann 2011) des entwickelten Artefakts durchgeführt. Evaluierungen sind in der gestaltungsorientierten Forschung jedoch notwendig um die Nützlichkeit der Artefakte für die Unternehmenspraxis zu prüfen. Außerdem können sie zur Weiterentwicklung der Artefakte dienen. Letztlich könnten somit auch Vorbedingungen sowie Kontextfaktoren, welche die Nützlichkeit der Artefakte beeinflussen, geklärt werden. Eine Evaluierung im Rahmen eines Einsatzes des Artefakts in der Praxis setzt jedoch eine geeignete Tool-Unterstützung voraus, die für die vorgeschlagenen Methoden nicht ausreichend thematisiert wird. Wiederum Karagiannis (2008) stellt in diesem Zusammenhang heraus, dass Methoden und Tools den gesamten Management-Prozess durchgehend unterstützen sollten. Zur Überwachung der operativen Prozessausführung ist weiterhin eine

Integration in die operativen Systeme (bspw. ERP-Systeme) notwendig. Hiermit stellt sich grundsätzlich die Frage, welche funktionalen Anforderungen GPM-Systeme erfüllen sollten, um auch das GRC-Management unterstützen zu können. Des Weiteren legen Theorien der Informationsverarbeitung (siehe bspw. Information Processing Theory nach Miller 1956) sowie Arbeiten zur Verständlichkeit von Prozessmodellen (Houy et al. 2013; Houy et al. 2014a) nahe, dass die Adressaten von Prozessmodellen nicht beliebig viele Informationen verarbeiten können. Dem Gedanken folgend sollten Prozessmodelle auf besonders wichtige Aspekte fokussieren, die für verschiedene Adressaten unterschiedlich aufbereitet sein können. Aus diesem Grund führen Rieke und Winkelmann (2008) das Konzept der adaptiven Informationsmodellierung ein. Aus der Perspektive des GRC-Managements stellen sich hierbei die Fragen, welches die Adressatengruppen der Informationsmodellierung sind und welche Informationsbedarfe diese haben.

Insgesamt ergeben sich somit insbesondere zwei Forschungsbedarfe, die sich wechselseitig beeinflussen. Zum einen erscheint eine Weiterentwicklung der Methoden zur Geschäftsprozessmodellierung im Kontext von GRC erforderlich, wobei die genannten Aspekte zu berücksichtigen wären (siehe Forschungsbedarf 3.2.1 in Tab. 16). Des Weiteren erscheint eine umfangreichere Evaluierung der entwickelten Artefakte angebracht (siehe Forschungsbedarf 3.2.2 in Tab. 16), was wiederum die Weiterentwicklung unterstützen könnte.

3.5.6 Forschungsstand: Management-Systeme

3.5.6.1 Forschungsziel: Beschreiben und Erklären

Bzgl. der weiteren Management-Systeme ist die Diskussion der Beziehung von GRC zum Controlling, dem Finanzbereich und hiermit im Zusammenhang stehend der internen Revision und der Abschlussprü-

fung, dem GPM sowie dem IT-Management hervorzuheben. Ein weiteres diskutiertes Management-System ist das Wissensmanagement. Die Beziehung von GRC und GPM wurde bereits im Rahmen der Anforderung Geschäftsprozessorientierung besprochen und wird daher nachfolgend nicht betrachtet.

Am umfassendsten wird in der Literatur der Einfluss von GRC auf die IT bzw. das IT-Management diskutiert (Braganza und Desouza 2006; Braganza und Franken 2007; Currie 2008; Damianides 2004; Damiandes 2005; Hall und Liedtka 2007; Karanja und Zaveri 2012; Krell et al. 2009; Knolmayer 2007; Leih 2007; Leih 2006a; Leih 2006b; Leon et al. 2012; Li et al. 2010; Li et al. 2012; Mishra und Weistroffer 2007; Mossanen und Amberg 2008; Mossanen 2010; Mossanen et al. 2010; Panko 2006; Racz et al. 2010a; Schwering 2010; Smith und McKeen 2006; Tanriverdi und Du 2009). Hierbei wird ein weites Themenspektrum diskutiert. Beispiele sind die Auswirkungen von einzelnen GRC-Vorgaben, wie dem SOX auf die IT (Braganza und Desouza 2006; Braganza und Franken 2007; Damianides 2004; Damiandes 2005; Hall und Liedtka 2007; Karanja und Zaveri 2012; Leih 2007; Leih 2006a; Leih 2006b; Leon et al. 2012; Li et al. 2010; Li et al. 2012; Mishra und Weistroffer 2007) oder GRC im Kontext des IT-Outsourcing (Hall und Liedtka 2007; Knolmayer 2007; Mossanen und Amberg 2008; Mossanen et al. 2010; Mossanen 2010). Besonders relevant erscheinen in diesem Bereich Analysen, die die Beziehungen von mehreren Beteiligten untersuchen. Maheshwari et al. (2009) untersuchen die Einstellungen des CFO als Leiter der Finanzberichterstattung und des IT-Leiters bei der Implementierung von regulatorischen Kontrollen. Während die Finanzberichterstattung den Fokus auf das Design der Kontrollen legt, ist für das IT-Management die Implementierung dieser Kontrollen zentral. Braganza und Franken (2007) erweitern den Blick auf den

CFO, den CIO sowie den CEO und Auditoren. Sie kommen zu dem Ergebnis, dass alle Beteiligten Taktiken einsetzen, um die von ihnen gewünschten Resultate zu erzielen. Sie folgern, dass eine Compliance-Initiative dann schwierig sein wird, wenn die Interessen stark voneinander abweichen. Gleichzeitig wird festgestellt, dass der CIO oft nur eine direkte Beziehung zum CFO besitzt und auf dessen Führung angewiesen ist. Der CIO sollte daher aktiv Beziehungen zu den Schlüsselbeteiligten aufbauen, um diese beeinflussen zu können.

Arbeiten zum Controlling im Kontext von GRC stammen von Bhimani (2009), Panitz et al. (2010; 2011) sowie von Werder und Grundei (2006) bzw. Isensee (2008). Bhimani (2009) argumentiert in einem Editorial im Journal „Management Accounting Research", dass die Bedeutung von Controlling insbesondere aufgrund der Transparenzanforderungen im Kontext von GRC steigt. Unternehmen müssen demnach nicht lediglich Kontrollen umsetzen, sondern die Umsetzung gegenüber externen Parteien auch nachweisen können. Panitz et al. (2011) identifizieren „compliance reporting and controlling" als eine Schlüsselkomponente von Compliance-Programmen. Auf der Grundlage einer empirischen Erhebung wird festgestellt, dass bislang überwiegend Checklisten zur Feststellung des Compliance-Status eingesetzt werden. Die gleichen Autoren explorieren zwar in einer früheren Publikation (Panitz et al. 2010) mögliche Anforderungen an ein umfassendes Compliance-Reporting mit Hilfe der Balanced Scorecard, eine Untersuchung, welche Beziehungen zum Controlling bestehen und inwiefern die Controlling-Funktion diese Aufgabe unterstützen kann, wird jedoch nicht vorgenommen. Von Werder und Grundei (2006) sowie Isensee (2008) nehmen für das Organisations-Controlling eine Zweiteilung vor. Diese unterscheidet die Sicherstellung der Einhaltung von organisatorischen Regeln und rechtlichen Vorgaben (Conformance-Controlling) und die

Sicherstellung der Effizienz der Organisation (Performance-Controlling).

Lohre (2009) betrachtet die Möglichkeiten der Internen Revision zur Förderung der IT-Compliance. Hierbei werden drei Modelle der Integration der IT-Compliance in vorhandene Organisationsstrukturen unterschieden. In Modell (1) ist IT-Compliance eine Stabsstelle, in Modell (2) Teil der Rechtsabteilung und in Modell (3) Teil der Internen Revision. Lediglich im Rahmen der Modelle (1) und (2) kann die Interne Revision eine unabhängige Prüfung des Compliance-Programms vornehmen und die Compliance fortlaufend überwachen. Schultz et al. (2012) leiten auf der Grundlage einer Expertenbefragung eine „Concept Map" für relevante Informationen im Kontext von internen und externen Audits her. Hierbei wird deutlich, dass im Kontext von Audits vielfältige Informationen zu Compliance und Risiken benötigt werden.

Wipawayangkool (2009) bezieht sich zwar auf Wissensmanagement-Fähigkeiten im Kontext von Compliance und hebt somit die Bedeutung dieses Management-Systems hervor, es werden jedoch nicht konkret die organisatorischen Beziehungen der Management-Systeme zueinander diskutiert.

Insgesamt betrachten die angeführten Arbeiten somit im Wesentlichen Einzelfragen, wobei entweder lediglich Beziehungen einzelner Personen oder die Beziehung eines einzelnen Management-Systems zu GRC betrachtet werden. Ein umfassendes Bild, welche Aufgaben die einzelnen Management-Systeme im Kontext von GRC übernehmen sollten und welche Abstimmungsbedarfe hierbei entstehen, kann hierdurch nicht gewonnen werden (siehe Forschungsbedarf 4.1.1 in Tab. 17). Zur Beantwortung dieser Fragen sind zwei grundsätzliche Vorgehensweisen denkbar. Zum einen könnte mit entsprechender Standardliteratur die Aufgaben der einzelnen Management-Systeme im Kontext von GRC

definiert und mögliche Überschneidungen identifiziert werden. Zum anderen sind empirische Ansätze möglich, um die gegenwärtige Herangehensweise in der Praxis zu erfassen und so gegebenenfalls Schwachstellen und Verbesserungspotentiale aufzeigen zu können.

3.5.6.2 Forschungsziel: Gestalten

Aus gestaltungsorientierter Sicht stellt sich hinsichtlich der Anforderung „Management-Systeme" die Frage, welche Methoden und Werkzeuge eingesetzt werden können, um eine Abstimmung von GRC mit den weiteren Management-Systemen zu ermöglichen und wie Methoden und Werkzeuge dieser Management-Systeme im Kontext von GRC eingesetzt werden können. Lediglich vier Arbeiten (Grünninger und Jantz 2013; Lohre 2009; von Werder und Grundei 2006; Isensee 2008) beschäftigen sich mit der Anforderung „Management-Systeme" aus Sicht der Gestaltungsorientierung.

Grünninger und Jantz (2013) befassen sich mit Möglichkeiten und Grenzen der Prüfung von Compliance-Management-Systemen, an welchen sich Entscheider in Unternehmen bei der Beauftragung von internen oder externen Prüfungen orientieren können. Die Autoren unterscheiden zwischen Konzeptionsprüfungen, Angemessenheitsprüfungen und Implementierungsprüfungen sowie Wirksamkeits- bzw. Umsetzungsprüfungen des Compliance-Management-Systems. Hiervon abzugrenzen sind wiederum Prozessanalysen bzw. Compliance-Audits hinsichtlich bestimmter Vorgaben. Die Autoren weisen ebenfalls darauf hin, dass solche Prüfungen von unabhängigen Personen, bspw. aus der Internen Revision, erfolgen sollten. In eine ähnliche Richtung geht der Beitrag von Lohre (Lohre 2009), der verschiedene Aspekte herausarbeitet, bei denen die Interne Revision einen Beitrag zur IT-Compliance leisten kann. Einen Beitrag leisten kann die Interne Revision demnach bei risikoorientierten Prüfungen, Ordnungsmäßigkeitsprüfungen, der

Prüfung des IT-Compliance-Programms in seiner Gesamtheit und durch Beobachtung des Umfeldes einschließlich der Früherkennung von Änderungen im IT-Compliance-Umfeld sowie deren Berücksichtigung im IT-Compliance-Programm. Von von Werder und Grundei (2006) bzw. zusammenfassend von Isensee (2008) wird eine Vorgehensweise zum Organisationscontrolling vorgestellt, die das sogenannte Conformance-Controlling einschließt. Hierbei wird ausgehend von der Bestimmung des konkreten Controlling-Gegenstandes und der Festlegung der Sollmaßstäbe, der Ist-Zustand erhoben und mit Hilfe einer Abweichungsanalyse weitere Maßnahmen festlegt. Für die organisatorische Ausgestaltung des Organisations-Controllings wird eine zentrale Einheit ebenso wie dezentrale, in den einzelnen Fachbereichen angesiedelte Einheiten, genannt.

Die Arbeiten zeigen insgesamt zwar auf, wie Methoden der Internen Revision bzw. des Controllings im Kontext von GRC eingesetzt werden können, jedoch wird nicht angesprochen, wie die Aufgaben abgestimmt werden sollten. Aufbauend auf verschiedenen Organisationsmodellen, welche die Management-Systeme in den GRC-Kontext einordnen könnten, sollten hierfür Methoden und Werkzeuge entwickelt werden. Außerdem sind weitere Untersuchungen zum Einsatz der Methoden aus den Management-Systemen im Kontext von GRC denkbar (siehe Forschungsbedarf 4.2.1 in Tab. 17).

3.5.7 Forschungsstand: Automatisierung

3.5.7.1 Forschungsziel: Beschreiben und Erklären

Empirische und theoriebasierte Forschungsansätze zur Anforderungskategorie Automatisierung mit dem Forschungsziel „Beschreiben und Erklären“ existieren in der Literatur, im Gegensatz zu der noch zu betrachtenden Vielzahl an gestaltungsorientierten Ansätzen, nur verein-

zelt. Zieht man die doppelte Bedeutung der IT im Kontext von GRC heran, so kann zwischen Arbeiten zu IT als Gegenstand und Arbeiten zu IT als Unterstützer von GRC unterschieden werden. Veröffentlichungen, die den Einfluss von GRC auf das IT-Management bzw. die IT betrachten[71] kommen insbesondere zu der Feststellung, dass eine Berücksichtigung von GRC für das IT-Management und für die Entwicklung von Informationssystemen von hoher Bedeutung ist. Im Zentrum der Anforderungskategorie Automatisierung stehen jedoch die Unterstützungsmöglichkeiten der IT für die Automatisierung der Compliance-Sicherung und Risikosteuerung sowie die Management-Aufgaben von GRC.

Racz et al. (2010a) kommen in einer ersten Studie zum Stand von GRC-Software in der Praxis ganz allgemein zu dem Schluss, dass GRC-Software dabei hilft, die Nutzenpotentiale von GRC zu verwirklichen. In einer weiteren Studie (Racz et al. 2011c) identifizieren die gleichen Autoren konkrete Nutzenpotentiale. Hierzu gehören unter anderem verbesserte Transparenz, gesteigerte Effizienz, verbessertes Risikomanagement und reduzierte Kosten. In eine ähnliche Richtung gehen die Arbeiten von Krcmar et al. (2011) bzw. Wiesche et al. (2011b), die den Beitrag der IT zum GRC-Management auf der Grundlage der fünf Anwendungsszenarien Widerstandsfähigkeit, Frühwarnung, integriertes Kontrollsystem, automatisierte Überwachung und Integration heterogener Informationsquellen herausarbeiten. In allen Bereichen werden der Beitrag der IT sowie der Einfluss im Sinne von Nutzenpotentialen hergeleitet. Demnach verbessert die IT Informationen zur Entscheidungsfindung, die Überwachung der Kontrolleffizienz, die Sicherstel-

[71] Siehe Forschungsstand zur Anforderungskategorie Management-Systeme (Abschnitt 3.5.6).

lung der Implementierung der Kontrollen und reduziert die Kosten der Datensammlung für Kontrollen bei gleichzeitiger Erhöhung ihrer Vollständigkeit.

Walser et al. (2007, S. 45-51), Christiaanse und Hulstijn (2012) und Oh et al. (2007) betrachten im Gegensatz zu diesen Arbeiten konkret Nutzeneffekte als auch Kosten der Automatisierung, beziehen sich aber nicht auf GRC als integriertes Konzept, sondern auf Einzelaspekte des Compliance- oder Risikomanagements. Oh et al. (2007) entwickeln ein theoretisches Modell, welches die IT als wichtige Komponente zur Unterstützung eines unternehmensweiten Risikomanagements herausstellt. IT unterstützt Risikomanagement in den Bereichen „risk measurement", „risk control" und „risk monitoring" und steigert letztlich die Fähigkeit des Risikomanagements einen Wertbeitrag zu leisten. Christiaanse und Hulstijn (2012) untersuchen den Einfluss der Automatisierung von Kontrollen zur Compliance-Sicherung auf die Kontrollkosten, also die Kosten der Compliance-Sicherung. Automatisierung hat demnach einen zweifachen Effekt auf die Kosten. Zum einen wird durch Kontrollen, die innerhalb der Informationssysteme deviantes Verhalten verhindern, die Wahrscheinlichkeit von solchem Verhalten reduziert. Zum anderen werden durch automatisierte Kontrollen die Nachweise für Prüfungen verbessert. Beide Effekte führen dazu, dass das Compliance-Risiko bzw. das Prüfungsrisiko sinkt, was wiederum dazu führt, dass entsprechende Testaktivitäten des internen Kontrollsystems reduziert werden können. Walser et al. (2007, S. 45-51) stellen in einer empirischen Studie fest, dass Kostenvorteile, welche durch die Automatisierung der Compliance-Sicherung erzielt werden sollen, in der Praxis nicht immer eindeutig festgestellt werden können. Jedoch entstehen durch die Einführung von IT-Werkzeugen Kosten. Gleichzeitig wird von Befragungsteilnehmern auch die Einschätzung geäußert, dass sich

die steigenden Anforderungen an Compliance ohne eine geeignete Tool-Unterstützung kaum erfüllen lassen. Im weiteren Verlauf der Studie werden außerdem konkrete Nutzenpotentiale des IT-Einsatzes im Kontext von Compliance angeführt. Diese basieren jedoch nicht auf empirischen Daten und lassen sich kaum nachvollziehen. Insgesamt erscheint die Untersuchung der Wirtschaftlichkeit der Automatisierung von Kontrollen im Kontext von GRC ein wichtiges zukünftiges Forschungsfeld zu sein. Wie auch die Arbeit von Christiaanse und Hulstijn (2012) zeigt, scheint die Transaktionskostentheorie eine sinnvolle theoretische Perspektive zu sein um Kosten-Nutzen-Betrachtungen vorzunehmen (siehe Forschungsbedarf 5.1.1 in Tab. 17).

Die Frage, welche Kontrolltypen sich überhaupt sinnvoll automatisieren lassen, wird bislang nicht explizit betrachtet und sollte daher zukünftig aufgegriffen werden (siehe Forschungsbedarf 5.1.2 in Tab. 17). Wiesche et al. (2012) untersuchen in diesem Zusammenhang die Frage, wie sich existierende Kontrollmodelle hinsichtlich der Anwendung unterschiedlicher Kontrolltypen, wie Prozess- oder Ergebniskontrollen[72] durch den Einsatz von IT verändern. Die Autoren argumentieren, dass bspw. durch die Automatisierung von Kontrollen oder die Möglichkeit zur Massenauswertung von Daten mittels IT, Verhaltenskontrollen auch implementiert werden können, wenn das Wissen des kontrollierten Prozesses lediglich gering ist.

3.5.7.2 Forschungsziel: Gestalten

Für die Automatisierung existieren bereits Literaturreviews (El Kharbili et al. 2008a; Rinderle-Ma et al. 2008), die zur inhaltlichen Strukturierung

[72] Siehe zur Erläuterung Abschnitt 3.3.3.

herangezogen werden können.[73] Die Automatisierungsmethoden zur Compliance-Sicherung lassen sich, wie bereits ausgeführt[74], in die Ansätze „compliance by design“ und „compliance by detection“ gliedern. Ersteres beinhaltet einen präventiven Ansatz, in welchem Fehlverhalten technisch nicht möglich ist (Sackmann 2008c, S. 43; Sadiq et al. 2007). Rinderle-Ma et al. (2008) unterscheiden hierfür wiederum die Ansätze „compliance by generation“ und „compliance by validation“. Eine weitere verwendete Bezeichnung für diese Unterteilung ist „compliance aware design“ und „post design verification“ (Awad et al. 2008, S. 13; Awad et al. 2009, S. 13). Bei „compliance by generation“ werden nur konforme Prozessmodelle erzeugt und bei „compliance by validation“ werden bestehende Prozessmodelle auf Konformität analysiert. Beide Ansätze zielen somit auf eine Phase ab, die zeitlich vor der Prozessausführung liegt. „Compliance by detection“ stellt im Gegensatz hierzu einen reaktiven Ansatz dar, der Fehlverhalten nach der Prozessausführung identifiziert. Verschiedene Rahmenwerke versuchen zudem durch eine Kombination der Ansätze „compliance by design“ und „compliance by detection“ die Nachteile der Einzelansätze zu reduzieren (El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b; El Kharbili et al. 2008c; Ly et al. 2012; Sackmann 2008c; Sackmann und Kähmer 2008; Sackmann et al. 2008; Turetken et al. 2011; Turetken et al. 2012). Als methodische Grundlage verwenden die Automatisierungsansätze unter anderem Temporale Logik (Ghose und Koliadis 2007; Liu et al. 2007), die Formal Contract Language (Governatori et al. 2006) oder

[73] Eine Zuordnung von Literaturquellen zu den verschiedenen Automatisierungsansätzen findet sich in Tab. 69.

[74] Siehe Abschnitt 3.4.2.5.

ECA-Regeln (Namiri und Stojanovic 2007b, siehe auch Rinderle-Ma et al. 2008).

Außerdem existieren zahlreiche Veröffentlichungen zu kommerziellen Softwarelösungen, die vorwiegend Einzelaspekte der Compliance-Sicherung adressieren (Abrams et al. 2007; Agrawal et al. 2006; Cannon und Byers 2006; Götz et al. 2008; Johnson und Grandison 2007; Kudo et al. 2007; Pohlman 2008; PwC 2007; Ramanathan et al. 2007; RedMonk 2008; SAP 2009; Schöler und Zink 2008). Das GRC Capability Model (OCEG 2009) sowie die Arbeiten von Wiesche et al. (2011a) und RedMonk (2008) versuchen die Auswahl von GRC-Software zu erleichtern, indem eine Einteilung und Zuordnung von Softwarefunktionalitäten im Kontext von GRC erfolgt. Wiesche et al. (2011a) entwickeln bspw. sogenannte „Control Pattern", die auf der Basis von GRC-Vorgaben entwickelt wurden und konkrete Anforderungen an Software zur Unterstützung von GRC beinhalten sollen.

Im Bereich von SOA sind Automatisierungsmethoden vorhanden, die versuchen, die besonderen Aspekte derartiger IT-Architekturen zu berücksichtigen (Birukou et al. 2010; Lotz et al. 2008; Weigand et al. 2011). Weitere Veröffentlichungen beschäftigen sich ebenfalls mit Flexibilität jedoch im Kontext von Workflows (Agrawal et al. 2006; Kittel 2013; Kittel et al. 2013; Sadiq et al. 2005). Accorsi et al. (2011) beschäftigen sich weiterhin mit der Compliance-Zertifizierung im Kontext des Cloud-Computing.

Die Darstellung des Forschungsstandes zeigt, dass im Kontext der Automatisierung der Compliance-Sicherung und Risikosteuerung bereits eine Vielzahl von Ansätzen existieren. Hierbei stehen jedoch methodische Fragen im Vordergrund. Die Ansätze sind vor dem Hintergrund der Unterstützung des gesamten Prozesslebenszyklus (siehe unter anderem Ly et al. 2012) weiterzuentwickeln. Dies erfordert insbe-

sondere eine Kombination der Ansätze „compliance by design“ und „compliance by detection“. Obwohl bereits einige Arbeiten, wie dargestellt, eine solche Kombination aufgreifen, ist bislang nicht ersichtlich, wie sich die Einzelansätze in ein umfassendes Rahmenwerk integrieren lassen (siehe Forschungsbedarf 5.2.1 in Tab. 17). Ein weiterer Kritikpunkt der vorgebracht werden kann ist, dass nur wenige Arbeiten auch eine Anwendung und Evaluierung der entwickelten Artefakte beschreiben. Dies ist erforderlich um die Nützlichkeit des Artefakts in einem realen Praxisumfeld nachzuweisen. Solche Evaluierungen würden ebenso nützliche Hinweise für eine Weiterentwicklung der Methoden liefern (siehe Forschungsbedarf 5.2.2 in Tab. 17).

Nur wenige Arbeiten gehen zudem auf die Vorbedingungen wie den Aufbau des Kontrollmodells bzw. die Frage ein, in welcher Situation der Ansatz „compliance by design“ bzw. „compliance by detection“ zu wählen ist (siehe Forschungsbedarf 5.1.3 in Tab. 17). Allein Sackmann (2008c, S. 43-44) diskutiert diese Frage. Hinsichtlich des Non-Compliance-Risikos bietet „compliance by design“ demnach den Vorteil, dass Normverletzungen präventiv verhindert werden, wohingegen „compliance by detection“ Verletzungen nur nachträglich aufdeckt. Problematisch ist, dass durch die Verhinderung kein Compliance-Nachweis erbracht wird und inhärent weitere reaktive Kontrollen notwendig werden (Sackmann 2008c, S. 43). Die Implementierungskosten sind ein weiterer Einflussfaktor. Im Kontext der Geschäftsprozesse schränkt „compliance by design“ im Gegensatz zu „compliance by detection“ die Flexibilität der Reaktion auf veränderte Prozessanforderungen ein. Außerdem ist die Kenntnis aller möglichen Prozessabläufe und somit eine hohe Strukturiertheit der Geschäftsprozesse erforderlich (Sackmann 2008c, S. 44). Für „compliance by detection“ werden im Bereich der IT-Systeme geeignete Log Files bzw. Reports benötigt.

Weiterhin ist eine maschinenlesbare Beschreibung der aufzudeckenden Systemzustände ebenso wie ein integriertes und einheitliches Datenmodell notwendig (Sackmann 2008c, S. 44). Im Kontext der beteiligten Menschen erhöhen eine GRC-sensible Unternehmenskultur und ein hoher GRC-Ausbildungsstand die Wahrscheinlichkeit von normkonformen Verhalten, was den Verzicht auf die Erzwingung dieses Verhaltens ermöglichen würde. Schnelle Reaktionen auf deviantes Verhalten erfordern außerdem automatisierte Kontrollen. Dieses ist ebenso wie eine hohe Aufdeckungswahrscheinlichkeit und geeignete Anreiz- und Sanktionsmechanismen ein entscheidender Faktor für die abschreckende Wirkung reaktiver Kontrollen.

Letztlich sind Arbeiten zu erwähnen, die sich mit der Unterstützung von GRC-Managementaufgaben durch IT beschäftigen (Puspasari et al. 2011; PwC 2004; Teuteberg und Freundlieb 2009). Hervorzuheben ist hierbei die Arbeit von Puspasari et al. (2011), die auf Basis einer Fallstudie eine IT-Architektur zur Unterstützung eines integrierten GRC-Managements entwirft. Weitere Veröffentlichungen, die der Anforderungskategorie Automatisierung zuzuordnen sind, befassen sich eher allgemein mit den Möglichkeiten der IT zur Unterstützung von GRC. Neben dem bereits in der Anforderungskategorie Geschäftsprozessorientierung angesprochenen Beitrag von Ly et al. (2012), der sich mit dem Einsatz von GPM-Systemen zur Unterstützung von Compliance beschäftigt, sowie den Hinweis auf die „Technology Modules“ im Rahmen der Aktivitäten des GRC Capability Models (OCEG 2009), behandeln ebenso Racz et al. (2011c), Wiesche et al. (2011a) und RedMonk (2008) die Unterstützung von GRC-Management-Aufgaben. Racz et al. (2011c) führen eine erste explorative Studie zum GRC-Software-Markt durch. Die Studie stellt fest, dass die Softwareangebote zu einem hohen Grad auf einem integrierten GRC-Ansatz basieren.

Gleichzeitig sind die Funktionalitäten, die unter dem Schlagwort GRC angeboten werden vielfältig und unterschiedlich, wobei die Studie insgesamt 35 sogenannte „high level" Funktionalitäten identifiziert. Auch die weiteren Arbeiten zeigen, dass bislang kaum untersucht wurde, wie Software, die primär eine operative Normerfüllung bspw. hinsichtlich Zugangskontrollen und Funktionstrennung (engl. segregation of duties) unterstützt, mit Software verknüpft werden kann, die eine Unterstützung von Management-Aufgaben ermöglicht. Auch zeigt sich insgesamt, dass existierende Software stärker operative Aspekte als GRC-bezogene Managementaufgaben unterstützt. Die ist insbesondere deswegen problematisch, da ein Überblick über die Gesamtsituation bzgl. der Risiken und des Compliance-Status wohl nur durch eine IT-gestützte Aggregation der Informationen möglich ist. Die Entwicklung von Informationssystemen zur Unterstützung von Managementaufgaben von GRC stellt somit einen weiteren Forschungsbedarf dar (siehe Forschungsbedarf 5.2.3 in Tab. 17).

3.5.8 Forschungsstand: Flexibilität

3.5.8.1 Forschungsziel: Beschreiben und Erklären

Aus verhaltenswissenschaftlicher Sicht stellen Müller (2007) und Sackmann (2008b) allgemein die Auswirkungen der Flexibilisierung der Geschäftsprozesse und unterstützenden IT auf GRC dar. Müller (2007, S. 109) spricht hierbei zwei Änderungsarten an. Zum einen können Änderungen im Compliance-Umfeld, wie geänderte oder neue Compliance-Vorgaben, auftreten, die hinsichtlich ihrer Auswirkungen auf die Geschäftsprozesse und IT zu untersuchen sind. Auf der anderen Seite sind auch Auswirkungen von Prozess- oder IT-Änderungen auf die Compliance zu betrachten. Sackmann (2008b, S. 1138) geht zusätzlich auf die Herausforderung der Flexibilisierung im Kontext des Risikoma-

nagements ein. Er stellt insbesondere fest, dass eine Notwendigkeit besteht die Geschäftsrisiken genau zu überwachen, da die Risikovermeidung zum Entwurfszeitpunkt der Geschäftsprozesse bei sich ständig ändernden Prozessabläufen und unterstützender IT nur noch begrenzt möglich ist.

Technische Herausforderungen der Flexibilisierung durch SOA und Cloud-Computing werden ebenfalls betrachtet. Im Kontext von SOA entstehen Herausforderungen insbesondere durch die Wiederverwendung und dynamische Orchestrierung der Services (Bindung zur Laufzeit). Hieraus ergibt sich die Problematik, dass bei Änderung des Service-Bestandes verhindert werden muss, dass nicht konforme Services eingebunden werden, was bei einer rein auf finanzielle Aspekte abstellenden Auswahlmethode nicht der Fall wäre. Außerdem besteht das Problem, dass ein Service, der in einem bestimmten Geschäftsprozess zu einem regelkonformen Verhalten führt, nicht notwendigerweise auch in einem anderen Kontext regelkonform ist, da unterschiedliche regulatorische Vorgaben existieren können. Somit lässt sich die Normkonformität eines Services nicht zur Entwicklungszeit mit der Einbindung in ein Repository überprüfen, sondern muss zur Laufzeit bestimmt werden (Loosli 2008). Im Kontext des Cloud-Computings wird ebenfalls auf spezifische Herausforderungen hingewiesen, welche insbesondere auch die Bereiche der Informationssicherheit und des Datenschutzes betreffen (Accorsi et al. 2011, S. 139; Martens und Teuteberg 2011, S. 1). Hierdurch wird eine Zertifizierung der Cloud-Lösung notwendig, die, wenn manuell ausgeführt, eine starke Einschränkung für die durch das Cloud-Computing versprochene schnelle Einsatzbereitschaft von neuen Informationssystemen und damit eine Reduzierung des Flexibilitätspotentials darstellt. GRC-Aspekte scheinen damit sogar zu einem Hemmnis zur Verwendung von Cloud-Lösungen zu

werden (Accorsi et al. 2011, S. 139; Chow et al. 2009). Obwohl diese Forschungsfelder wichtig sind, ist ihre Bedeutung für die Entwicklung eines GRC-Management-Ansatzes eher untergeordnet.

Grundei (2006) diskutiert die Problematik aus Sicht der Organisationsgestaltung und stellt Flexibilität und Compliance gegenüber, wobei Flexibilität durch einen vertrauensbasierten und Compliance durch einen kontrollbasierten Ansatz repräsentiert wird.[75] Hiermit wird der Konflikt zwischen Flexibilität und GRC in den „trade-off" zwischen GRC und strategischer Zielerreichung eingebettet. Böhm et al. (2009) diskutieren den „trade-off" zwischen GRC und der strategischen Zielerreichung im Kontext des Business/IT-Alignements. Unbeachtet bleibt derzeit die Frage, welche konkreten Aspekte bspw. im IT-Management oder in der Organisationsgestaltung konfliktär sind (siehe Forschungsbedarf 6.1.1 in Tab. 17). So wird zwar darauf hingewiesen, dass bspw. der Zeitaufwand bei der Änderung oder Neuimplementierung dadurch steigt, dass ebenfalls mögliche Kontrollen implementiert und getestet werden müssen (Böhm et al. 2009, S. 12), jedoch ist zu vermuten, dass eine Vielzahl solcher Konflikte besteht. Außerdem wird noch nicht der Nutzen dieser Maßnahmen, bspw. im Rahmen einer Risikominimierung berücksichtigt. Ein Verständnis der konkreten Konflikte sowie der hiermit verbundenen Kosten- und Nutzeneffekte ist die Grundlage um eine systematische Methode zu entwickeln, die in der Lage ist, eine Ausbalancierung von GRC und strategischer Zielerreichung zu ermöglichen.

Sowohl Böhm et al. (2009) als auch Grundei (2006) betonen die Bedeutung von situativen Einflüssen auf den „trade-off" zwischen GRC und

[75] Siehe hierzu auch Abschnitt 3.4.2.6.

strategischer Zielerreichung. Methodisch wird hierbei auf das IT Strategic Impact Grid von Nolan und McFarlan (2005) bzw. auf Gresov und Drazin (1997) zurückgegriffen. Beide Ansätze liefern zwar einen ersten Ansatzpunkt zur Analyse des Einflusses von situationsbezogenen Aspekten auf den „trade-off", jedoch stehen detaillierte Untersuchungen noch aus (siehe Forschungsbedarf 6.1.2 in Tab. 17).

3.5.8.2 Forschungsziel: Gestalten

Gestaltungsorientierte Arbeiten zur Herausforderung flexibler Geschäftsprozesse und IT-Systeme im Kontext von GRC existieren in verschiedenen Bereichen. Die Automatisierung der Compliance-Sicherung wird auch im speziellen Kontext von SOA diskutiert. Lotz et al. (2008) stellen einen Ansatz zur Implementierung und kontinuierlichen Bewertung von Kontrollen in einer SOA vor. Die Arbeit von Weigand et al. (2011) beschäftigt sich mit der Automatisierung von Policies zu Geschäftsprozessen in SOA. Lowis (2008) entwickelt eine Methode zur automatisierten Identifikation der Risikowirkung von Schwachstellen in Geschäftsprozessen, deren Ausführung auf Basis von SOA erfolgt. Darüber hinaus werden auch einzelne Probleme wie die Auswahl von Services bei der Prozessausführung unter Berücksichtigung von GRC-Aspekten aufgegriffen (Sackmann et al. 2009) und einer Lösung zugeführt.

Accorsi et al. (2011) sowie Martens und Teuteberg (2011) befassen sich mit spezifischen Problemen von Risiko- und Compliance-Management, welche durch Cloud Computing entstehen. Während Martens und Teuteberg ein Referenzmodell für Risiko- und Compliance-Aspekte im Cloud-Computing entwickeln, konstruieren Accorsi et al. (2011) eine Methode zur automatisierten Compliance-Zertifizierung von Cloud-basierten Geschäftsprozessen. Kittel (2013) und Kittel et al. (2013) sowie Sadiq et al. (2005) betrachten das Thema Flexibilität allgemeiner

ohne sich auf bestimmte Ansätze wie SOA oder Cloud Computing, welche eine Steigerung der Flexibilität versprechen, zu konzentrieren. Kittel (2013) sowie Kittel et al. (2013) schlagen hierbei eine getrennte Modellierung der Geschäftsprozesse und Compliance-Vorgaben vor. Die Compliance-Vorgaben werden als Referenzkontrollprozesse modelliert, wozu ebenfalls Geschäftsprozessmodellierungssprachen als geeignet angesehen werden. Die automatische Integration der Referenzkontrollprozesse erfolgt ad-hoc und situationsabhängig in den Workflowinstanzen, was zu einer Flexibilitätssteigerung gegenüber herkömmlichen Workflowansätzen führen soll.

Neben diesen Herausforderungen werden jedoch auch Chancen der Flexibilisierung in Form von SOA bei der Unterstützung des Compliance-Managements beschrieben. Die „Compliance Oriented Architecture“ (RedMonk 2008) versucht nach eigenen Angaben eine SOA für das Compliance-Management aufzubauen, die verschiedene Compliance-Vorgaben flexibel unterstützen soll. Daher werden generische „core services“ des Compliance-Managements identifiziert. Die Annahme ist, dass diese generischen Services zur Unterstützung verschiedener regulatorischer Vorgaben verwendet werden können. Als Beispiel werden die Gemeinsamkeiten des SOX und des HIPAA angeführt. Den jeweiligen „core services“ werden entsprechende Softwareprodukte zugeordnet. Der Ansatz greift zwar die Grundidee einer flexiblen Kombination von Softwarekomponenten auf, jedoch ist zu bezweifeln, dass die unterschiedlichen Softwareprodukte, die aufgeführt werden, im Sinne einer SOA als Services gekapselt und flexibel orchestriert werden können. Die Arbeit von Birukou et al. (2010) setzt an der gleichen Stelle an. Die Autoren verwenden einen serviceorientierten Ansatz zur Automatisierung des Compliance-Managements. Hierbei werden die Schritte Auswahl der Compliance-Vorgaben, Design von konformen

Geschäftsprozessen, Überwachung der Compliance bei der Prozessausführung und Kommunikation des Compliance-Status betrachtet.

Insgesamt setzt sich diese Anforderungskategorie aus vielfältigen Themen zusammen und konzentriert sich überwiegend auf technische Aspekte. Ein allgemeiner Zugang zum Zielkonflikt zwischen Flexibilität und GRC wird jedoch nicht gefunden. Insbesondere die Auflösung des angesprochenen Zielkonflikts stellt einen wichtigen Forschungsbereich für einen strategischen GRC-Management-Ansatz dar, der aus gestaltungsorientierter Sicht in die Konstruktion einer Methode zur Auflösung dieses Konflikts führen sollte (siehe Forschungsbedarf 6.2.1 in Tab. 17). Des Weiteren erscheinen die im Rahmen des Forschungsziels „Beschreiben und Erklären" angesprochenen Änderungen im GRC-Umfeld ein wichtiges Forschungsfeld zu sein, für welches bislang noch keine methodische Unterstützung existiert. Wünschenswert ist daher die Entwicklung einer Methode zur schnellen Reaktion auf Änderungen von GRC-Vorgaben und Risiken (siehe Forschungsbedarf 6.2.2 in Tab. 17).

3.5.9 Forschungsstand: Menschliche Faktoren

3.5.9.1 Forschungsziel: Beschreiben und Erklären

Im Kontext der Anforderungskategorie „Menschliche Faktoren" existieren eine Vielzahl von überwiegend quantitativ-empirischen Arbeiten zum Forschungsziel „Beschreiben und Erklären". Schwerpunktmäßig wird das Compliance-Verhalten hinsichtlich Vorgaben der Informationssicherheit untersucht (Abraham 2011; Al-Omari et al. 2013; Al-Omari et al. 2012a; Al-Omari et al. 2012b; Aurigemma und Panko 2012; Boss et al. 2009; Bulgurcu et al. 2009; Bulgurcu et al. 2010; D' Arcy et al. 2009; Goo et al. 2012; Guo und Yuan 2012; Herath und Rao 2009; Hu et al. 2012; Hsu 2009; Hu et al. 2011; Johnston und Warken-

tin 2010; Johnston et al. 2010; Lebek et al. 2013; Liang et al. 2013; Lowry und Moody 2013; Milicevic und Goeken 2012; Milicevic und Goeken 2013a; Milicevic und Goeken 2013b; Myyry et al. 2009; Pahnila et al. 2007; Puhakainen und Siponen 2010; Siponen et al. 2006; Siponen und Vance 2010; Son 2011; Spears und Barki 2010; Vance et al. 2012; Yayla 2011). In diesem Kontext ist darauf hinzuweisen, dass für das Thema Informationssicherheit sowohl Aspekte des Compliance- als auch des Risikomanagements relevant sind. Obwohl die Arbeiten größtenteils quantitativ-empirisch ausgerichtet sind, werden unterschiedliche forschungsmethodische Herangehensweisen, theoretischen Perspektiven sowie Konstrukte verwendet. Dies wirft die Frage auf, wie die bisherigen Forschungsergebnisse strukturiert, zusammengefasst und gegebenenfalls aggregiert werden können. Zu diesem Zweck existieren bereits systematische Reviews (Abraham 2011; Aurigemma und Panko 2012; Lebek et al. 2013; Milicevic und Goeken 2012; Milicevic und Goeken 2013a; Milicevic und Goeken 2013b)[76].

Diese Reviews zeigen, dass die empirischen Untersuchungen zu heterogenen Ergebnissen kommen. Es muss festgestellt werden, dass nicht alle Hypothesen, die auf Grundlage von Theorien aufgestellt werden, empirisch signifikant bestätigt werden können. Des Weiteren existieren auch widersprüchliche Ergebnisse (Milicevic und Goeken 2013a, S. 1074). Lebek et al. (2013, S. 2980) identifizieren die Theorien des geplanten Verhaltens bzw. die Theorie des überlegten Handelns, die General Deterrence Theorie, die Theorie der Schutzmotivation sowie das Technology Acceptance Modell als dominierende Theorien bei der Erforschung des Compliance-Verhaltens. Zudem wird festgestellt, dass

[76] Siehe Tab. 59 bis Tab. 63.

ein empirisch-quantitatives Vorgehen dominierend ist. In Übereinstimmung mit den Arbeiten von Milicevic und Goeken (2012; 2013a; 2013b) können hierbei die Kernelemente der Theorie des geplanten Handelns nämlich Einstellung, subjektive Norm und wahrgenommene Verhaltenskontrolle als Kernkonstrukte für das Compliance-Verhalten identifiziert werden. Wie im Rahmen der Analyse der Anforderungskategorie „Menschliche Faktoren" dargestellt wurde, hat die Literatur eine Vielzahl von weiteren Einflussfaktoren auf das Compliance-Verhalten identifiziert. Obwohl die Ergebnisse heterogen sind, stellt Lebek et al. (2013, S. 2986) fest, dass solide Ergebnisse bzgl. der Beziehungen zwischen den Kerndeterminanten des Compliance-Verhaltens bestehen. Weitere Forschung sollte sich daher auf die Identifizierung weiterer Faktoren konzentrieren, wozu auch qualitative Methoden vermehrt eingesetzt werden sollten. Außerdem könnte sich weitere Forschung mit widersprüchlichen Ergebnissen befassen (Milicevic und Goeken 2013b, S. 2986). Zusammenfassend lässt sich jedoch sagen, dass es noch keine vereinheitliche Theorie des Compliance-Verhaltens gibt. Auch ist fragwürdig, ob die Erkenntnisse, die ausschließlich im Kontext der Informationssicherheit erzielt wurden, auch für andere Bereiche uneingeschränkt Gültigkeit besitzen.

Neben dem Bedarf zur Weiterentwicklung und Konsolidierung der bisherigen theoretischen und empirischen Untersuchungen (siehe Forschungsbedarf 7.1.1 in Tab. 17) ist insbesondere eine Zusammenführung der hier gewonnen Erkenntnissen mit den Kontrollen bzw. Kontrolltypen, welche konkret eine Beeinflussung des Verhaltens ermöglichen, angebracht.[77] Obwohl in den existierenden Arbeiten bspw. An-

[77] Zur Einteilung der Kontrolltypen nach Lange (2008) siehe Abschnitt 3.3.3.2.

reiz- und Sanktionsmechanismen auf Basis der General Deterrence Theorie untersucht werden (D' Arcy et al. 2009; Goo et al. 2012; Guo und Yuan 2012; Herath und Rao 2009; Pahnila et al. 2007; Siponen et al. 2006; Siponen und Vance 2010; Son 2011), steht eine Zuordnung der Determinanten des Compliance-Verhaltens zu den möglichen Kontrolltypen und Kontrollen noch aus (siehe Forschungsbedarf 7.1.2 in Tab. 17). Des Weiteren weist Lange (2008, S. 727) darauf hin, dass Kontrollen in der Literatur größtenteils isoliert untersucht werden. Eine Untersuchung der Beziehungen ist jedoch notwendig um zu verstehen, welche Kontrolltypen komplementär eingesetzt werden können und welche in einem konfliktären Verhältnis zueinanderstehen (Lange 2008, S. 711). Dies ist in den dargestellten Arbeiten nicht explizit betrachtet worden (siehe Forschungsbedarf 7.1.3 in Tab. 17).

3.5.9.2 Forschungsziel: Gestalten

Gestaltungsorientierte Arbeiten sind zu den menschlichen Faktoren seltener. Teilweise wird im Rahmen der Management-Ansätze die Berücksichtigung verhaltensspezifischer Aspekte gefordert ohne ein begründetes Konzept für deren Umsetzung zu liefern (siehe Diskussion der Management Ansätze[78] und bspw. Menzies (2006) sowie OCEG (2009)). Lange (2008) liefert aus gestaltungsorientierter Sicht ein Modell zur Strukturierung von Kontrollen, die zur Beeinflussung der Determinanten des Compliance-Verhaltens herangezogen werden können. Hierbei stellt sich die Frage, welche Kontrollen auf welche Verhaltensdeterminanten wirken. Puhakainen und Siponen (2010) betrachten mit einem Trainingskonzept für die Informationssicherheit, das auf Grundlage von Aktionsforschung entwickelt wurde, lediglich einen

[78] Vgl. Abschnitt 3.5.2.7.

Teilaspekt. Aus Sicht eines umfassenden Ansatzes unter Berücksichtigung der analysierten Verhaltensdeterminanten und der möglichen Kontrollen existieren bislang lediglich Ansatzpunkte zur Berücksichtigung menschlicher Faktoren in einen GRC-Management-Ansatz.

Sowohl Milicevic und Goeken (Milicevic und Goeken 2013b, S. 4483) als auch Lebek et al. (2013, S. 2986) stellen fest, dass die vielfältigen Forschungsergebnisse zum Forschungsziel „Beschreiben und Erklären" in der Anforderungskategorie „Menschliche Faktoren" eine geeignete Wissensbasis zur Entwicklung von Artefakten wie Prozessen, Methoden und Informationssystemen, die eine Beeinflussung des Compliance-Verhaltens ermöglichen, darstellen. Basierend hierauf ergibt sich der folgende weitere Forschungsbedarf. Zuerst ist die Entwicklung von Techniken und Methoden zur Verbesserung des Compliance-Verhaltens und der Compliance-Kultur notwendig (siehe Forschungsbedarf 7.2.1 in Tab. 17). Außerdem sollte die Auswahl von Kontrollen, sowie deren Kombination auch aus gestaltungsorientierter Sicht betrachtet werden (siehe Forschungsbedarf 7.2.2 in Tab. 17). Eine solche Methode rückt auch die Bewertung der Folgen einer Compliance-Verletzung sowie die Auswirkung der Kontrollen selbst auf die Geschäftsprozesse in den Fokus. Hierfür ist eine Methode zu Kosten-Nutzen-Betrachtungen von Kontrollen, wie sie bspw. auch im Kontext der Informationssicherheit existieren (Kronschnabl 2010) notwendig (siehe Forschungsbedarf 7.2.3 in Tab. 17).

3.5.10 Zwischenfazit

In den vorangegangenen Abschnitten wurde der Forschungsstand zum strategischen GRC-Management anhand der Anforderungskategorien und zugehörigen Unterkategorien und auf der Grundlage der Forschungsziele „Beschreiben und Erklären" sowie „Gestalten" struktu-

riert aufgearbeitet. Zusätzlich wurde zum Forschungsziel „Gestalten“ auf eine Systematisierung der relevanten Artefakte zurückgegriffen. Eine Zusammenfassung des Forschungsstandes nach Anforderungskategorie und Forschungsziel ist in Tab. 13 und Tab. 14 enthalten. Insgesamt zeigt sich, dass GRC derzeit ein sehr heterogenes Forschungsfeld ist. Die Arbeiten aus den GRC-Teilbereichen stellen zwar wichtige Vorarbeiten zur Entwicklung eines strategischen GRC-Management-Ansatzes dar, erfordern jedoch zur Zusammenführung in einen solchen Ansatz weitere Anstrengungen hinsichtlich der Konsolidierung und Ergänzung. Die Aufarbeitung des Forschungsstandes stellte zugleich den Ausgangspunkt zur Herleitung des weiteren Forschungsbedarfs dar. Hierbei sollten insbesondere solche Forschungsbedarfe herausgearbeitet werden, die zur Entwicklung eines strategischen GRC-Management-Ansatzes führen können.

Tab. 13: Forschungsstand nach Anforderungskategorie und Forschungsziel (1 von 2)

Anf. kat.	Forschungsstand zum Forschungsziel „Beschreiben und Erklären“	Forschungsstand zum Forschungsziel „Gestalten“
Strat. Ausrichtung	Hinsichtlich der strategischen Bedeutung von GRC werden lediglich Teilaspekte analysiert. Der Fokus liegt auf der Untersuchung des Einflusses von GRC auf strategische Ziele bzw. den Unternehmenswert und weniger darauf wie das GRC-Management mit den strategischen Zielen abgestimmt werden könnte. Die Verbindung von GRC mit verschiedenen Nutzenpotentialen basiert überwiegend auf heuristischen Überlegungen. Des Weiteren beziehen sich diese potentiellen Nutzeneffekte auf unterschiedliche Aspekte. Der Zielkonflikt zwischen Geschäfts- und GRC-Zielen wird in der Literatur kaum untersucht. Im Rahmen der Forderung nach einer Orientierung des GRC-Managements an den Interessen der Stakeholder gibt es ebenfalls kaum konkrete Forschungsergebnisse.	Obwohl die strategische Ausrichtung in einigen Management-Ansätzen berücksichtigt wird, existieren kaum Management-Methoden, die eine solche ermöglichen würden. Die Literatur legt nahe, dass strategische Planungsmethoden die strategische Ausrichtung des GRC-Managements unterstützen könnten. Zum Ausbalancieren von GRC und strategischer Zielerreichung existieren derzeit nur sehr grundlegende Ergebnisse, die Hinweise geben, wie situative Aspekte zu berücksichtigen sind. Bzgl. der Unterstützung der Stakeholderorientierung existiert lediglich eine Arbeit (Menzies 2006, 360), welche die Stakeholderanalyse im Kontext von GRC anwendet.
Integration	Für GRC hat sich in Forschung und Praxis noch keine einheitliche Terminologie durchgesetzt. Die Untersuchung der Integration der GRC-Teildisziplinen befindet sich noch auf einem hohen Abstraktionsniveau. Gleiches gilt für die integrierte Erfüllung von GRC-Vorgaben bzw. die Integration über Risikobereiche. In der Literatur wird zudem der Zusammenhang von IT-bezogenen und unternehmensweiten Ansätzen im Kontext von GRC thematisiert, wobei eine ähnliche methodische Vorgehensweise festgestellt und separate Ansätze teilweise in Frage gestellt werden.	Einige Management-Ansätze verfolgen zwar explizit die Integration, weisen jedoch Schwächen auf. Weitere gestaltungsorientierte Publikationen beziehen sich überwiegend entweder auf einzelne GRC-Vorgaben bzw. GRC-Bereiche, wie die Informationssicherheit, das interne Kontrollsystem oder ausschließlich auf Aspekte des Risiko-, des Compliance-Managements oder der IT-Governance. Methoden, die explizit eine Integration ermöglichen, existieren kaum. Des Weiteren wird auch eine integrierte Erfüllung von mehreren GRC-Vorgaben bzw. eine Harmonisierung von Risikobereichen in den Management-Ansätzen bspw. im Kontext von Best Practices angesprochen. Es werden jedoch kaum Hinweise auf eine konkrete Umsetzung gegeben.

Tab. 14: Forschungsstand nach Anforderungskategorie und Forschungsziel (2 von 2)

Anf. kat.	Forschungsstand zum Forschungsziel „Beschreiben und Erklären“	Forschungsstand zum Forschungsziel „Gestalten“
GP-Orientierung	Bislang existiert lediglich eine Veröffentlichung zu Anforderungskategorie Geschäftsprozessorientierung mit dem Forschungsziel „Beschreiben und Erklären“. Ly et al. (2012) geben Hinweise wie das GPM und verwandte Informationssysteme hinsichtlich einer Unterstützung von Compliance erweitert werden können. Weitere Aspekte wie die Vorteile eines geschäftsprozessorientierten Ansatzes werden nicht analysiert.	Aus gestaltungsorientierter Sicht wird die Geschäftsprozessorientierung im Kontext von GRC auf den verschiedenen Ebenen des GPM diskutiert, wobei bereits eine Vielzahl an Publikationen existiert. Es werden hierbei vielfältige methodische Herangehensweisen und unterschiedliche Aspekte von GRC thematisiert. Die Methoden stellen insbesondere an den Reifegrad des GPM der jeweiligen Organisation, welche die Methode in der Praxis anwenden möchte, hohe Anforderungen.
Management-Systeme	Die existierenden Arbeiten zeigen, dass verschiedene Management-Systeme wie Controlling, Finanzberichterstattung, Interne Revision und IT-Management im Kontext von GRC relevant sind, jedoch werden die Beziehungen zu GRC nur in Ausschnitten dargestellt und untersucht. Ein umfassendes Bild der Aufgabenverteilung dieser Management-Systeme im Kontext von GRC lässt sich hieraus nicht ableiten.	Nur wenige Arbeiten beschäftigen sich mit der Anforderungskategorie Management-Systeme aus gestaltungsorientierter Sicht. Die Arbeiten zeigen insgesamt zwar auf wie Methoden der Internen Revision bzw. des Controllings im Kontext von GRC eingesetzt werden können, jedoch wird nicht angesprochen, wie die Aufgaben der unterschiedlichen Management-Systeme im Kontext von GRC miteinander abgestimmt werden können.
Automatisierung	Empirische und theoriebasierte Forschungsansätze zur Anforderungskategorie Automatisierung mit dem Forschungsziel „Beschreiben und Erklären“ existieren nur vereinzelt. Unter anderem werden hierbei Nutzeneffekte einer Automatisierung untersucht bzw. der Frage nachgegangen, welche Kontrolltypen sich überhaupt sinnvoll automatisieren lassen.	Es existiert ein breites Spektrum an Automatisierungsmethoden, die jedoch größtenteils ohne Evaluierung sind. Des Weiteren ist unklar, wie diese in das strategische GRC-Management zu integrieren sind und organisatorisch unterstützt werden können. Auch existieren nur vereinzelt Arbeiten, die sich explizit auf die informationstechnische Unterstützung der Managementaufgaben von GRC beziehen.

Anf. kat.	Forschungsstand zum Forschungsziel „Beschreiben und Erklären“	Forschungsstand zum Forschungsziel „Gestalten“
Flexibilität	Flexibilität wird im Kontext von GRC aus organisatorischer und technischer Sicht diskutiert und in den Konflikt zwischen GRC-Erfordernissen und strategischen Zielerreichungsgrad eingeordnet. Eine detaillierte Analyse dieses Konflikts ist jedoch ausgeblieben. Unbeachtet bleibt derzeit auch die Frage, welche konkreten Aspekte bspw. im IT-Management oder in der Organisationsgestaltung konfliktär sind.	Gestaltungsorientierte Arbeiten zur Herausforderung flexibler Geschäftsprozesse und IT-Systeme im Kontext von GRC existieren in verschiedenen Bereichen. So existieren gestaltungsorientierte Arbeiten, die SOA und Cloud-Computing im Kontext der Compliance-Sicherung berücksichtigen. Es wird jedoch auch auf die Chancen von SOA bei der Entwicklung von Informationssystemen zur Unterstützung des GRC-Managements eingegangen. Durch den technischen Fokus existiert noch keine Methode, die Organisationen beim allgemeinen Konflikt zwischen Flexibilität und GRC unterstützen würde.
Menschliche Faktoren	Es existiert eine Vielzahl empirischer Studien zu menschlichen Faktoren im Kontext von GRC. Die gewonnenen Erkenntnisse werden jedoch noch nicht zur Definition von Maßnahmen, die ein GRC-konformes Verhalten unterstützen, herangezogen bzw. systematisch mit diesen in Verbindung gebracht.	Gestaltungsorientierte Arbeiten sind zu den menschlichen Faktoren seltener. Teilweise wird im Rahmen der Management-Ansätze die Berücksichtigung verhaltensspezifischer Aspekte gefordert ohne ein begründetes Konzept für deren Umsetzung zu liefern. Ein umfassender Ansatz, der die unterschiedlichen Verhaltensdeterminanten durch entsprechende Maßnahmen berücksichtigt, existiert nicht.

Die Bearbeitung des Forschungsbedarfs kann aufgrund des erheblichen Aufwandes nicht im Rahmen eines einzelnen Forschungsvorhabens erfolgen. Vielmehr stellt das strategische GRC-Management ein innovatives Forschungsfeld dar, das durch die Forschungsgemeinschaft bearbeitet werden sollte. Um dies bestmöglich zu unterstützen soll eine Forschungsagenda entwickelt werden, die neben den Forschungsbedarfen weitere Information bspw. zu den inhaltlichen Zusammenhängen zwischen Forschungsbedarfen und der Bedeutung der Forschungsbedarfe enthält. Die aus der Literatur hergeleiteten Forschungsbedarfe erfordern weiterhin eine Evaluierung durch die Forschungsgemeinschaft, was durch eine Delphi-Studie erfolgen soll.

3.6 Zusammenfassung der Ergebnisse als Forschungsagenda

3.6.1 Vorgehensweise zur Entwicklung der Forschungsagenda

Der Themenkomplex des strategischen GRC-Managements ist durch vielfältige Anforderungen geprägt und erstreckt sich auf eine Reihe unterschiedlicher Themen. Der im Folgenden zu entwickelnden Forschungsagenda liegt die Annahme zu Grunde, dass zur Entwicklung eines Management-Ansatzes, alle dargestellten Anforderungen an ein strategisches GRC-Management zu berücksichtigen sind. Die Beantwortung der offenen Forschungsfragen aus den einzelnen Anforderungskategorien soll die Entwicklung eines strategischen GRC-Management-Ansatzes ermöglichen. Die Diskussion der existierenden Management-Ansätze[79] zeigt, dass ein solcher Ansatz bislang noch nicht vorliegt. Die analysierten Ansätze bieten jedoch interessante Möglichkeiten zur Weiterentwicklung, wobei die im Folgenden dargestellte Forschungsagenda berücksichtigt werden sollte.

Der Umfang und die Komplexität von GRC erfordert, dass der weitere Forschungsbedarf strukturiert dargestellt wird. Vorliegend findet diese Strukturierung anhand der Anforderungskategorien und anhand der zentralen Aufgaben von Forschung „Beschreiben und Erklären“ sowie „Gestalten“ statt. Des Weiteren wäre es sinnvoll, den Forschungsbedarf in eine sachlogische Bearbeitungsreihenfolge zu bringen, sowie die Bedeutung der Forschungsbedarfe zu bestimmen um weitere For-

[79] Siehe Abschnitt 3.5.2.

schungsanstrengungen durch eine Priorisierung hinsichtlich eines effizienten Ressourceneinsatzes zu leiten. In den folgenden Abschnitten wird zuerst der weitere Forschungsbedarf zusammengefasst. Anschließend werden Möglichkeiten zur Bestimmung der Bedeutung und Bearbeitungsreihenfolge des Forschungsbedarfs erörtert, bevor die Elemente der Forschungsagenda dargestellt werden.

3.6.2 Zusammenfassung des weiteren Forschungsbedarfs

Der weitere Forschungsbedarf für das strategische GRC-Management wird auf zweifache Weise ermittelt. Zum einen basiert dieser auf der durchgeführten Diskussion des Forschungsstandes. Außerdem wurden die Forschungsarbeiten der GRC-Literatur hinsichtlich des dort explizit aufgeführten weiteren Forschungsbedarfs ausgewertet. Diese Literaturbelege wurden den aus der Diskussion des Forschungsstandes hergeleiteten Forschungsbedarfen zugeordnet und sind in Tab. 15 bis Tab. 17 referenziert. Zur Strukturierung des Forschungsbedarfs werden das verfolgte Forschungsziel („Beschreiben und Erklären" versus „Gestalten") sowie inhaltliche Kriterien in Form der Anforderungskategorien herangezogen.

Die Auswertung des explizit aufgeführten Forschungsbedarfs in Arbeiten aus der Literatursuche wurde wie folgt durchgeführt. In einem ersten Schritt wurden alle relevanten Forschungsarbeiten, die im Rahmen der Literatursuche identifiziert wurden, auf die explizite Nennung von weiterem Forschungsbedarf durchsucht.[80] Soweit explizit aufgeführter Forschungsbedarf identifiziert wurde, ist dieser in eine Microsoft

[80] Gemäß Tab. 1 hatte die durchgeführte Literatursuche 241 gefundene Forschungsbeiträge zum Ergebnis.

Excel™ Arbeitsmappe übernommen worden. Dort wurde dieser analysiert, wobei ermittelt wurde, ob lediglich auf eine Weiterentwicklung der eigenen Forschungsergebnisse verwiesen wurde oder ob weiterer Forschungsbedarf referenziert wurde, der für das strategische GRC-Management von Relevanz ist. War letzteres der Fall, wurde der Literaturbeleg an einem geeigneten Forschungsbedarf referenziert, der in der Analyse des Forschungsstandes gefundenen wurde.[81] Tab. 15 bis Tab. 17 fassen den weiteren Forschungsbedarf für das strategische GRC-Management zusammen.

[81] Da die Forschungsbedarfe eine ausreichende inhaltliche Breite aufweisen, konnten alle hierdurch gefundenen Forschungsbedarfe an Forschungsbedarfen aus der Diskussion des Forschungsstandes referenziert werden, und es mussten keine weiteren Bedarfe ergänzt werden.

Tab. 15: Forschungsbedarf zum strategischen GRC-Management (1 von 3)

Beschreiben und Erklären	Gestalten
Strategische Ausrichtung	
1.1.1 Untersuchung des strategischen Beitrags von GRC in Abhängigkeit der gewählten Strategie (Fokus, Kostenführerschaft, Diversifikation) 1.1.2 Untersuchung der Ressourcen von GRC auf ihre strategische Bedeutung 1.1.3 Untersuchung der theoretischen Grundlagen von Nutzenpotentialen durch GRC 1.1.4 Empirische Exploration und Validierung der Nutzenpotentiale (Abdullah et al. 2010b, S. 555-556; Hoyt und Liebenberg 2011, S. 818; Masli et al. 2010, S. 31; Racz et al. 2010a, S. 6; Spanaki und Papazafeiropoulou 2013, S. 10) 1.1.5 Untersuchung des Einflusses der Erfüllung einzelner Stakeholderinteressen auf den Unternehmenswert	1.2.1 Adaption und Evaluierung strategischer Planungsmethoden für das GRC-Management 1.2.2 Berücksichtigung des „trade-offs“ von GRC und strategischer Zielerreichung in den strategischen Planungsmethoden 1.2.3 Adaption der Stakeholderanalyse für das GRC-Management
Integration	
2.1.1 Empirische Untersuchungen zur Vorteilhaftigkeit des Koordinierungsansatzes für GRC (Koordination mit einer zentralen Organisationseinheit, Integration in die Kernprozesse oder hybrider Ansatz) 2.1.2 Untersuchungen zu Überschneidungen / Synergieeffekten und Inkonsistenzen zwischen den GRC-Disziplinen (Abdullah et al. 2010a, S. 263; Hardy und Leonard 2011, S. 8; Racz et al. 2010a, S. 6; Weiss und Winkelmann 2011, S. 9) 2.1.3 Untersuchung der Integration von GRC-Management und operativen Geschäftsprozessen anhand unterschiedlicher Dimensionen und Rahmenwerke 2.1.4 Untersuchung der Integration von IT-bezogenen und unternehmensweiten Ansätzen (Racz et al. 2010d, S. 6) 2.1.5 Untersuchungen zu Überschneidungen / Synergieeffekten und Inkonsistenzen von einzelnen Vorgaben	2.2.1 Konzeptionelle Modellierung der Elemente und Beziehungen von GRC (Racz et al. 2011b, S. 337; Schultz et al. 2012, S. 12) 2.2.2 Weiterentwicklung existierender Prozessmodelle für ein integriertes Management von GRC (Racz et al. 2010c, S. 14; Racz et al. 2010b, S. 11; Walser et al. 2007, S. 59) 2.2.3 Entwicklung einer Aufbauorganisation für ein strategisches GRC-Management 2.2.4 Integration von GRC ins Methodensystem der Referenzmodellierung (bspw. ARIS, MEMO) (Turetken et al. 2011, S. 11; Vicente und da Silva 2011a, S. 6) 2.2.5 Evaluierungen von existierenden Vorschlägen für die Integration der GRC-Disziplinen 2.2.6 Entwicklung von allgemeinen und branchenspezifischen Kontrollreferenzmodellen (Referenzprozesse) zur integrierten Erfüllung von GRC-Vorgaben (Abdullah et al. 2010a, S. 262; Kittel 2013, S. 978)

Tab. 16: Forschungsbedarf zum strategischen GRC-Management (2 von 3)

Beschreiben und Erklären	Gestalten
Integration (Fortsetzung)	
2.1.6 Untersuchung der Grenzen der integrierten Erfüllung von GRC-Vorgaben 2.1.7 Gibt es „Basiskontrollen", die für jedes Compliance-System relevant sind? Gibt es hierbei Branchenunterschiede? 2.1.8 Vergleich von Standards und Best Practices zu den Teilgebieten von GRC im Hinblick auf Überschneidungen / Synergieeffekte 2.1.9 Untersuchung von Nutzenpotentialen und Schwachstellen von Software, die ein integriertes Management von GRC ermöglicht (Abdullah et al. 2010b, S. 555-556; Racz et al. 2010a, S. 6)	2.2.7 Referenzmodell für integrierte Steuerungssysteme für GRC bspw. auf Grundlage der Balanced Scorecard (Abdullah et al. 2010a, S. 263; Goeken und Knackstedt 2009, S. 367-368; Goeken und Knackstedt 2008, S. 56-57; Panitz et al. 2010, S. 10-11; Racz et al. 2010a, S. 7; Racz et al. 2011b, S. 337) 2.2.8 Erweiterung von Sprachen der Geschäftsprozessmodellierung um alle Aspekte von GRC 2.2.9 Entwicklung von Ansätzen für die Erfüllung von Compliance-Vorgaben unter Berücksichtigung des Compliance-Risikos (Abdullah et al. 2010b, S. 555-556) 2.2.10 Methode zur Ableitung von unternehmensspezifischen Kontrollen aus regulatorischen Vorgaben (z.B. Gesetzen) (Julisch 2008, S. 73; Rinderle-Ma et al. 2008, S. 5; Kittel 2013, S. 980) 2.2.11 Entwicklung eines Referenzmodells für GRC-Software (Racz et al. 2011a, S. 435) 2.2.12 Entwicklung einer IT-Unterstützung für das GRC-Management (Racz et al. 2010c, S. 14)
Geschäftsprozessorientierung	
3.1.1 Untersuchung der Vorteilhaftigkeit eines geschäftsprozessorientierten Ansatzes mit Hilfe der Transaktionskostentheorie (Becker et al. 2012, S. 9) 3.1.2 Untersuchung der Kontextfaktoren, welche die Vorteilhaftigkeit eines geschäftsprozessorientierten Ansatzes unterstützen (Becker et al. 2012, S. 9) 3.1.3 Untersuchung der Integration von Geschäftsprozess- und GRC-Management (Marinos et al. 2009, S. 375; Sackmann 2008a, S. 10; Weiss und Winkelmann 2011, S. 9; Sackmann 2009, S. 151)	3.2.1 Erweiterung von Prozessmodellierungsmethoden um GRC-relevante Aspekte (Abdullah et al. 2010a, S. 263; Becker et al. 2011a, S. 10; Julisch 2008, S. 73; Rinderle-Ma et al. 2008, S. 5; Rozinat und van der Aalst 2008, S. 41; Bai et al. 2012, S. 17; Kittel et al. 2013; Strecker et al. 2011; Sackmann 2009, S. 150) 3.2.2 Evaluierung von Artefakten des GPM (Vorgehensmodelle, Methoden, Werkzeuge) im Kontext von GRC

Tab. 17: Forschungsbedarf zum strategischen GRC-Management (3 von 3)

Beschreiben und Erklären	Gestalten
Management-Systeme	
4.1.1 Wie sollten die GRC-bezogenen Aufgaben über die unterschiedlichen in GRC involvierten Management-Systeme (z.B. Interne Revision, Qualitätsmanagement) verteilt werden und wie kann die verteilte Erfüllung der Aufgaben koordiniert werden? (Bhimani 2009)	4.2.1 Entwicklung von Vorgehensweisen, Methoden und Werkzeugen für die Abstimmung der Management-Systeme
Automatisierung	
5.1.1 Wirtschaftlichkeit der Automatisierung von GRC-Kontrollen: Kosten-Nutzen-Betrachtungen (Transaktionskostentheorie) 5.1.2 Welche Kontrolltypen können automatisiert werden? (Wiesche et al. 2011b, S. 10) 5.1.3 Untersuchungen zu den Vorbedingungen für die Automatisierungsansätze (bspw. verwendetes Kontrollmodell, compliance by design vs. compliance by detection) (Wiesche et al. 2011b, S. 10)	5.2.1 Weiterentwicklung der bestehenden Automatisierungsansätze im gesamten Prozesslebenszyklus (Abdullah et al. 2010a, S. 263; Abdullah et al. 2010b, S. 555-556; El Kharbili et al. 2008a, S. 111-112; Sackmann 2008b, S. 1147; Schumm et al. 2010, S. 12) 5.2.2 Anwendung und Evaluierung der Automatisierungsmethoden 5.2.3 Entwicklung von Informationssystemen zur Unterstützung von Managementaufgaben von GRC (Abdullah et al. 2010a, S. 263; Abdullah et al. 2010b, S. 555-556)
Flexibilität	
6.1.1 Untersuchungen zu einzelnen Konflikten zwischen GRC-Erfordernissen und strategischer Zielerreichung 6.1.2 Untersuchungen zum Einfluss von situationsbezogenen Aspekten auf den „trade-off" zwischen GRC-Erfordernissen und strategischer Zielerreichung	6.2.1 Entwicklung einer methodischen Unterstützung zum Ausbalancieren des „trade-offs" zwischen GRC und strategischer Zielerreichung 6.2.2 Entwicklung von Methoden zur schnellen Reaktion auf Änderungen von GRC-Vorgaben und Risiken (Abdullah et al. 2010b, S. 555-556; Sackmann 2008b, S. 1147; Sackmann et al. 2008, S. 85; Schumm et al. 2010, S. 12)
Menschliche Faktoren	
7.1.1 Erweiterung und Konsolidierung der theoretischen und empirischen Untersuchungen (Abdullah et al. 2010a, S. 263; Ali et al. 2009, S. 11; Bulgurcu et al. 2009; Bulgurcu et al. 2010, S. 543; Cannoy und Salam 2010, S. 131; Grundei und Talaulicar 2009, S. 77; Hu et al. 2007, S. 170; Johnston et al. 2010, S. 11; MacLean und Behnam 2010, S. 1517; Myyry et al. 2009, S. 135; Pahnila et al. 2007, S. 11; Wiesche et al. 2012, S. 10-11; Al-Omari et al. 2012a;	7.2.1 Entwicklung von Techniken und Methoden zur Verbesserung des Compliance-Verhaltens und der Compliance-Kultur 7.2.2 Entwicklung von Methoden zur Auswahl und Kombination von Kontrollen (einschl. Kosten-Nutzen-Betrachtungen) (Kittel 2013, S. 979; Kittel et al. 2013; Wiesche et al. 2011b, S. 10) 7.2.3 Methode zur Bewertung der Folgen einer Compliance-Verletzung einschließlich der Auswirkung von Regeln auf den operati-

Beschreiben und Erklären	Gestalten
Al-Omari et al. 2012b; Abraham 2011) 7.1.2 Untersuchung des Zusammenhangs der Determinanten des Compliance-Verhaltens und der Kontrolltypen 7.1.3 Untersuchungen zum isolierten und kombinierten Einsatz von verschiedenen Kontrolltypen (Lange 2008, S. 724)	ven Geschäftsprozess (Kosten-Nutzen-Betrachtung von Kontrollen) (Sackmann 2008c, S. 45)

3.6.3 Möglichkeiten zur Bestimmung der Bedeutung und Bearbeitungsreihenfolge des weiteren Forschungsbedarfs

Für die Bestimmung der Bedeutung und Bearbeitungsreihenfolge des weiteren Forschungsbedarfs existieren unterschiedliche Möglichkeiten, die in diesem Abschnitt kurz erläutert werden sollen, bevor im Anschluss die relevanten Elemente der Forschungsagenda dargestellt werden. Wie bereits angesprochen soll die Forschungsagenda nicht nur einen strukturierten Überblick über den Forschungsbedarf geben, sondern auch eine Priorisierung von weiteren Forschungsanstrengungen ermöglichen. Die Priorisierung kann auf der einen Seite auf der Bedeutung der Forschungsbedarfe für Forschung und Praxis aufbauen. Auf der anderen Seite kann es aufgrund der Zusammenhänge der Forschungsbedarfe notwendig sein, einen bestimmen Forschungsbedarf vorzuziehen, wenn hierdurch wichtige Vorarbeiten für einen anderen Forschungsbedarf erbracht werden.

Die Bestimmung der Bedeutung Forschungsbedarfe erfolgt vorliegend durch Befragung der Forschungsgemeinschaft im Rahmen einer Delphi-Studie (siehe bspw. Linstone und Turoff 1975). Diese wird im nächsten Kapitel dargestellt. Die Ergebnisse hinsichtlich der Forschungsbedarfe werden im Rahmen der Darstellung der Forschungsagenda vorweggenommen. Die Analyse der Zusammenhänge zwischen den Forschungsbedarfen könnte zwar ebenfalls auf der Grundlage von

Expertenmeinungen erfolgen. Die Delphi-Studie verfolgt diesen Aspekt aus Komplexitätsgründen jedoch nicht. Im Weiteren werden basierend auf eigenen Überlegungen Beziehungen zwischen den Forschungsbedarfen hergestellt. Diese stellen lediglich Vorschläge dar, die im Rahmen eines konkreten Forschungsprojekts erste Hinweise auf Zusammenhänge zu anderen Themen liefern sollen. Im Folgenden werden Möglichkeiten zur Bestimmung der Bearbeitungsreihenfolge diskutiert.

Wie bereits erläutert, soll die Bearbeitung der Forschungsbedarfe zu den Anforderungskategorien zu einem wissenschaftlich-begründeten strategischen GRC-Management-Ansatz führen, welcher somit das Gesamtziel der Forschungsagenda darstellt. Ein strategischer GRC-Management-Ansatz stellt ein Artefakt im Sinne von Hevner et al. (2004, S. 82-84) dar. Die Entwicklung eines strategischen GRC-Management-Ansatzes ist somit im Kontext der gestaltungsorientierten Forschung zu verorten. Wie einleitend bereits dargestellt wurde, ist der Prozess der gestaltungsorientierten Forschung üblicherweise durch die Phasen Analyse, Entwurf, Evaluation und Diffusion charakterisiert (Österle et al. 2010, S. 4-5). Es wird weiter argumentiert, dass gestaltungsorientierte Forschung, auf theoretischem und empirischem Wissen und somit auf Erkenntnissen zum Forschungsziel „Beschreiben und Erklären" aufbauen sollte. Gleichzeitig bieten gestaltungsorientierte Forschungsergebnisse wiederum Ansatzpunkte für Forschung zum Forschungsziel „Beschreiben und Erklären" (Hevner et al. 2004, S. 79-81). Wir unterscheiden daher für die Forschungsagenda die Phasen (1) Problemidentifikation und Wissensaufbereitung, (2) Konstruktion sowie (3) Anwendung und Evaluierung. Ähnliche Unterteilungen werden zur Entwicklung von Forschungsagenden in anderen Bereichen der Wirtschaftsinformatik herangezogen (Martens und Teuteberg 2009;

Meyer und Teuteberg 2012; Ortwerth und Teuteberg 2012; Teuteberg und Wittstruck 2010).

Neben dieser eher grundsätzlichen Überlegung zum Aufbau der Forschungsagenda ist auch die Darstellung der Forschungsagenda von Bedeutung, da dieser Aspekt einen wesentlichen Einfluss auf die Nutzbarkeit der Agenda durch die Forschungsgemeinschaft hat. Verschiedene Publikationen (Martens und Teuteberg 2009; Meyer und Teuteberg 2012; Ortwerth und Teuteberg 2012; Teuteberg und Wittstruck 2010) verwenden hierbei eine Darstellungsvariante (in Meyer und Teuteberg 2012 auch als „Research Roadmap" bezeichnet), die relevante Aspekte einer Forschungsagenda wie die Forschungsziele und Forschungsmethoden den einzelnen zuvor genannten Phasen des Forschungsprozesses zuordnen. Es wird hierbei angenommen, dass der Reifegrad der Forschung beim Durchlaufen der Phasen steigt bis jeweils das Gesamtziel erreicht wird. Eine solche Darstellungsform würde jedoch bei der Anwendung auf das strategische GRC-Management nur sehr eingeschränkt die Zusammenhänge der Forschungsbedarfe berücksichtigen und nahezu trivial wirken. Des Weiteren ist auch davon auszugehen, dass verschiedenen „Forschungsstränge" nebeneinander verfolgt werden können, welches in einer solchen Darstellung ebenso nicht zum Ausdruck kommen würde. Eine weitere Möglichkeit ergibt sich aus dem Umfeld des Projektmanagements (PMI 2008). In diesem Zusammenhang kann eine Forschungsagenda wie ein Projektplan aufgefasst werden, was wiederum Methoden des Projektmanagements bzw. der Projektplanung nahelegt. Insbesondere sind für diese Frage-

stellung der Projektstrukturplan sowie der Projektablaufplan[82] von Bedeutung. Für die Abbildung von Abhängigkeiten zwischen einzelnen Aktivitäten eines Projekts, hier Forschungsbedarfen, eignet sich besonders die Netzplantechnik, die anders als bei den ebenfalls weitverbreiteten Gantt-Charts die logischen Beziehungen der einzelnen Aktivitäten zueinander dargestellt werden (Domschke und Drexl 2011, S. 97-120). Eine solche Darstellung würde sich eignen, um die Zusammenhänge innerhalb einer Anforderungskategorie darzustellen und die Forschungsbedarfe in die Phasen des Forschungsprozesses einzuordnen. Hingegen würde die Abbildung von anforderungskategorieübergreifenden Beziehungen schnell zu einem unübersichtlichen Bild führen. Des Weiteren würde eine solche Darstellung einen linearen Forschungsprozess abbilden und Wechselbeziehungen, bspw. zwischen verhaltenswissenschaftlicher und gestaltungsorientierter Forschung oder zwischen Entwurf und Evaluierung eher vernachlässigen.

Aufgrund der Grenzen anderer Darstellungsformen wurde für die Forschungsagenda zum strategischen GRC-Management die Darstellungsform einer Matrix gewählt, wobei die Forschungsbedarfe gegeneinander abgetragen wurden und dann nach Beziehungen gesucht wurde. Hiermit wird zwar kein konkreter Ablaufplan entworfen, jedoch können Forscher, die einen Forschungsbedarf aufgreifen möchten, diesen relativ einfach in seinen Gesamtzusammenhang einordnen und potentielle notwendige Vorarbeiten erkennen. Wie im nächsten Abschnitt dargestellt wird, werden hierbei den Forschungsbedarfen noch weitere Attri-

[82] Der Begriff Projektstrukturplan (engl. work breakdown structure) bezeichnet im Kern die Zerlegung eines Projektes in seine Elemente wie bspw. Arbeitspakete (PMI 2008, S. 116). Der Projektablaufplan (nach PMI (2008) im Englischen bspw. als „Sequence Activities" bezeichnet) legt hingegen insbesondere die Bearbeitungsreihenfolge fest (PMI 2008, S. 136).

bute, wie die ermittelte Bedeutung des Forschungsbedarfs aus der Delphi-Studie, zugeordnet

3.6.4 Elemente einer Forschungsagenda für das strategische GRC-Management

In diesem Abschnitt wird die Forschungsagenda für ein strategisches GRC-Management dargestellt, welche den Forschungsbedarfen die in Tab. 18 erläuterten Attribute zuordnet.

Tab. 18: Erläuterung der Attribute der Forschungsagenda

Attribut	Erläuterung
Bedeutung	Die Bedeutung der Forschungsbedarfe wurde aus der in Kapitel 4 dargestellten Delphi-Studie übernommen. Dort wurden GRC-Experten in einer dreistufigen Befragung unter anderem um eine Validierung der Liste der Forschungsbedarfe sowie anschließend um die Bewertung ihrer Bedeutung auf einer 6-stufigen-Likert-Skala (1 = unwichtig; 6 = sehr wichtig) gebeten.
Referenz zur Delphi-Studie („Referenz Delphi“)	Die Forschungsbedarfe werden innerhalb der Darstellung der Delphi-Studie mit §1 bis §55 referenziert. Diese Referenz wird auch in der Forschungsagenda wiedergegeben.
Kommentar	Ein Kommentar gibt an, ob der Forschungsbedarf im Rahmen der Evaluierungsrunde der Delphi-Studie entfernt, verändert bzw. kombiniert oder hinzugefügt wurde.
Anforderungskategorie („Anforderung“)	Im Rahmen der Forschungsagenda werden die Forschungsbedarfe den Anforderungskategorien zugeordnet.
Forschungsziel („Ziel“)	Es wird zwischen den Forschungszielen „Beschreiben und Erklären“ (DandE) sowie „Gestalten“ (Design) unterschieden.
Forschungsprozess („Prozess“)	Die Forschungsbedarfe werden den Phasen des generischen Forschungsprozesses zugeordnet. Die Phasen sind (1) Problemidentifikation und Wissensaufbereitung, (2) Konstruktion sowie (3) Anwendung und Evaluierung.
Mögliche Theorien	Den Forschungsbedarfen werden auf der Grundlage der vorangegangenen Analysen mögliche Theorien zugeordnet, die zur Bearbeitung relevant sein könnten (Abkürzungen gemäß Tab. 5).

Attribut	Erläuterung
Nummer	Es wird die Nummer des Forschungsbedarfes gemäß Tab. 15 bis Tab. 17 angegeben. Für Forschungsbedarfe, die im Zuge der Evaluierungsrunde der Delphi-Studie hinzugefügt wurden, werden neue Nummern gebildet. Die Nummer dient zum Referenzieren der Forschungsbedarfe bei der Darstellung der Zusammenhänge.
Forschungsbedarf	Der Forschungsbedarf wird genannt.
Beziehung	Eine inhaltliche Beziehung liegt insbesondere dann vor, wenn das Forschungsergebnis aus einem Forschungsbedarf zur Bearbeitung eines anderen Forschungsbedarfs hilfreich ist. Nach Hevner et al. (2004, S. 78-81) können insbesondere Forschungsbedarfe zum verhaltenswissenschaftlichen Forschungsparadigma (Forschungsziel „Beschreiben und Erklären") notwendiges Wissen für gestaltungsorientierte Forschung liefern. Die Beziehungen können jedoch auch wechselseitig sein, weshalb vorliegend keine Richtung angegeben wird. Darüber hinaus können Forschungsbedarfe unterschiedliche Perspektiven auf den gleichen Forschungsgegenstand darstellen. So können sich Forschungsbedarfe aus verschiedenen Anforderungskategorien auf den gleichen Forschungsgegenstand beziehen, jedoch einen unterschiedlichen Fokus und Schwerpunkt haben, der sich jeweils aus dem Standpunkt der Anforderungskategorie ergibt.

Auf eine Zuordnung möglicher Forschungsmethoden zu den Forschungsbedarfen wird innerhalb der Forschungsagenda verzichtet, da die Auswahl einer Forschungsmethode von verschiedenen Faktoren beeinflusst ist und eine genaue Prüfung erfordert. Für empirische Forschungsvorhaben ist die Auswahl unter anderem auch vom Feldzugang abhängig. In den meisten Fällen ist grundsätzlich eine Vielzahl von Forschungsmethoden anwendbar. Eine Zuordnung aller möglichen Forschungsmethoden würde Forschern kaum bei der Auswahl einer konkreten Forschungsmethode helfen.

Es ist leicht intuitiv nachvollziehbar, dass Forschungsbedarfe insbesondere Zusammenhänge zu anderen Forschungsbedarfen aus der gleichen

Anforderungskategorie aufweisen. Interessant sind jedoch auch Beziehungen zwischen Forschungsbedarfen, die zu verschiedenen Anforderungskategorien gehören. Die Berücksichtigung solcher Beziehungen ermöglicht es, die Anforderungen des strategischen GRC-Managements ganzheitlich zu berücksichtigen. In diesem Sinne kann es auch nützlich sein Ketten von Beziehungen zu verfolgen. Die Forschungsagenda ermöglicht es somit weitere Forschungsanstrengungen im Gesamtkontext des strategischen GRC-Managements zu verorten. Es könnte empfehlenswert sein, Forschungsbedarfe zu priorisieren, welchen zum einen eine hohe Bedeutung zugemessen wird und die zum anderen mit vielen anderen Forschungsbedarfen in Verbindung stehen. Solche Forschungsbedarfe würden durch ihre Bedeutung direkt einen Wert für Forschung und Praxis darstellen und indirekt eine verbesserte Bearbeitung von weiteren Forschungsbedarfen ermöglichen.

Wie bereits ausgeführt wurde die Forschungsagenda mit Hilfe einer Microsoft Excel™ Arbeitsmappe aufgebaut, indem insbesondere im Rahmen einer Matrix die Forschungsbedarfe gegeneinander abgetragen und dann nach Beziehungen gesucht wurde. Aus Darstellungsgründen ist die Matrix nicht Bestandteil dieser Schrift. Es werden an Stelle dessen mehrere Tabellen verwendet. Tab. 19 bis Tab. 22 stellen die Beziehungen der Forschungsbedarfe dar. Tab. 23 bis Tab. 30 beinhalten die Zuordnung der weiteren Attribute zu den Forschungsbedarfen. Eine Verbindung der Tabellen ist durch die Nummer der Forschungsbedarfe wie bspw. 1.1.1, 1.1.2 usw. möglich.

Folgende Beispiele sollen die Tabelle veranschaulichen. Der Forschungsbedarf „Gibt es „Basiskontrollen“ (2.1.7) die für jedes Compliance-System relevant sind? Gibt es hierbei Branchenunterschiede?“ ist gemäß der Bewertung der GRC-Experten, die im Rahmen der Delphi-Studie vorgenommen wurde, mit einer Bedeutung von 5,36 als bedeu-

tendster Forschungsbedarf herausgestellt worden. Wie Tab. 24 zu entnehmen ist, ist der Forschungsbedarf der Kategorie Integration zuzuordnen, verfolgt das Forschungsziel „Beschreiben und Erklären“ und kann in die Phase (1) Problemidentifikation und Wissensaufbereitung eingeordnet werden. Des Weiteren wurden keine Theorien identifiziert, die dessen Untersuchung unterstützen können, da der Forschungsbedarf sich auf eine Auswertung und den Vergleich existierender Kontrollmodelle bezieht. Dieser Forschungsbedarf hat jedoch, wie Tab. 20 zu entnehmen ist, nur eine Beziehung zu drei weiteren Forschungsbedarfen (2.1.5 / 2.1.6 / 2.1.8), die alle aus der Anforderungskategorie Integration stammen und dem Forschungsziel „Beschreiben und Erklären“ zuzuordnen sind. Diese habe wiederum lediglich eine mittlere bzw. niedrige Bedeutung. Es ist demnach davon auszugehen, dass der Forschungsbedarf zwar eine hohe Bedeutung hat, jedoch isoliert einen Bezug zur Anforderungskategorie Integration aufweist. Eine ähnliche Beobachtung lässt sich für den Forschungsbedarf „Methode zur Bewertung der Folgen einer Compliance-Verletzung einschließlich der Auswirkung von Regeln auf den operativen Geschäftsprozess (Kosten-Nutzen-Betrachtung von Kontrollen)“ (7.2.3) machen, der keine Beziehungen zu anderen Forschungsbedarfen aufweist, jedoch aufgrund der Expertenbewertung in der Delphi-Studie als zweitwichtigster Forschungsbedarf identifiziert wurde. Im Unterschied hierzu weist der Forschungsbedarf „Empirische Exploration und Validierung der Nutzenpotentiale“ (1.1.3), der in der Delphi-Studie mit dem Forschungsbedarf 1.1.4 kombiniert wurde und von der Bedeutung den Rang 5 einnimmt, eine Vielzahl von Verbindungen zu Forschungsbedarfen auch aus anderen Anforderungskategorien auf, da hiermit auch Nutzenpotentiale, die sich spezifisch aus der Integration, der Geschäftsprozessorientierung oder der Automatisierung ergeben, in Beziehung stehen. Man kann argumentieren, dass die strategische Perspektive zur Zu-

sammenführung dieser unterschiedlichen Ansatzpunkte für Nutzenpotentiale eine Klammer zur Verfügung stellt und somit dieser Ansatz sowohl von der Bedeutung als auch von den Beziehungen zu anderen Forschungsbedarfen eine hohe Priorität aufweist.

Tab. 19: Forschungsagenda für das strategische GRC-Management (1 von 12)

Nr.	Forschungsbedarf	Beziehung
1.1.1	Untersuchung des strategischen Beitrags von GRC in Abhängigkeit der gewählten Strategie (Fokus, Kostenführerschaft, Diversifikation)	1.1.2 / 1.2.1 / 6.1.1 / 6.1.2 / 6.2.1
1.1.2	Untersuchung der Ressourcen von GRC auf ihre strategische Bedeutung	1.1.1 / 1.2.1 / 6.1.1/ 6.1.2 / 6.2.1
1.1.3	Untersuchung der theoretischen Grundlagen von Nutzenpotentialen durch GRC	1.1.4 / 1.2.1 / 2.1.1 / 2.1.2 / 2.1.3 / 2.1.4 / 2.1.5 / 2.1.8 / 2.1.9 / 3.1.1 / 3.1.2 / 3.1.3 / 5.1.1
1.1.4	Empirische Exploration und Validierung der Nutzenpotentiale	1.1.3 / 1.2.1 / 2.1.1 / 2.1.2 / 2.1.3 / 2.1.4 / 2.1.5 / 2.1.8 / 2.1.9 / 3.1.1 / 3.1.2 / 3.1.3 / 5.1.1
1.1.5	Untersuchung des Einflusses der Erfüllung einzelner Stakeholderinteressen auf den Unternehmenswert	1.2.3
1.1.6	Zusammenspiel von GRC und „normalem“ Management	4.1.1 / 4.2.1
1.2.1	Adaption und Evaluierung strategischer Planungsmethoden für das GRC-Management	1.1.1 / 1.1.2 / 1.1.3 / 1.1.4 / 1.2.2 / 1.2.3 / 6.2.1
1.2.2	Berücksichtigung des „trade-offs“ von GRC und strategischer Zielerreichung in den strategischen Planungsmethoden	1.2.1 / 6.2.1
1.2.3	Adaption der Stakeholderanalyse für das GRC-Management	1.1.5 / 1.2.1 / 6.2.1
2.1.1	Empirische Untersuchungen zur Vorteilhaftigkeit des Koordinierungsansatzes für GRC (Koordination mit einer zentralen Organisationseinheit, Integration in die Kernprozesse oder hybrider Ansatz)	1.1.3 / 1.1.4 / 2.1.2 / 2.1.3 / 2.2.3 / 2.2.5 / 3.1.1 / 3.1.2 / 4.1.1
2.1.2	Untersuchungen zu Überschneidungen / Synergieeffekten und Inkonsistenzen zwischen den GRC-Disziplinen	1.1.3 / 1.1.4 / 2.1.1 / 2.1.8 / 2.2.1 / 2.2.2 / 2.2.3 / 2.2.4 / 2.2.5 / 2.2.9 / 2.2.11 / 2.2.12 / 4.1.1
2.1.3	Untersuchung der Integration von GRC-Management und operativen Geschäftsprozessen anhand unterschiedlicher Dimensionen und Rahmenwerke	1.1.3 / 1.1.4 / 2.1.1 / 2.2.1 / 2.2.4 / 2.2.8 / 2.2.11 / 3.1.1 / 3.1.2
2.1.4	Untersuchung der Integration von IT-bezogenen und unternehmensweiten Ansätzen	1.1.3 / 1.1.4
2.1.5	Untersuchungen zu Überschneidungen / Synergieeffekten und Inkonsistenzen von einzelnen Vorgaben	1.1.3 / 1.1.4 / 2.1.6 / 2.1.7 / 2.1.8 / 2.2.6 / 4.1.1
2.1.6	Untersuchung der Grenzen der integrierten Erfüllung von GRC-Vorgaben	2.1.5 / 2.1.7 / 2.1.8 / 2.2.6 / 4.1.1

Tab. 20: Forschungsagenda für das strategische GRC-Management (2 von 12)

Nr.	Forschungsbedarf	Beziehung
2.1.7	Gibt es „Basiskontrollen“, die für jedes Compliance-System relevant sind? Gibt es hierbei Branchenunterschiede?	2.1.5 / 2.1.6 / 2.1.8
2.1.8	Vergleich von Standards und Best Practices zu den Teilgebieten von GRC im Hinblick auf Überschneidungen / Synergieeffekte	1.1.3 / 1.1.4 / 2.1.2 / 2.1.5 / 2.1.6 / 2.1.7 / 2.2.1 / 2.2.6 / 2.2.7 / 4.1.1
2.1.9	Untersuchung von Nutzenpotentialen und Schwachstellen von Software, die ein integriertes Management von GRC ermöglicht	1.1.3 / 1.1.4 / 2.2.11 / 2.2.12 / 5.2.3
2.2.1	Konzeptionelle Modellierung der Elemente und Beziehungen von GRC	2.1.2 / 2.1.3 / 2.1.8 / 2.2.2 / 2.2.3 / 2.2.4 / 2.2.5 / 2.2.7 / 2.2.8 / 2.2.11 / 2.2.12 / 3.1.3 / 3.2.1 / 4.1.1 / 5.2.3
2.2.2	Weiterentwicklung existierender Prozessmodelle für ein integriertes Management von GRC	2.1.2 / 2.2.1 / 2.2.3 / 2.2.4 / 2.2.5 / 2.2.11 / 2.2.12 / 3.1.3 / 5.2.3
2.2.3	Entwicklung einer Aufbauorganisation für ein strategisches GRC-Management	2.1.1 / 2.1.2 / 2.2.1 / 2.2.2 / 2.2.4 / 2.2.5 / 2.2.11 / 2.2.12 / 3.1.3 / 5.2.3
2.2.4	Integration von GRC ins Methodensystem der Referenzmodellierung (bspw. ARIS, MEMO)	2.1.2 / 2.1.3 / 2.2.1 / 2.2.2 / 2.2.3 / 2.2.5 / 2.2.7 / 2.2.8 / 2.2.11 / 2.2.12 / 3.1.3 / 3.2.1 / 3.2.2 / 5.2.3
2.2.5	Evaluierungen von existierenden Vorschlägen für die Integration der GRC-Disziplinen	2.1.1 / 2.1.2 / 2.2.1 / 2.2.2 / 2.2.3 / 2.2.4 / 2.2.11 / 2.2.12
2.2.6	Entwicklung von allgemeinen und branchenspezifischen Kontrollreferenzmodellen (Referenzprozesse) zur integrierten Erfüllung von GRC-Vorgaben	2.1.5 / 2.1.6 / 2.1.8
2.2.7	Referenzmodell für integrierte Steuerungssysteme für GRC bspw. auf Grundlage der Balanced Scorecard	2.1.8 / 2.2.1 / 2.2.4
2.2.8	Erweiterung von Sprachen der Geschäftsprozessmodellierung um alle Aspekte von GRC	2.1.3 / 2.2.1 / 2.2.4 / 3.2.1/ 5.2.1 / 5.2.3
2.2.9	Entwicklung von Ansätzen für die Erfüllung von Compliance-Vorgaben unter Berücksichtigung des Compliance-Risikos	2.1.2 / 6.1.2 / 6.2.1
2.2.10	Methode zur Ableitung von unternehmensspezifischen Kontrollen aus regulatorischen Vorgaben (z.B. Gesetzen)	---
2.2.11	Entwicklung eines Referenzmodells für GRC-Software	2.1.2 / 2.1.3 / 2.1.9 / 2.2.1 / 2.2.2 / 2.2.3 / 2.2.4 / 2.2.5 / 2.2.12 / 5.1.4 / 5.2.3

Tab. 21: Forschungsagenda für das strategische GRC-Management (3 von 12)

Nr.	Forschungsbedarf	Beziehung
2.2.12	Entwicklung einer IT-Unterstützung für das GRC-Management	2.1.2 / 2.1.9 / 2.2.1 / 2.2.2 / 2.2.3 / 2.2.4 / 2.2.5 / 2.2.11 / 5.1.4 / 5.2.3
2.2.13	Konstruktion von Entwicklungsmethoden für Software/Informationssysteme, welche GRC-Vorgaben berücksichtigen	---
3.1.1	Untersuchung der Vorteilhaftigkeit eines geschäftsprozessorientierten Ansatzes mit Hilfe der Transaktionskostentheorie	1.1.3 / 1.1.4 / 2.1.1 / 2.1.3 / 3.1.2
3.1.2	Untersuchung der Kontextfaktoren, welche die Vorteilhaftigkeit eines geschäftsprozessorientierten Ansatzes unterstützen	1.1.3 / 1.1.4 / 2.1.1 / 2.1.3 / 3.1.1
3.1.3	Untersuchung der Integration von Geschäftsprozess- und GRC-Management	1.1.3 / 1.1.4 / 2.2.1 / 2.2.2 / 2.2.3 / 2.2.4 / 3.2.2
3.2.1	Erweiterung von Prozessmodellierungsmethoden um GRC-relevante Aspekte	2.2.1 / 2.2.4 / 5.2.1 / 2.2.8
3.2.2	Evaluierung von Artefakten des GPM (Vorgehensmodelle, Methoden, Werkzeuge) im Kontext von GRC	2.2.4 / 3.1.3 / 5.2.1 / 5.2.2
4.1.1	Wie sollten die GRC-bezogenen Aufgaben über die unterschiedlichen in GRC involvierten Management-Systeme (z.B. Interne Revision, Qualitätsmanagement) verteilt werden und wie kann die verteilte Erfüllung der Aufgaben koordiniert werden?	1.1.6 / 2.1.1 / 2.1.2 / 2.1.5 / 2.1.6 / 2.1.8 / 2.2.1 / 4.2.1
4.2.1	Entwicklung von Vorgehensweisen, Methoden und Werkzeugen für die Abstimmung der Management-Systeme	1.1.6 / 4.1.1
5.1.1	Wirtschaftlichkeit der Automatisierung von GRC-Kontrollen: Kosten-Nutzen-Betrachtungen (Transaktionskostentheorie)	1.1.3 / 1.1.4 / 5.1.2 / 5.1.3 / 5.2.1 / 5.2.2
5.1.2	Welche Kontrolltypen können automatisiert werden?	5.1.1 / 5.1.3 / 5.2.1 / 5.2.2
5.1.3	Untersuchungen zu den Vorbedingungen für die Automatisierungsansätze (bspw. verwendetes Kontrollmodell, compliance by design vs. compliance by detection)	5.1.1 / 5.1.2 / 5.2.1 / 5.2.2
5.1.4	Verständnis wie Organisationen existierende Werkzeuge und Methoden im Kontext von GRC anwenden	2.2.11 / 2.2.12 / 5.2.1 / 5.2.2 / 5.2.3
5.2.1	Weiterentwicklung der bestehenden Automatisierungsansätze im gesamten Prozesslebenszyklus	2.2.8 / 3.2.1 / 3.2.2 / 5.1.1 / 5.1.2 / 5.1.3 / 5.1.4 / 5.2.2 / 6.2.2
5.2.2	Anwendung und Evaluierung der Automatisierungsmethoden	3.2.2 / 5.1.1 / 5.1.2 / 5.1.3 / 5.1.4 / 5.2.1 / 6.2.2

Tab. 22: Forschungsagenda für das strategische GRC-Management (4 von 12)

Nr.	Forschungsbedarf	Beziehung
5.2.3	Entwicklung von Informationssystemen zur Unterstützung von Managementaufgaben von GRC	2.1.8/ 2.1.9 / 2.2.1 / 2.2.2 / 2.2.3 / 2.2.4 / 2.2.8 / 2.2.11 / 2.2.12/ 5.1.4
6.1.1	Untersuchungen zu einzelnen Konflikten zwischen GRC-Erfordernissen und strategischer Zielerreichung	1.1.1 / 1.1.2 / 6.1.2 / 6.2.1
6.1.2	Untersuchungen zum Einfluss von situationsbezogenen Aspekten auf den „trade-off" zwischen GRC-Erfordernissen und strategischer Zielerreichung	1.1.1 / 1.1.2 / 2.2.9 / 6.1.1 / 6.2.1
6.2.1	Entwicklung einer methodischen Unterstützung zum Ausbalancieren des „trade-offs" zwischen GRC und strategischer Zielerreichung	1.1.1 / 1.1.2 / 1.2.1 / 1.2.2 / 1.2.3 / 2.2.9 / 6.1.1 / 6.1.2
6.2.2	Entwicklung von Methoden zur schnellen Reaktion auf Änderungen von GRC-Vorgaben und Risiken	5.2.1 / 5.2.2
7.1.1	Erweiterung und Konsolidierung der theoretischen und empirischen Untersuchungen	7.1.2 / 7.1.3 / 7.1.4 / 7.1.5 / 7.2.1 / 7.2.2
7.1.2	Untersuchung des Zusammenhangs der Determinanten des Compliance-Verhaltens und der Kontrolltypen	7.1.1 / 7.1.3 / 7.1.4 / 7.1.5 / 7.2.1 / 7.2.2
7.1.3	Untersuchungen zum isolierten und kombinierten Einsatz von verschiedenen Kontrolltypen	7.1.1 / 7.1.2 / 7.1.4 / 7.1.5 / 7.2.1 / 7.2.2
7.1.4	Untersuchung des Einflusses der Unternehmenskultur auf GRC	7.1.1 / 7.1.2 / 7.1.3 / 7.1.5 / 7.2.1 / 7.2.2
7.1.5	Längsschnittsanalyse von Aspekten des Verhaltens und der Kultur im Kontext von GRC (Entwicklung von wenig effektiven zu hoch effektiven GRC-Systemen)	7.1.1 / 7.1.2 / 7.1.3 / 7.1.4 / 7.2.1 / 7.2.2
7.1.6	Untersuchung der notwendigen Ausbildung zur Implementierung, Anwendung und Aufrechterhaltung von GRC (z.B. Wissen von internen vs. Wissen von externen Ressourcen)	---
7.2.1	Entwicklung von Techniken und Methoden zur Verbesserung des Compliance-Verhaltens und der Compliance-Kultur	7.1.1 / 7.1.2 / 7.1.3 / 7.1.4 / 7.1.5 / 7.2.2
7.2.2	Entwicklung von Methoden zur Auswahl und Kombination von Kontrollen (einschl. Kosten-Nutzen-Betrachtungen)	7.1.1 / 7.1.2 / 7.1.3 / 7.1.4 / 7.1.5 / 7.2.1
7.2.3	Methode zur Bewertung der Folgen einer Compliance-Verletzung einschließlich der Auswirkung von Regeln auf den operativen Geschäftsprozess (Kosten-Nutzen-Betrachtung von Kontrollen)	---

Tab. 23: Forschungsagenda für das strategische GRC-Management (5 von 12)

Nr.	Bedeutung	Referenz Delphi	Kommentar	Anforderung	Ziel	Prozess	Mögliche Theorien	Forschungsbedarf
1.1.1	4,36	§42	---	Strategische Ausrichtung	DandE	Phase (1)	MBV, RBV	Untersuchung des strategischen Beitrags von GRC in Abhängigkeit der gewählten Strategie (Fokus, Kostenführerschaft, Diversifikation)
1.1.2	4,14	§49	---	Strategische Ausrichtung	DandE	Phase (1)	RBV	Untersuchung der Ressourcen von GRC auf ihre strategische Bedeutung
1.1.3	5,14	§5	---	Strategische Ausrichtung	DandE	Phase (1)	MBV, RBV, SHT	Untersuchung der theoretischen Grundlagen von Nutzenpotentialen durch GRC
1,1,4	---	---	kombiniert mit 1.1.3	Strategische Ausrichtung	DandE	Phase (1)	MBV, RBV; SHT	Empirische Exploration und Validierung der Nutzenpotentiale
1,1,5	---	---	entfernt	Strategische Ausrichtung	DandE	Phase (1)	SHT	Untersuchung des Einflusses der Erfüllung einzelner Stakeholderinteressen auf den Unternehmenswert
1.1.6	4,77	§22	hinzugefügt	Strategische Ausrichtung	DandE	Phase (1)	---	Zusammenspiel von GRC und „normalem“ Management
1.2.1	4,67	§28	---	Strategische Ausrichtung	Design	Phase (2)	MBV, RBV	Adaption und Evaluierung strategischer Planungsmethoden für das GRC-Management
1.2.2	4,42	§41	---	Strategische Ausrichtung	Design	Phase (2)	MBV, RBV; SHT	Berücksichtigung des „trade-offs“ von GRC und strategischer Zielerreichung in den strategischen Planungsmethoden
1.2.3	4,75	§24	---	Strategische Ausrichtung	Design	Phase (2)	SHT	Adaption der Stakeholderanalyse für das GRC-Management

Tab. 24: Forschungsagenda für das strategische GRC-Management (6 von 12)

Nr.	Bedeutung	Referenz Delphi	Kommentar	Anforderung	Ziel	Prozess	Mögliche Theorien	Forschungsbedarf
2.1.1	5,07	§10	---	Integration	DandE	Phase (1)	TKT	Empirische Untersuchungen zur Vorteilhaftigkeit des Koordinierungsansatzes für GRC (Koordination mit einer zentralen Organisationseinheit, Integration in die Kernprozesse oder hybrider Ansatz)
2.1.2	4,93	§13	---	Integration	DandE	Phase (1)	---	Untersuchungen zu Übersheidungen / Synergieeffekten und Inkonsistenzen zwischen den GRC-Disziplinen
2.1.3	4,62	§32	leicht verändert	Integration	DandE	Phase (1)	---	Untersuchung der Integration von GRC-Management und operativen Geschäftsprozessen anhand unterschiedlicher Dimensionen und Rahmenwerke
2.1.4	4,79	§17	---	Integration	DandE	Phase (1)	---	Untersuchung der Integration von IT-bezogenen und unternehmensweiten Ansätzen
2.1.5	4,71	§25	---	Integration	DandE	Phase (1)	---	Untersuchungen zu Übersheidungen / Synergieeffekten und Inkonsistenzen von einzelnen Vorgaben
2.1.6	4,14	§50	---	Integration	DandE	Phase (1)	---	Untersuchung der Grenzen der integrierten Erfüllung von GRC-Vorgaben
2.1.7	5,36	§1	---	Integration	DandE	Phase (1)	---	Gibt es „Basiskontrollen", die für jedes Compliance-System relevant sind? Gibt es hierbei Branchenunterschiede?

Tab. 25: Forschungsagenda für das strategische GRC-Management (7 von 12)

Nr.	Bedeutung	Referenz Delphi	Kommentar	Anforderung	Ziel	Prozess	Mögliche Theorien	Forschungsbedarf
2.1.8	4,92	§15	---	Integration	DandE	Phase (1)	---	Vergleich von Standards und Best Practices zu den Teilgebieten von GRC im Hinblick auf Überschneidungen / Synergieeffekte
2.1.9	4,43	§38	---	Integration	DandE	Phase (1)	---	Untersuchung von Nutzenpotentialen und Schwachstellen von Software, die ein integriertes Management von GRC ermöglicht
2.2.1	4,15	§48	leicht verändert	Integration	Design	Phase (2)	---	Konzeptionelle Modellierung der Elemente und Beziehungen von GRC
2.2.2	4,43	§39	---	Integration	Design	Phase (2) / Phase (3)	---	Weiterentwicklung existierender Prozessmodelle für ein integriertes Management von GRC
2.2.3	3,93	§54	---	Integration	Design	Phase (2)	TKT	Entwicklung einer Aufbauorganisation für ein strategisches GRC-Management
2.2.4	4,36	§43	---	Integration	Design	Phase (2)	---	Integration von GRC in Methodensystem der Referenzmodellierung (bspw. ARIS, MEMO)
2.2.5	---	---	entfernt	Integration	Design	Phase (3)	---	Evaluierungen von existierenden Vorschlägen für die Integration der GRC-Disziplinen
2.2.6	5,14	§6	---	Integration	Design	Phase (2)	---	Entwicklung von allgemeinen und branchenspezifischen Kontrollreferenzmodellen (Referenzprozesse) zur integrierten Erfüllung von GRC-Vorgaben

Tab. 26: Forschungsagenda für das strategische GRC-Management (8 von 12)

Nr.	Bedeutung	Referenz Delphi	Kommentar	Anforderung	Ziel	Prozess	Mögliche Theorien	Forschungsbedarf
2.2.7	4,79	§18	---	Integration	Design	Phase (2)	---	Referenzmodell für integrierte Steuerungssysteme für GRC bspw. auf Grundlage der Balanced Scorecard
2.2.8	3,93	§55	---	Integration	Design	Phase (2) / Phase (3)	---	Erweiterung von Sprachen der Geschäftsprozessmodellierung um alle Aspekte von GRC
2.2.9	4,57	§33	---	Integration	Design	Phase (2)	---	Entwicklung von Ansätzen für die Erfüllung von Compliance-Vorgaben unter Berücksichtigung des Compliance-Risikos
2.2.10	5,14	§7	---	Integration	Design	Phase (2)	---	Methode zur Ableitung von unternehmensspezifischen Kontrollen aus regulatorischen Vorgaben (z.B. Gesetzen)
2.2.11	4,43	§40	---	Integration	Design	Phase (2)	---	Entwicklung eines Referenzmodells für GRC-Software
2.2.12	4,64	§29	---	Integration	Design	Phase (2)	---	Entwicklung einer IT-Unterstützung für das GRC-Management
2.2.13	4,79	§19	hinzugefügt	Integration	Design	Phase (2)	---	Konstruktion von Entwicklungsmethoden für Software/Informationssysteme, welche GRC-Vorgaben berücksichtigen
3.1.1	4,21	§47	---	GP-Orientierung	DandE	Phase (1)	TKT	Untersuchung der Vorteilhaftigkeit eines geschäftsprozessorientierten Ansatzes mit Hilfe der Transaktionskostentheorie

Tab. 27: Forschungsagenda für das strategische GRC-Management (9 von 12)

Nr.	Bedeutung	Referenz Delphi	Kommentar	Anforderung	Ziel	Prozesss	Mögliche Theorien	Forschungsbedarf
3.1.2	4,07	§52	---	GP-Orientierung	DandE	Phase (1)	TKTe	Untersuchung der Kontextfaktoren, welche die Vorteilhaftigkeit eines geschäftsprozessorientierten Ansatzes unterstützen
3.1.3	4,71	§26	---	GP-Orientierung	DandE	Phase (1)	---	Untersuchung der Integration von Geschäftsprozess- und GRC-Management
3.2.1	---	---	kombiniert mit 3.2.2	GP-Orientierung	Design	Phase (2) / Phase (3)	---	Erweiterung von Prozessmodellierungsmethoden um GRC-relevante Aspekte
3.2.2	4,5	§37	---	GP-Orientierung	Design	Phase (3)	---	Evaluierung von Artefakten des GPM (Vorgehensmodelle, Methoden, Werkzeuge) im Kontext von GRC
4.1.1	4	§53	---	Management-Systeme	DandE	Phase (1)	TKT, InT	Wie sollten die GRC-bezogenen Aufgaben über die unterschiedlichen in GRC involvierten Management-Systeme (z.B. Interne Revision, Qualitätsmanagement) verteilt werden und wie kann die verteilte Erfüllung der Aufgaben koordiniert werden?
4.2.1	4,31	§45	---	Management-Systeme	Design	Phase (2)	TKT, InT	Entwicklung von Vorgehensweisen, Methoden und Werkzeugen für die Abstimmung der Management-Systeme
5.1.1	4,57	§34	---	Automatisierung	DandE	Phase (1)	TKT	Wirtschaftlichkeit der Automatisierung von GRC-Kontrollen: Kosten-Nutzen-Betrachtungen (Transaktionskostentheorie)

Tab. 28: Forschungsagenda für das strategische GRC-Management (10 von 12)

Nr.	Bedeutung	Referenz Delphi	Kommentar	Anforderung	Ziel	Prozess	Mögliche Theorien	Forschungsbedarf
5.1.2	5,21	§4	---	Automatisierung	DandE	Phase (1)	PAT, OCT	Welche Kontrolltypen können automatisiert werden?
5.1.3	5,14	§8	---	Automatisierung	DandE	Phase (1)	PAT, OCT	Untersuchungen zu den Vorbedingungen für die Automatisierungsansätze (bspw. verwendetes Kontrollmodell, compliance by design vs. compliance by detection)
5.1.4	5,29	§3	hinzugefügt	Automatisierung	DandE	Phase (1)	---	Verständnis wie Organisationen existierende Werkzeuge und Methoden im Kontext von GRC anwenden
5.2.1	4,79	§20	---	Automatisierung	Design	Phase (2)	---	Weiterentwicklung der bestehenden Automatisierungsansätze im gesamten Prozesslebenszyklus
5.2.2	5	§12	---	Automatisierung	Design	Phase (3)	---	Anwendung und Evaluierung der Automatisierungsmethoden
5.2.3	4,64	§30	---	Automatisierung	Design	Phase (2)	---	Entwicklung von Informationssystemen zur Unterstützung von Managementaufgaben von GRC
6.1.1	4,31	§46	---	Flexibilität	DandE	Phase (1)	PAT, SteT	Untersuchungen zu einzelnen Konflikten zwischen GRC-Erfordernissen und strategischer Zielerreichung

Tab. 29: Forschungsagenda für das strategische GRC-Management (11 von 12)

Nr.	Bedeutung	Referenz Delphi	Kommentar	Anforderung	Ziel	Prozess	Mögliche Theorien	Forschungsbedarf
6.1.2	4,08	§51	---	Flexibilität	DandE	Phase (1)	PAT, SteT	Untersuchungen zum Einfluss von situationsbezogenen Aspekten auf den „trade-off“ zwischen GRC-Erfordernissen und strategischer Zielerreichung
6.2.1	4,36	§44	---	Flexibilität	Design	Phase (2)	PAT, SteT	Entwicklung einer methodischen Unterstützung zum Ausbalancieren des „trade-offs“ zwischen GRC und strategischer Zielerreichung
6.2.2	4,86	§16	---	Flexibilität	Design	Phase (2)	---	Entwicklung von Methoden zur schnellen Reaktion auf Änderungen von GRC-Vorgaben und Risiken
7.1.1	5,07	§11	---	Menschliche Faktoren	DandE	Phase (1)	TÜH, TGV; GDT, TAM; ISM; TRE; DT, PAT, SteT	Erweiterung und Konsolidierung der theoretischen und empirischen Untersuchungen
7.1.2	4,71	§27	---	Menschliche Faktoren	DandE	Phase (1)	siehe Theorien zu 7.1.1	Untersuchung des Zusammenhangs der Determinanten des Compliance-Verhaltens und der Kontrolltypen

Tab. 30: Forschungsagenda für das strategische GRC-Management (12 von 12)

Nr.	Bedeutung	Referenz Delphi	Kommentar	Anforderung	Ziel	Prozess	Mögliche Theorien	Forschungsbedarf
7.1.3	4,64	§31	---	Menschliche Faktoren	DandE	Phase (1)	Insb. PAT, OCT	Untersuchungen zum isolierten und kombinierten Einsatz von verschiedenen Kontrolltypen
7.1.4	4,93	§14	hinzugefügt	Menschliche Faktoren	DandE	Phase (1)	siehe Theorien zu 7.1.1	Untersuchung des Einflusses der Unternehmenskultur auf GRC
7.1.5	4,57	§35	hinzugefügt	Menschliche Faktoren	DandE	Phase (1)	siehe Theorien zu 7.1.1	Längsschnittsanalyse von Aspekten des Verhaltens und der Kultur im Kontext von GRC (Entwicklung von wenig effektiven zu hoch effektiven GRC-Systemen)
7.1.6	4,77	§23	hinzugefügt	Menschliche Faktoren	DandE	Phase (1)	siehe Theorien zu 7.1.1	Untersuchung der notwendigen Ausbildung zur Implementierung, Anwendung und Aufrechterhaltung von GRC (z.B. Wissen von internen vs. Wissen von externen Ressourcen)
7.2.1	5,14	§9	---	Menschliche Faktoren	Design	Phase (2)	siehe Theorien zu 7.1.1	Entwicklung von Techniken und Methoden zur Verbesserung des Compliance-Verhaltens und der Compliance-Kultur
7.2.2	4,79	§21	---	Menschliche Faktoren	Design	Phase (2)	---	Entwicklung von Methoden zur Auswahl und Kombination von Kontrollen (einschl. Kosten-Nutzen-Betrachtungen)
7.2.3	5,36	§2	---	Menschliche Faktoren	Design	Phase (2)	---	Methode zur Bewertung der Folgen einer Compliance-Verletzung einschließlich der Auswirkung von Regeln auf den operativen Geschäftsprozess (Kosten-Nutzen-Betrachtung von Kontrollen)

3.7 Grenzen des Literaturreviews

Die Grenzen des Literaturreviews sollen anhand der Bereiche Literatursuche, Herleitung der Anforderungskategorien, Analyse der Anforderungskategorien, Diskussion des Forschungsstandes und Ableitung des weiteren Forschungsbedarfs sowie Herleitung der Forschungsagenda diskutiert werden. Zudem ist anzumerken, dass Literaturreviews mit den bekannten Problemen qualitativer Forschung konfrontiert sind, da eine Reihe unterschiedlicher vor allem qualitativer Forschungsmethoden angewendet werden. Um diesen Problemen zu begegnen wurde der Forschungsprozess so transparent wie möglich beschrieben. Hierdurch soll die Nachvollziehbarkeit erhöht und eventuell vorhandene Subjektivität offengelegt werden (Brühl und Buch 2006, S. 37; Wrona 2006, S. 207). Außerdem wurde vor der Durchführung jedes Forschungsschrittes die gewählte Vorgehensweise expliziert, was im Sinne einer Handlungs- und Denkanweisung zur Erhöhung der Zuverlässigkeit beitragen sollte (Brühl und Buch 2006, S. 37; Flick 2000, S. 170).

Aufgrund der Vielzahl an Publikationen ist die systematische Suche nach relevanter Literatur von hoher Bedeutung. Gleichzeitig ist es kaum möglich, alle Veröffentlichungen zu einem Themengebiet zu berücksichtigen. In dieser Arbeit wird daher der Empfehlung gefolgt, insbesondere qualitativ hochwertige Veröffentlichungen zu berücksichtigen. Ob ein Beitrag relevant für das Forschungsziel ist, bleibt trotzdem eine Entscheidung, die nicht vollständig unabhängig vom Standpunkt des Autors ist. In diesem Beitrag wurde versucht, die Literatursuche transparent darzustellen um die Nachvollziehbarkeit zu erhöhen. Auch erscheint es aufgrund der Vielzahl an berücksichtigten Arbeiten unwahrscheinlich, dass wichtige Forschungsbereiche vollständig unberücksichtigt geblieben sind.

Bei der Herleitung der Anforderungskategorien wurde die Interkoderreliabilität nicht bestimmt. Unter Reliabilität wird die Verlässlichkeit der Messung bzw. hier der Kodierung verstanden. Interkoderreliabilität meint die Unterschiede zwischen mindestens zwei verschiedenen Kodierern (Atteslander 2010, S. 206). Zur Messung der Interkoderreliabilität liegen verschiedene Koeffizienten vor (Atteslander 2010, S. 206; Craig 1981; Krippendorff 2004, S. 221-256; Scott 1955). Da die vorliegende Schrift Teil eines Promotionsvorhabens ist, stand kein weiterer Forscher zur Verfügung. Die Analyse der Anforderungskategorien und Herleitung der Anforderungen ist somit ebenfalls nicht vollständig unbeeinflusst vom Standpunkt des Autors. Es ist jedoch anzumerken, dass die qualitative Inhaltsanalyse eine anerkannte Forschungsmethode ist, der gefolgt wurde. Zur Herleitung der Anforderungen wurden zudem die identifizierten Theorien aus der GRC-Literatur eingesetzt.

Die Analyse des Forschungsstandes ist aufgrund der Vielzahl an berücksichtigten Publikationen auf einem hohen Abstraktionsniveau. Es wäre daher sinnvoll, ausgehend von dem hier dargestellten Überblick, detaillierte Analysen des Forschungsstandes zu den einzelnen Anforderungskategorien vorzunehmen. Die gewählte Betrachtungsebene ist jedoch für die Herleitung des Forschungsbedarfs im Hinblick auf die Entwicklung eines strategischen GRC-Management-Ansatzes adäquat. Des Weiteren ist darauf hinzuweisen, dass zur sinnvollen Strukturierung und Erhaltung von Übersichtlichkeit eine Trennung zwischen der Bewertung der existierenden Management-Ansätze anhand der Anforderungen und der Darstellung des Forschungsstandes je Anforderungskategorie stattgefunden hat.

In diesem Kapitel werden weiterhin besonders relevante Forschungsbedarfe zu den einzelnen Anforderungskategorien abgeleitet. Es ist darauf hinzuweisen, dass die im Rahmen der Forschungsagenda be-

stimmten Beziehungen auf sachlogischen Überlegungen beruhen, die lediglich erste Hinweise für Forscher darstellen, die den jeweiligen Forschungsbedarf aufgreifen wollen. Wie bereits ausgeführt, werden die Beziehungen aus Komplexitätsgründen nicht innerhalb der Delphi-Studie evaluiert. Eine Einbeziehung einer solchen Evaluierung der Beziehungen hätte den Zeitaufwand für die Befragungsteilnehmer signifikant erhöht.

Insgesamt besteht auch weiterer Forschungsbedarf hinsichtlich der Validität im Sinne der Glaubwürdigkeit (Brühl und Buch 2006, S. 40; Lincoln und Guba 1985, S. 296) der Analysen. Diese Glaubwürdigkeit soll durch eine anschließende Delphi-Studie für bedeutsame Aspekte wie die Anforderungen und den Forschungsbedarf mittels der Konsensbildung zwischen Experten gestärkt werden.

3.8 Zwischenfazit

In diesem Kapitel wurden anhand eines umfassenden Literaturreviews relevante Theorien identifiziert und Anforderungskategorien an einen strategischen GRC-Management-Ansatz hergeleitet. Diese Anforderungskategorien wurden anhand von relevanten Theorien in konkrete Anforderungen verdichtet um eine Synthese der bisherigen Erkenntnisse zu ermöglichen. Des Weiteren wurde der Forschungsstand zu den Anforderungskategorien diskutiert, wobei auch existierende Management-Ansätze anhand der Anforderungen bewertet wurden. Die Diskussion des Forschungsstandes führt darüber hinaus zur Identifikation weiterer Forschungsbedarfe. Diese wurden im Rahmen einer Forschungsagenda strukturiert. Die Forschungsagenda bietet Forschern relevante Informationen zur Bearbeitung der einzelnen Forschungsbedarfe und legt insbesondere ein Augenmerk auf die Bedeutung und Beziehungen der Forschungsbedarfe um eine Priorisierung zu ermögli-

chen. Wie bereits ausgeführt, sollen die hier erzielten Forschungsergebnisse im Rahmen einer Delphi-Studie weiterentwickelt und evaluiert werden.

Das Kapitel leistet somit einen wichtigen Beitrag zur Erreichung des Forschungsziels dieser Arbeit, welches in der Grundlegung eines allgemeinen Verständnisses für ein strategisches GRC-Management liegt. Insbesondere erfolgte in diesem Kapitel eine strukturierte Aufarbeitung der relevanten Veröffentlichungen zum strategischen GRC-Management. Die Anforderungskategorien zeigen die relevanten Aspekte für das strategische GRC-Management, welche im Rahmen der Unterkategorien weiter detailliert sind. Es konnte gezeigt werden, dass die Integration von GRC, die bereits von einigen Arbeiten thematisiert wurde, von hoher Bedeutung ist. GRC sollte insgesamt jedoch nicht auf den Integrationsaspekt beschränkt werden. Die entwickelten Anforderungen fassen das bestehende Wissen zusammen und können von Praxis und Forschung leicht aufgegriffen werden. Die Forschungsagenda zeigt weiterhin die notwendigen Schritte zur Entwicklung eines GRC-Management-Ansatzes.

4 Delphi-Studie zu Anforderungen und Forschungsbedarfen eines strategischen GRC-Managements

4.1 Zielsetzung, Auswahl und Methodik der Delphi-Studie

In den vorangegangenen Kapiteln wurden mit Hilfe eines systematischen Literaturreviews Anforderungen und Forschungsbedarfe für ein strategisches GRC-Management entwickelt. Die Delphi-Studie, welche von Februar bis Juni 2014 durchgeführt wurde, baut auf diesen Forschungsergebnissen auf und verfolgt zwei Ziele.

1. Evaluierung der Ergebnisse des Literaturreviews
2. Priorisierung von Anforderungen und Forschungsbedarfen

Die Delphi-Studie stellt zum einem aus Sicht der gestaltungsorientierten Forschung (Peffers et al. 2006) eine Evaluierung der bislang erzielten Forschungsergebnisse dar. Das zweite Ziel der Delphi-Studie, nämlich die Priorisierung der Anforderungen und Forschungsbedarfe, geht über diesen Aspekt hinaus. Eine solche Priorisierung ist für die weitere Verwendung der Forschungsergebnisse von großer Bedeutung, da diese eine Fokussierung von Ressourcen in Forschung und Praxis auf besonders bedeutsame Bereiche ermöglicht. Die Priorisierung wird in dieser Delphi-Studie durch eine Bewertung der Bedeutung der Anforderungen und Forschungsbedarfe vorgenommen. Des Weiteren ist darauf hinzuweisen, dass die beiden Forschungsziele aufeinander aufbauen, da eine Priorisierung nur mit einem möglichst abgesicherten Wissen über die relevanten Anforderungen und Forschungsbedarfe sinnvoll ist. Die

Bestimmung der Bedeutung der Forschungsbedarfe ist bereits im Rahmen der Forschungsagenda berücksichtigt.[83]

Nach Linstone und Turoff (1975) kann die Delphi-Methode wie folgt definiert werden: „Delphi may be characterized as a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem." Neben der in dieser Definition sich widerspiegelten Auffassung, dass die Delphi-Methode eine Methode zur Gruppenkommunikation ist, wird diese Methode auch mit bestimmten Forschungsgegenständen wie der Zukunftsforschung in Verbindung gebracht (Häder 2009, S. 21-22). Nach Häder (2009, S. 24-25) werden im klassischen Design einer Delphi-Studie Experten mit Hilfe eines formalisierten Fragebogens befragt. Hierbei bleiben die Einzelantworten anonym, jedoch erhalten die Beteiligten innerhalb einer mehrfachen Wiederholung Feedback über die statistische Gruppenantwort. Von der Gracht (2012, S. 1526) nennt ebenso die gegenseitige Anonymität der Befragungsteilnehmer, die iterative Vorgehensweise, welche sich in mehreren Befragungsrunden ausdrückt, und das kontrollierte Feedback insbesondere der statistischen Gruppenantwort (hier: Mittelwerte) als wesentliche Charakteristika von Delphi-Studien. Die Delphi-Methode ist durch vielfältige Modifikationsmöglichkeiten bzw. methodische Freiheitsgrade geprägt. Diese bestehen unter anderem hinsichtlich der Zahl und Struktur der Experten, der Anzahl der Befragungsrunden, der Gestaltung des Feedbacks, der Möglichkeit der Selbsteinschätzung der Expertise durch die Befragungsteilnehmer, den Abbruchs- und Konsenskriterien und der Nutzung von Workshops (Häder 2009, S. 25).

[83] Siehe Abschnitt 3.6.4.

Aufgrund dieser Variationsmöglichkeiten wurde in der Literatur versucht, Delphi-Befragungen zu typisieren. Bislang existiert jedoch keine einheitliche Typisierung, sondern unterschiedliche Einteilungen (Häder 2009, S. 25-27). Häder (2009, S. 30-37) unterscheidet auf der Grundlage möglicher Zielsetzungen die folgenden vier Typen: Delphi-Befragungen zur Ideenaggregation (Typ 1), Delphi-Befragungen zur Vorhersage von Sachverhalten (Typ 2), Delphi-Befragungen zur Ermittlung von Expertenansichten (Typ 3) und Delphi-Befragungen zur Konsensbildung (Typ 4). Novakowski und Wellar (2008, S. 1486) unterscheiden hingegen Delphi-Studien mit normativem Charakter, Delphi-Studien zur Vorhersage und Delphi-Studien für Policy-Zwecke. Basierend auf der Einteilung von Häder lässt sich die vorliegende Studie primär den Typen 3 und 4 zuordnen.

Die Delphi-Methode wird insbesondere dann als adäquat betrachtet, wenn ein komplexes Problem vorliegt, für das empirische Evidenz fehlt (Murphy et al. 1998; Ono und Wedemeyer 1994). Sie ist weiterhin in Kontexten geeignet, in welchen eine Forschungsfrage nicht direkt durch Forschung im Feld beantwortet werden kann, sondern eine Qualifizierung von Expertenmeinungen notwendig und sinnvoll ist (Skulmoski et al. 2007; Pare et al. 2013). Die Delphi-Methode ist in verschiedenen Anwendungsszenarien einsetzbar (Okoli und Pawlowski (2004, S. 17) zur Strukturierung). In der Wirtschaftsinformatik- und Information Systems-Forschung ist die Delphi-Studie ebenfalls eine verbreitete Forschungsmethode. Insbesondere wird die Methode auch zur Exploration von zukünftig bedeutsamen Forschungsgegenständen sowohl in Deutschland (Heinzl et al. 2001; König et al. 1995) als auch international eingesetzt (Ball und Harris 1982; Brancheau et al. 1996; Dickson et al. 1984; Niederman et al. 1991).

Häder (2009, S. 55-62) vergleicht die Delphi-Methode mit zwei alternativen Forschungsansätzen: der einfachen Expertenbefragung und der Gruppendiskussionen. Die Delphi-Methode besitzt im Gegensatz zu einfachen Experteninterviews den Vorteil, dass durch mehrere Befragungsrunden Feedback an die Befragten gegeben werden kann, wodurch ein Konsens erreicht werden soll. Einfache Expertenbefragungen stellen zudem im Gegensatz zu Delphi-Studien lediglich eine Einzelleistung dar, und es kommt zu keiner Gruppeninteraktion. Häder weist zudem darauf hin, dass für einfache Expertenbefragungen nur eine geringe methodische Unterstützung verfügbar ist. Bei Gruppendiskussionen besteht im Gegensatz zu Delphi-Befragungen die Gefahr, dass Meinungsführerschaft und Gruppenzwang die Forschungsergebnisse beeinflussen. Jedoch können bei Gruppendiskussionen soziale Prozesse innerhalb der Gruppe aufgedeckt werden. Dies ist jedoch nicht Ziel des vorliegenden Forschungsvorhabens. Des Weiteren weisen Delphi-Studien forschungsökonomische Vorteile gegenüber Gruppendiskussionen auf. Unter anderem besteht keine Notwenigkeit für ein persönliches Gespräch, die Experten können sich die Zeit zur Beantwortung der Fragen frei einteilen und es entstehen insgesamt geringere Kosten. Es ist darauf hinzuweisen, dass die Forschungsergebnisse bei Delphi-Studien im Gegensatz zu Gruppendiskussionen nicht direkt zur Verfügung stehen und der Zeitaufwand aufgrund mehrmaliger Befragung auch wesentlich höher als bei einfachen Expertenbefragungen ist. Dies war für die vorliegende Studie jedoch unproblematisch.

Für das hier dargestellte Forschungsvorhaben ist die Delphi-Studie eine angemessene Forschungsmethode, da GRC ein neues Forschungsgebiet darstellt, für welches theoretisches und empirisches Wissen nur begrenzt verfügbar ist. Bei den strategischen GRC-Anforderungen handelt es sich außerdem um normative Empfehlungen zur zukünftigen

Weiterentwicklung von GRC-bezogenen Management-Systemen. Diese lassen sich daher nur eingeschränkt durch Feldforschung erfassen. Gleiches gilt für die Explikation und insbesondere Priorisierung des weiteren Forschungsbedarfs. Rosemann und de Bruin (2005) zählen weiterhin folgende Vorteile der Delphi-Methode auf, die auch für das vorliegende Forschungsvorhaben zutreffend sind. (1) Durch Anonymität werden kreativere Ergebnisse erzielt und reichhaltiger Daten erzeugt (Delbecq et al. 1975). (2) Probleme, die inhärent mit Gruppendiskussion verbunden werden, wie Meinungsführerschaft durch dominante Personen und Gruppendruck werden eliminiert (Murphy et al. 1998). (3) Geografische Grenzen und hiermit verbundene Koordinations- und Reiseaufwände treten nicht auf (Okoli und Pawlowski 2004).

Hinsichtlich der Bedeutung der Erzielung eines Konsenses in Delphi-Studien argumentiert von der Gracht (2012, S. 1527-1528) bezugnehmend auf Dajani et al. (1979, S. 84), dass das primäre Ziel einer Delphi-Studie die effiziente Strukturierung des Kommunikationsprozesses einer Gruppe ist. Die Bildung eines Konsenses zwischen den Gruppenmitgliedern stellt zwar eine wichtige Komponente von Delphi-Studien dar, ist jedoch nicht ihr primäres Ziel. Von der Gracht führt weiter aus, dass Konsens daher nicht als Kriterium zur Beendigung einer Delphi-Studie verwendet werden sollte, wie es häufig vorkommt. Vielmehr ist zwischen den Konzepten des Konsenses und der Stabilität der Antworten zu unterscheiden. Dajani et al. (1979, S. 84) führen aus, dass Stabilität eine Konsistenz zwischen den Antworten aufeinanderfolgender Befragungsrunden sicherstellt.

Aufgrund der Flexibilität von Delphi-Studien bzgl. des Forschungsdesigns wird kritisiert, dass methodische Anpassungen in existierenden Delphi-Studien teilweise scheinbar willkürlich vorgenommen werden. Pare et al. (2013, S. 214-215) empfehlen Modifikationen darauf zu un-

tersuchen, ob diese bereits in anderen Studien verwendet wurden. Dieser Empfehlung wird vorliegend gefolgt. Des Weiteren können basierend auf der Typisierung der vorliegenden Studie anhand der genannten Typen von Häder, Entscheidungen hinsichtlich des Forschungsdesigns unterstützt werden. Um eine effiziente Durchführung der Studie zu gewährleisten, wurden die einzelnen Befragungsrunden jeweils mit Hilfe eines Online-Fragebogens umgesetzt. Hierfür wurde die Software „Enterprise Feedback Suite (EFS Survey)" des Unternehmens QuestBack AG verwendet.

Die Darstellung der Delphi-Studie zu Anforderungen und Forschungsbedarfen eines strategischen GRC-Managements gliedert sich im Anschluss wie folgt. In Abschnitt 4.2 wird die Planung der Studie dargestellt. Diese beinhaltet die Zusammenstellung des Expertenpanels, die Erläuterung der Struktur und Vorgehensweise der Delphi-Studie sowie den Pretest. Im anschließenden Abschnitt 4.3 werden die Ergebnisse der einzelnen Befragungsrunden ausgewertet, wobei auch Überlegungen zu den verwendeten Analysemethoden angestellt werden. Abschnitt 4.4 widmet sich der Diskussion der Grenzen der durchgeführten Studie. Das Kapitel schließt mit einem Fazit in Abschnitt 4.5.

4.2 Planung der Delphi-Studie

4.2.1 Das Expertenpanel

Da sich GRC auf ein weites Themenspektrum bezieht, bilden die Experten, die für die hier dargestellte Studie relevant sind, keine homogene Gruppe. Es ist vielmehr wünschenswert, eine heterogene Expertengruppe zu bilden, um möglichst viele unterschiedliche Perspektiven auf das Themengebiet einzubeziehen. Es bestehen insbesondere zwei Spannungsfelder.

1. Die Studie soll sowohl das Wissen der Forschung als auch der Praxis nutzen (Melnyk et al. 2009; Rosemann und de Bruin 2005; Schmiedel et al. 2013).
2. In der GRC-Forschung existiert ein Spannungsfeld zwischen gestaltungsorientierter Forschung, welche vor allem in der deutschsprachigen Wirtschaftsinformatik dominiert, und verhaltenswissenschaftlicher Forschung.

Die Auswahl der Experten ist von hoher Bedeutung für die Qualität der Delphi-Befragung und sollte daher einer strukturierten Vorgehensweise folgen (Linstone und Turoff 1975; Powell 2003). Nach Häder (2000) lässt sich das Vorgehen zur Auswahl von Experten an Hand von drei Schritten beschreiben. Diese sind (1) die Festlegung der Anzahl der notwendigen Experten, (2) die Klärung der Struktur der Expertengruppe und (3) das Auffinden der Experten.

Zu (1): Im Kontext anderer Delphi-Studien wird auf die Problematik der Bestimmung der Anzahl der Experten hingewiesen (siehe hierzu bspw. Diskussion in Kasiri et al. 2012, S. 260). So wird darauf verwiesen, dass bislang keine Empfehlungen für spezifische Panelgrößen vorliegen (Reid 1988). Obwohl vereinzelt gezeigt wurde, dass durch die Erhöhung der Anzahl der Experten auch eine Erhöhung der Reliabilität der Ergebnisse erzielt werden kann (Murphy et al. 1998), gibt es keinen breit nachgewiesenen Zusammenhang zwischen der Reliabilität bzw. Validität und der Anzahl der Experten. Ebenfalls liegt der Delphi-Methode üblicherweise keine repräsentative Stichprobe zu Grunde (Powell 2003; Okoli und Pawlowski 2004, S. 19). Des Weiteren kann eine hohe Expertenzahl zu niedrigen Rücklaufquoten führen (Pare et al. 2013, S. 213). Eine allgemeine Empfehlung ist eine Panelgröße von 10 bis 18 Teilnehmern (Okoli und Pawlowski 2004, S. 18). Da Delphi-Studien aus mehreren Befragungsrunden bestehen und nach der initia-

len Befragungsrunde üblicherweise weitere Teilnehmer ausscheiden, wurde für die erste Befragungsrunde eine Mindestteilnehmerzahl von 20 definiert. Hierbei sollte auch sichergestellt werden, dass die Hauptgruppen (Forscher und Praktiker sowie nationale und internationale Vertreter) angemessen vertreten sind.

Tab. 31: „Knowledge resource nomination worksheet" für die vorliegende Delphi-Studie

Struktur des Expertenpanels	Quellen zur Identifikation von GRC-Experten
Forschung: - Betriebswirtschaftslehre - Wirtschaftsinformatik / Information Systems - Rechtswissenschaften	Persönliche Kontakte Literatur Organisationen (bspw. OCEG, ISACA) Wissenschaftliche Konferenzen
Praxis: - Berater/ Wirtschaftsprüfer/ Juristen - Unternehmensangehörige - Softwareanbieter	Persönliche Kontakte Praxisnahe Literatur Organisationen (bspw. OCEG, ISACA) Wissenschaftliche / Praxisnahe Konferenzen

Zu (2) und (3): Okoli und Pawlowski (2004, S. 20-23) konkretisieren die Aufgaben der Festlegung der Expertenstruktur und der Auswahl der Experten in fünf Schritte, die für dieses Forschungsvorhaben zu Grunde gelegt wurden. In einem ersten Schritt wird die Struktur der Experten durch ein sogenanntes „knowledge resource nomination worksheet" festgelegt. Zur Festlegung der Expertenstruktur werden die eingangs gemachten Überlegungen herangezogen und hierzu die in Tab. 31 dargestellte Expertenstruktur entwickelt (linke Spalte). Anschließend müssen Experten in den Kategorien identifiziert werden. Für die Identifikation werden persönliche Kontakte, Organisationen, Veröffentlichungen und einschlägige Konferenzen genutzt (rechte Spalte). Gemäß Okoli und Pawlowski (2004, S. 20-21) können auch praxis-

nahe Publikationen zur Identifikation von relevanten Praxisvertretern verwendet werden. Für GRC trifft dies in besonderem Maße zu, da eine Vielzahl an praxisnahen Publikationsorganen sowie White Papers vorliegt. Gleichzeitig zeigen die Personen durch ihre Publikationstätigkeit bereits Expertise und Interesse. Anschließend wurden die identifizierten Experten kontaktiert. Hierbei konnten auch weitere Empfehlungen im Sinne eines Schneeballprinzips (Skulmoski et al. 2007) gemacht werden. Zur Evaluierung der Experten wird auf öffentlich verfügbare Informationen (Anzahl an Publikationen, Akademischer Grad, Zeit der Beschäftigung mit GRC anhand des Lebenslaufs) zurückgegriffen, um eine Kontaktierung der Experten zur reinen Abfrage biografischer Informationen zu vermeiden. Die Experten sollen in den einzelnen Unterkategorien nach ihrer Expertise gerankt werden. Die Kontaktierung der Experten erfolgt dann dem Ranking der Experten folgend in mehreren Wellen bis die angestrebte Panelgröße erreicht ist. Den möglichen Teilnehmern wird hierbei erklärt, dass sie als GRC-Experten ausgewählt wurden und eingeladen werden an der Delphi-Studie teilzunehmen. Ihnen wird weiterhin der Studienaufbau erläutert, und sie werden darauf hingewiesen, dass für die Delphi-Studie drei Befragungsrunden geplant sind, wobei jede Befragungsrunde aus einem 20-minütigen Fragebogen besteht. Der Link zum Fragebogen der ersten Runde wurde direkt in der Einladungsmail versendet.

Es ist darauf hinzuweisen, dass die Studie aufgrund der internationalen Beteiligung vollständig auf Englisch durchgeführt wurde. Es wurde auf eine Rückübersetzung der demografischen Angaben, Anforderungen und Forschungsbedarfe verzichtet, um die Ergebnisse im Original wiederzugeben.

4.2.2 Struktur und Vorgehensweise der Delphi-Studie

Eine „klassische“ Delphi-Studie beginnt üblicherweise mit einer Brainstorming-Runde (Okoli und Pawlowski 2004, S. 24; Schmidt 1997, S. 769-770). In der vorliegenden Studie wird anstatt der Durchführung einer Brainstorming-Runde mit einer initialen Liste von Anforderungen und Forschungsbedarfen des strategischen GRC-Managements begonnen, welches sich in ähnlichen Studien bewährt hat (De Haes und Van Grembergen 2008a; Kasi et al. 2008; Kasiri et al. 2012; Keill et al. 2002; Melnyk et al. 2009; Nakatsu und Iacovou 2009; Ogden et al. 2005; Olbrich et al. 2012; O'Neill et al. 2009; Philip et al. 2010; Saunders und Jones 1992; Wamba und Ngai 2011; Wamba und Ngai 2012). Hierdurch sollen durch eine Triangulation von Forschungsmethoden existierende Probleme qualitativer Forschung minimiert und das verfügbare Wissen bestmöglich genutzt werden. Die Studie besteht insgesamt aus zwei Phasen. Für die zweite Phase sind hierbei zwei Befragungsrunden geplant.

- **Phase 1:** Validierung der initialen Listen der Anforderungen und Forschungsbedarfe[84] des strategischen GRC-Managements durch das Panel
- **Phase 2:** Priorisierung der Anforderungen und Forschungsbedarfe des strategischen GRC-Managements durch das Panel

Ähnlich wie in anderen Studien wurde in der ersten Befragungsrunde (Phase 1) eine dreiteilige Struktur für den Fragebogen verwendet. Diese bestand (1) aus einer Einführung in die Studie und Ausführung der zu

[84] Die initiale Liste der Anforderungen ist in Tab. 9 enhalten. Die initiale Liste der Forschungsbedarfe ist in Tab. 15 bis Tab. **17** enthalten.

Grunde liegenden Konzepte, (2) demografischen Fragen einschließlich einer Selbstbewertung der Expertise der Experten und (3) dem Teil zu Anforderungen und Forschungsbedarfen des strategischen GRC-Managements. Die Einführung in die Studie besteht aus der Darstellung des Studiendesigns sowie dem hieraus zu erwartenden Nutzen sowohl für Forschung und Praxis als auch für die Studienteilnehmer. Die Expertise der Panelteilnehmer wird bereits durch eine Analyse von verfügbaren Informationen wie bspw. die Anzahl der Veröffentlichungen oder die Länge der Erfahrung in Forschung oder Praxis bewertet (Okoli und Pawlowski 2004, S. 22). Diese Informationen wurden durch die Abfrage des akademischen Grades, der gegenwärtigen Position sowie durch eine Selbstbewertung der Expertise ergänzt und abgesichert. Im letzten Teil wird dem Expertenpanel die Liste mit den Anforderungen und Forschungsbedarfen vorgelegt. Hierbei wird um Feedback gebeten, wobei in allen Bereichen die Möglichkeit gegeben wurde, einzelne Elemente zu ergänzen, zu verändern, zu löschen oder zu kommentieren. Eine gleiche Möglichkeit bestand auch für die Anforderungskategorien, welche die Anforderungen und Forschungsbedarfe strukturieren. Der Fokus der ersten Runde war somit die Validierung der Ergebnisse der literatur- und theoriebasierten Forschung. Ziel war es, eine möglichst umfassende Liste von Anforderungen und Forschungsbedarfen zu erhalten. Daher wurde in dieser Phase kein weiterer Input von den Befragten verlangt. Eine Herausforderung für die Erstellung des Fragebogens ist die Tatsache, dass verschiedene Personen unterschiedliche Begriffsverständnisse haben können (siehe „inadequate preoperational explication of constructs threat", Cook und Campbell 1979), was für GRC aufgrund der uneinheitlichen Terminologie in besonderem Maße zutrifft. Zum einem wird diesem Umstand entgegengewirkt, da durch den literaturbasierten Ansatz etablierte Begriffe verwendet werden, welche durch Publikation und hiermit ver-

bundene Peer-Reviews bereits Feedback aus der Forschungsgemeinschaft erfahren haben. Ein Pretest prüft zusätzlich auch die Verständlichkeit des Fragebogens (Abschnitt 4.2.3).

In der zweiten Phase erfolgte eine Bewertung der Bedeutung der überarbeiteten Anforderungen und Forschungsbedarfe. Für jedes Element wurde hierbei eine 6-stufige Likert-Skala (1 = not important und 6 = very important) verwendet, die aufgrund der insbesondere recht hohen Zahl von Forschungsbedarfen eine ausreichende Streuung der Bewertungen ermöglichen sollte. Die Bewertung der Anforderungen und Forschungsbedarfe auf einer Likert-Skala bietet im Gegensatz zum Ranking verschiedene Vorteile (siehe bspw. Niederman et al. 1991, S. 476), wobei hier insbesondere zwei hervorzuheben sind. (1) Es ist keine simultane Berücksichtigung aller Objekte des Fragebogens notwendig und (2) die Bewertung erlaubt den Ausdruck von Indifferenz zwischen den Antwortmöglichkeiten (hier Anforderungen und Forschungsbedarfe). Da die überarbeiteten Listen zu Anforderungen und Forschungsbedarfen bereits eine erhebliche Länge und Komplexität aufwiesen, wurde die Bewertung der Bedeutung für die Befragungsteilnehmer so einfach wie möglich gehalten und somit auf eine weitere Untergliederung der Bedeutung bspw. nach Relevanz für Forschung und Praxis verzichtet.

Wie bereits dargestellt, soll durch eine Delphi-Studie ein Konsens zwischen den Panelteilnehmern hergestellt werden, wozu mehrere Iterationen in Phase 2 vorgesehen sind. Des Weiteren wird, wie bereits ausgeführt, eine Stabilität in den Antworten angestrebt. Zur Festlegung der Anzahl dieser Iterationen sind verschiedene Kriterien relevant, wobei Konsens und Stabilität eine wichtige Rolle spielen. Dajani et al. (1979, S. 84) empfehlen hierbei Stabilität zuerst zu testen und anschließend einen möglichen Konsens zu untersuchen. Insgesamt sind Zeit- und

Kapazitätsbeschränkungen, auch bei den Befragungsteilnehmern, mit der Qualität der Befragungsergebnisse abzuwägen (Schmidt 1997). Andere Studien zeigen, dass die Befragten gegebenenfalls eine Teilnahme an weiteren Befragungsrunden verweigern, wenn keine weitere Verbesserung der Befragungsergebnisse erwartet wird (Keill et al. 2002, S. 110; Olbrich et al. 2012, S. 4153). In der vorliegenden Studie wurde den Teilnehmern außerdem eine Terminierung nach drei Runden versprochen, um mögliche Befragungsteilnehmer nicht durch einen zu hohen Aufwand abzuschrecken. Des Weiteren ist zu beachten, dass die vorliegende Studie nicht mit einer Brainstorming-Runde, sondern mit einer initialen und strukturierten Liste von Anforderungen und Forschungsbedarfen beginnt.

In Wiederholungsrunden zu Phase 2 werden die Befragten nach einer Neubewertung gefragt, wobei Ihnen der Gruppendurchschnitt sowie relevante Kommentare der anderen Teilnehmer als Feedback gegeben werden. Gemäß dem beispielhaften Design von Okoli und Pawlowski (2004) wäre in dieser Runde eine Unterscheidung in mehrere homogenere Panels bspw. für Praktiker und Forscher denkbar, wobei das Feedback zum Mittelwert je Panel ermittelt wird. Anzunehmen ist, dass für diese homogeneren Panels ein höheres Maß an Konsens erreicht werden könnte. Jedoch wurde diese Möglichkeit nicht gewählt, da die Zielsetzung verfolgt wurde, eine „praxisorientierte“ Forschungsagenda zu entwickeln, wobei Forscher und Praktiker ihre Meinung auch unter Einbeziehung der Ergebnisse der anderen Gruppe überdenken sollten.

4.2.3 Pretest

Wichtige Kriterien für die Evaluierung von empirischen Studien sind die Validität und Reliabilität. In einfachen Befragungen wird dies typischerweise auch durch Pre- und Retesting des Forschungsdesigns si-

chergestellt. Pretesting ist für Delphi-Studien ebenfalls ein wichtiges Instrument zur Sicherstellung der Validität und Reliabilität (Okoli und Pawlowski 2004) und wird dem Literaturreview von Pare et al. (2013, S. 213-214) folgend bislang nur unzureichend durchgeführt. Okoli und Pawlowski (2004) führen jedoch aus, dass die sogenannte „Test-Retest-Reliabilität" von untergeordneter Bedeutung ist, da die Studienteilnehmer aufgrund mehrerer Befragungsrunden inhärent die Möglichkeit zum Feedback haben. Der Pretest kann sich auf das gesamte Forschungsdesign beziehen (Häder 2009, S. 139) und demnach mehrere Befragungsrunden erfordern (Skulmoski et al. 2007). In der vorliegenden Studie wird eine initiale Liste von Anforderungen und Forschungsbedarfen des strategischen GRC-Managements verwendet, die bereits durch vorangegangene Publikationen Feedback durch die Forschungsgemeinschaft erfahren hat. Des Weiteren wird innerhalb jeder Befragungsrunde den Studienteilnehmern eine Feedbackmöglichkeit auch zu den Befragungsinstrumenten gegeben. Da zudem ähnliche Befragungsinstrumente in allen Befragungsrunden verwendet werden, besteht daher nur die Notwendigkeit eines Pretests der ersten Befragungsrunde, welcher sowohl die Verständlichkeit der Einführung und des Fragebogens als auch die technische Umsetzung prüfen soll. Hierfür wurden persönliche Kontakte aus Forschung und Praxis genutzt. In Folge des Pretests wurden mehrere leichte Anpassungen am Fragebogen vorgenommen. Diese betrafen sowohl die technische Umsetzung als auch die Formulierung der Anforderungen und Forschungsbedarfe.

4.3 Ergebnisse der Delphi-Studie

4.3.1 Vorüberlegungen zur Auswertung

Wie in Delphi-Studien üblich, die eine Bewertung mit Hilfe einer Likert-Skala vorsehen, soll auch vorliegend der Mittelwert der Anforde-

rungen und Forschungsbedarfe bestimmt und in weiteren Befragungsrunden den Teilnehmern im Sinne einer aggregierten Gruppenantwort als Feedback zur Verfügung gestellt werden. Weiterhin werden die Mittelwerte zur Bestimmung der Rangfolge der Anforderungen und Forschungsbedarfe herangezogen. Neben der Bestimmung der relativen Bedeutung ist die Analyse des erreichten Konsenses sowie der Stabilität von entscheidender Bedeutung für Delphi-Studien. Die Messung von Konsens bzw. Stabilität in Delphi-Studien wird in der Literatur kontrovers diskutiert, wobei eine Vielzahl unterschiedlicher Messgrößen angewendet werden (von der Gracht 2012, S. 1528-1533). Für die Information Systems-Forschung empfehlen Pare et. al. (2013, S. 212) Kendall's W zur Bestimmung des Grades an Konsens, was ebenfalls in dem vielbeachteten Paper von Schmidt (1997, S. 770) empfohlen wird. Es werden jedoch auch in der Information Systems-Literatur verschiedene deskriptive Statistiken wie Mittelwerte und Standardabweichungen hinsichtlich einer Konsensbildung interpretiert (Brancheau et al. 1996; Heinzl et al. 2001; Melnyk et al. 2009; Nevo und Chan 2007; Wamba und Ngai 2011; Wamba und Ngai 2012; Park et al. 2006). Zum Einsatz von Methoden der schließenden Statistik sind verschiedene Vorbedingungen zu beachten. Wenn die Daten kardinalskaliert sind und einer Normalverteilung entsprechen, können parametrische statistische Verfahren angewendet werden. Für die vorliegende Studie ist dies, ebenso wie für die meisten Delphi-Studien, nicht der Fall. Daher sind nichtparametrische statistische Verfahren anzuwenden.

Die folgenden Tabellen basieren auf der Darstellung in von der Gracht (2012, S. 1529-1533) und geben eine Übersicht zu Möglichkeiten der Bestimmung von Konsens und Stabilität in Delphi-Studien mit Hilfe von deskriptiver (Tab. 32) und schließender Statistik (Tab. 33). Außerdem findet eine Einteilung nach den Auswertungsmöglichkeiten statt,

und es wird auf die Relevanz für die vorliegende Studie eingegangen. Bzgl. der Auswertungsmöglichkeiten wird Konsens und Stabilität sowie die Tendenz, also die Entwicklung des Konsenses über die Befragungsrunden, betrachtet.

Tab. 32: Übersicht zu möglichen Analysemethoden der deskriptiven Statistik für Delphi-Studien und deren Relevanz für die vorliegende Studie

Messgröße	Beschreibung	Einteilung	Ausgewählt
Mittelwert (M), Rangfolge	Mittelwert und Rangfolge sind die am meisten verbreiteten deskriptiven Statistiken in Delphi-Studien und besitzen Vorteile hinsichtlich Vergleichbarkeit mit anderen Studien und hinsichtlich der einfachen Nachvollziehbarkeit. Der Mittelwert wird zur Bestimmung der Rangfolge der Bedeutung von Anforderungen und Forschungsbedarfen verwendet. Die Differenz des Mittelwertes bzw. des Rangwertes aus der zweiten und dritten Befragungsrunde wird als Kriterium für die Stabilität verwendet (von der Gracht 2012, S. 1529-1530).	Stabilität	Ja
Standardabweichung (SD)	Die Standardabweichung ist eine relative Messgröße (bezogen auf die verwendete Skala) für den Konsens. Je niedriger die Standardabweichung desto höher kann der Grad an Konsens angenommen werden. Perfekter Konsens entspricht einer Standardabweichung von 0. Die Differenz der Standardabweichungen für aufeinanderfolgende Befragungsrunden zeigt die Tendenz des Konsenses und misst somit den Erfolg der Konsensbildung (Dickson et al. 1984, S. 148; Park et al. 2006, S. 424; Wamba und Ngai 2012, S. 2882). Es ist anzumerken, dass ein perfekter Konsens bei Delphi-Studien nicht zu erwarten ist (Niederman et al. 1991, S. 482). Stabilität kann mit Hilfe des Vergleichs der Standardabweichung von zwei aufeinanderfolgenden Befragungsrunden analysiert werden.	Konsens Stabilität Tendenz	Ja

Messgröße	Beschreibung	Einteilung	Ausgewählt
Interquartilsabstand (IQR)	Der Interquartilsabstand (engl. interquartile range) ist ein Maß für die Streuung des Medians. Er wird berechnet als Differenz aus oberem und unterem Quartil. Ein Interquartilsabstand von < 1 bedeutet, dass mehr als 50% der Teilnehmer die gleiche Bewertung abgegeben haben (De Vet et al. 2005, S. 198).	Konsens Tendenz	Ja
Variationskoeffizient (CV)	Der Variationskoeffizient (engl. coefficient of variation) ist eine Messgröße für die Streuung. Hierbei wird eine Normierung am Mittelwert (Berechnung als Standardabweichung durch Mittelwert) vorgenommen, wodurch eine Unabhängigkeit von der verwendeten Skala entsteht. Der Koeffizient erlaubt somit einen Vergleich des erreichten Konsenses zwischen verschiedenen Studien (von der Gracht 2012, S. 1531). Für Yang (2003, S. 5) ist Konsens für ein Item des Fragebogens mit einem Variationskoeffizienten von 0,5 oder kleiner erreicht. Stabilität kann ebenfalls Yang (2003, S. 5) folgend durch Vergleich des Variationskoeffizienten von zwei aufeinanderfolgenden Runden festgestellt werden.	Konsens Stabilität	Ja

Auf zwei Aspekte sei weiterhin explizit hingewiesen. Zum einen ist die Bestimmung von Mittelwert, Standardabweichung und Variationskoeffizient bei Daten, die mit Hilfe von Likert-Skalen erhoben wurden aus streng methodischer Sicht nicht korrekt, da es sich um eine Ordinalskala handelt. Mit ihrer Berechnung wird daher ein gleicher Abstand zwischen den einzelnen Elementen der Skala unterstellt. Die Berechnung von Mittelwerten und Standardabweichung ist jedoch, insbesondere auch im Kontext von Delphi-Studien, weit verbreitet und für Skalen mit vielen Werten (die vorliegende Studie verwendet eine sechsstufige Likert-Skala) weniger problematisch (von der Gracht 2012, S. 1529-1530). Zum anderen argumentiert ebenfalls von der Gracht (2012, S. 1532) bezugnehmend auf Yang (2003, S. 5), dass es sich bei aufeinanderfolgenden Befragungsrunden einer Delphi-Studie um abhängige Stichproben handelt und somit statistische Methoden, die eine Unab-

hängigkeit voraussetzen (bspw. Kruskal-Wallis-Test) nicht adäquat sind. Die Anwendung des Kruskal-Wallis-Tests zur Auswertung der vorliegenden Delphi-Studie ist wie folgt begründet. In Runde zwei und drei der Studie wurde zum einen die gleiche Gruppe von Experten eingeladen. Die Einladung für die dritte Befragungsrunde erfolgte also unabhängig davon, ob ein Experte auch an der zweiten Runde teilgenommen hat. Hierdurch sollte eine Reduzierung der Teilnehmerzahlen verhindert werden. Zum anderen ist das Ausscheiden von Befragungsteilnehmern bei Delphi-Studien ein bekanntes Phänomen. Methoden für gepaarte Stichproben erfordern jedoch eine Zuordnung der Bewertungen (bspw. der gleichen Person) und somit auch eine gleiche Stichprobengröße. Ist dies nicht gegeben, können nicht alle Daten berücksichtigt werden. Müller et al. (2010, S. 182) verwenden bei einer ähnlichen methodischen Vorgehensweise daher ebenfalls den Kruskal-Wallis-Test zur Untersuchung der Stabilität im Rahmen ihrer Delphi-Studie.

Tab. 33: Übersicht zu möglichen Analysemethoden der schließenden Statistik für Delphi-Studien und deren Relevanz für die vorliegende Studie

Messgröße	Beschreibung	Einteilung	Ausgewählt
Chi-Quadrat-Unabhängigkeitstest	Der Chi-Quadrat-Unabhängigkeitstest (engl. Chi square test for independence) ist ein nichtparametrischer Test, der untersucht, ob eine Beziehung zwischen zwei Variablen existiert. Er wird daher als Methode vorgeschlagen, um im Rahmen von Delphi-Studien zu testen, ob eine Unabhängigkeit bei den Antworten von zwei Delphi-Runden besteht. Somit kann festgestellt werden, ob Stabilität bei den Antworten erreicht wurde (von der Gracht 2012, S. 1532). Der Test erfordert ordinalskalierte Daten und eine gewisse Stichprobengröße (bspw. einen Wert von größer bzw. gleich 5 für jedes Element der Kontingenztabelle (Dajani et al. 1979, S. 88)).	Stabilität	Nein, da Stichprobengröße zu gering

Messgröße	Beschreibung	Einteilung	Ausgewählt
McNemar Chi-square test	Der McNemar Chi-Quadrat Test ist ein nicht parametrischer Test für abhängige Stichproben mit nominalskalierten Daten (bspw. agree / disagree) und wird zur Prüfung der Stabilität in Delphi-Studien empfohlen (Yang 2003, S. 6-8; Okoli und Pawlowski 2004, S. 26; Pare et al. 2013, S. 212).	Stabilität	Nein, da keine nominalskalierte Variablen
Kruskal-Wallis-Test	Der Kruskal-Wallis-Test ist ein nichtparametrischer Test, welcher eine Verallgemeinerung des Rangsummentests von Wilcoxon darstellt. Die Daten müssen mindestens ordinales Messniveau haben und können auch aus mehr als zwei unabhängigen Grundgesamtheiten stammen. Gegenüber dem beschriebenen Chi-Quadrat-Test ist er robuster und auch für kleine Stichproben von unterschiedlicher Größe anwendbar (Kruskal und Wallis 1952).	Stabilität	Ja
Wilcoxon-Test für abhängige Stichproben	Wilcoxon-Test für abhängige Stichproben (engl. Wilcoxon matched-pairs signed-ranks test) ist eine nichtparametrische Alternative für den Student's t-test. Er vergleicht die Ränge von Bewertungspaaren eines Individuums (Ordinalskala). Er dient zur Analyse, ob ein signifikanter Unterschied zwischen zwei Befragungsrunden einer Delphi-Studie besteht und dient somit zur Determinierung der Stabilität (von der Gracht 2012, S. 1532). Hierbei ist vorausgesetzt, dass die Antworten eines Befragungsteilnehmers einander zugeordnet werden können. Außerdem müssten Bewertungen von Teilnehmern, die nicht an beiden Befragungsrunden teilgenommen haben, eliminiert werden.	Stabilität	Nein, da eine Zuordnung der Daten aus den verschiedenen Runden nur bedingt möglich ist
Kendall's W coefficient of concordance	Die Berechnung des Ausmaßes an Übereinstimmung zwischen den Teilnehmern kann ebenfalls mit Kendalls Konkordanzkoeffizient (Kendall's W) erfolgen. Kendall's W ist ebenfalls eine nichtparametrisierte Methode für Ordinalskalen. Hierbei signalisiert ein Koeffizient W > 0,7 starke Übereinstimmung, ein Koeffizient W zwischen 0,5 und 0,7 moderate Übereinstimmung und ein Koeffizient W zwischen 0,3 und 0,5 schwache Übereinstimmung (Schmidt 1997, S. 767). Kendall's W berechnet hierbei den Grad an Konsens über alle Items (hier Anforderungen bzw. Forschungsbedarfe) einer Delphi-Studie.	Konsens	Ja

4.3.2 Allgemeine Daten zum Expertenpanel

Um die angestrebte Teilnehmerzahl von 20 GRC-Experten zu erreichen, wurden die identifizierten Experten, wie dargestellt, in mehreren Wellen eingeladen. Jede dieser Einladungswellen umfasste etwa 80 mögliche Teilnehmer. Nach der dritten Einladungswelle hatten 27 Teilnehmer den Fragebogen beendet. Daher wurden anschließend keine weiteren Einladungen versendet. Insgesamt wurden 274 Einladungen versendet. Bei 17 möglichen Teilnehmern konnte die Einladung aufgrund falscher oder veralteter E-Mail-Adressen nicht zugestellt werden. 16 Teilnehmer haben die Umfrage zwar gestartet, jedoch abgebrochen. Alle diese Teilnehmer haben im Rahmen des Fragebogens keine Anmerkungen zu den Anforderungen und Forschungsbedarfen erfasst. Deshalb finden sie für die weitere Auswertung keine Berücksichtigung. Für die erfolgreich zugestellten Einladungen ergibt sich somit eine Beendigungsquote von 10,5 %. Berücksichtigt man, dass die Experten fast ausschließlich durch Publikationen und Internetrecherchen und nicht aus persönlichen Kontakten rekrutiert wurden, unterstreicht die Teilnehmerzahl die Bedeutung der Forschungsfrage. Alle weiteren Auswertungen beziehen sich ausschließlich auf die Teilnehmer, die den Fragebogen beendet haben. Es ist weiterhin anzumerken, dass einige Teilnehmer die erste Befragungsrunde zwar beendet, jedoch keine Anmerkungen zu den Anforderungen und Forschungsbedarfen gemacht haben. Für insgesamt 8 Befragungsteilnehmer der ersten Runde war dies der Fall. Die folgende Tabelle gibt die Anzahl der Teilnehmer bzw. die Anzahl der berücksichtigten Datensätze in den drei Befragungsrunden wieder. Zu beachten ist, dass in Runde zwei und drei auch Datensätze von Teilnehmern berücksichtig wurden, die den Fragebogen nicht beendet haben, wobei der Fragebogen z.B. nach der vollständigen Bewer-

tung der Anforderungen abgebrochen wurde. Die Teilnehmerzahlen sind somit über die Befragungsrunde in etwa stabil geblieben.

Tab. 34: Teilnehmerzahlen der einzelnen Befragungsrunden

Befragungsrunde	Runde 1	Runde 2	Runde 3
Teilnehmer / berücksichtigte Datensätze (Teilnehmer mit Kommentaren)	27 (19)	15	14
Einladungen	274 (Gruppe 1: 110 Gruppe 2: 98 Gruppe 3: 64 Auf Empfehlung: 2)	27	27
Teilnahmequote (aus erfolgreich zugestellte Einladungen)	10,51%	55,56%	51,85%
Abbrüche (ohne Berücksichtigung des Datensatzes)	16	3	2
Email nicht zustellbar	17	---	---

Wie angestrebt sind die Teilnehmer der Delphi-Studie international verteilt, wobei ein Schwerpunkt im deutschsprachigen Raum liegt. Es ist anzunehmen, dass der höhere Bekanntheitsgrad des Lehrstuhls im deutschsprachigen Raum die Teilnahmebereitschaft erhöht haben könnte. Zum anderen ist die Mehrheit der Publikationen, die GRC als Begriff aufgreifen, mit einem gestaltungsorientierten Forschungsansatz verknüpft, der traditionsgemäß in deutschsprachigen Ländern stärker verbreitet ist. Trotzdem kann aufgrund von neun Teilnehmern, die aus einem nicht-deutschsprachigen Land kommen, von einer ausreichenden internationalen Diversität in der Expertengruppe gesprochen werden. Weiterhin geben insgesamt 21 Personen an, aus der Forschung zu kommen. Vier Teilnehmer geben an, aus der Unternehmenspraxis zu sein. Zwei Personen machten keine Angaben zu ihrem beruflichen

Hintergrund. Hierbei ist anzumerken, dass durchaus ein Wechsel zwischen Forschung und Praxis auftritt. Zum einen ist dies bedingt durch die Teilnahme von verschiedenen Fachhochschulprofessoren. Zum anderen haben auch ehemalige Doktoranden teilgenommen, die mittlerweile in der Praxis arbeiten. Alle Teilnehmer haben mindestens einen Master bzw. ein Diplom. Die Selbstbewertung der Expertise zeigt, dass insgesamt 25 der Teilnehmer sich entweder in der Vergangenheit aktiv mit GRC beschäftig haben bzw. dies derzeitig tun. Dies bestätigt den Erfolg des strukturierten Auswahlprozesses der Experten.

Tab. 35: Demografische Angaben zum Expertenpanel (basierend auf Runde 1)

Demografische Angaben	Häufigkeit	Prozent
Herkunft		
Austria	1	3,70%
Germany	15	55,56%
Great Britain	1	3,70%
India	2	7,41%
Netherlands	1	3,70%
Portugal	2	7,41%
Switzerland	2	7,41%
Taiwan	1	3,70%
Denmark	1	3,70%
Keine Angabe	1	3,70%
Berufsbezeichnung		
Researcher	4	14,81%
Lecturer	2	7,41%
(Senior) Consultant	2	7,41%
Professor	10	37,04%
Assistant Professor	1	3,70%
PhD Student	1	3,70%
Vice President Development	1	3,70%
Chief Information Officer	1	3,70%
IT Security Manager	2	7,41%
keine Angabe	3	11,11%
Qualifikation		
Dr. / PhD	19	70,37%

Demografische Angaben	Häufigkeit	Prozent
Diplom	4	14,81%
Master	2	7,41%
MBA	1	3,70%
Keine Angabe	1	3,70%
GRC-Expertise		
VERY HIGH: I am currently actively working in the area of GRC (research or practice).	10	37,04%
HIGH: I have experience in the area of GRC based on active work (research or practice).	15	55,56%
MEDIUM: I am e.g. reading articles or go to talks related to the area of GRC, but I am not actively working on GRC related topics.	0	0,00%
LOW: I only have some basic information and experience related to GRC.	2	7,41%
NO: I have no expertise in the area of GRC.	0	0,00%

4.3.3 Ergebnisse der ersten Befragungsrunde

Wie bereits erwähnt, wurde die Delphi-Studie mit den aus dem Literaturreview hergeleiteten Anforderungen und Forschungsbedarfen gestartet. Ziel der ersten Runde war die Validierung dieser Listen hinsichtlich Relevanz und Verständlichkeit der einzelnen Anforderungen und Forschungsbedarfe sowie Vollständigkeit. In der ersten Befragungsrunde wurde eine Vielzahl an qualitativem Feedback von den Teilnehmern gesammelt. Dieses Feedback beinhaltet allgemeine Kommentare zu den Anforderungen und Forschungsbedarfen insgesamt, Kommentare zu einzelnen Anforderungen und Forschungsbedarfen sowie die Ergänzung von Anforderungen und Forschungsbedarfen.

Hinsichtlich der Anforderungen wurde mehrfach geäußert, dass jede Anforderung nur einen Aspekt aufgreifen sollte. So wurde die Anforderung „The management activities being relevant for GRC should be carried out by a central organizational unit (including integrated information systems and methods). The operational activities of GRC should be integrated into the business processes and IT systems (hybrid

approach).“ in zwei Anforderungen aufgespalten. Weitere Anmerkungen forderten eine weitere Konkretisierung der Anforderungen. So wurden innerhalb der Anforderungskategorie „Human factors“ mehrere Anforderungen gebildet, die in der initialen Liste lediglich implizit vorhanden waren. Insgesamt konnte somit die Verständlichkeit der Anforderungen, ohne dass zusätzliche Erläuterungen notwendig sind, erhöht werden. Anzumerken ist auch, dass von mehreren Teilnehmern eine Zustimmung zu einer Mehrzahl der Anforderungen ausgedrückt wurde. Die überarbeitete Liste der Anforderungen besteht, wie aus Tab. 36 ersichtlich ist, aus 19 Anforderungen und blieb über die weiteren Befragungsrunden stabil.

Im Hinblick auf die Forschungsbedarfe eines strategischen GRC-Managements führten die gemachten Kommentare zum einen zu einer Zusammenführung von einzelnen Forschungsbedarfen, da eine Behandlung innerhalb eines Forschungsvorhabens als sinnvoll oder notwendig erachtet wurde. Bspw. betraf dies die GRC-spezifische Erweiterung und Evaluation von Methoden des GPM, die in der initialen Liste auf zwei Forschungsbedarfe aufgeteilt war. Außerdem wurden Forschungsbedarfe aus der Liste entfernt. So haben bspw. Experten für einzelne Forschungsbedarfe angemerkt, dass diese nicht ausreichend spezifisch für GRC sind (bspw. „Examination of the influences that the fulfillment of individual stakeholder interests have on the company value”). Ebenso wurden weitere Forschungsbedarfe hinzugefügt (bspw. „Interplay of GRC and „normal“ management“). Wiederum wurde von mehreren Befragten Zustimmung zu einer Vielzahl von Forschungsbedarfen geäußert. Letztlich wurde auch von den Befragten explizit auf eine Notwendigkeit zur Priorisierung hingewiesen. Die überarbeitete Liste der Forschungsbedarfe besteht, wie aus Tab. 71 bis Tab. 75 er-

sichtlich ist, aus 55 Forschungsbedarfen und blieb ebenfalls über die weiteren Befragungsrunden stabil.

Insgesamt ist im Zusammenhang der Anpassungen an den Anforderungen und Forschungsbedarfe anzumerken, dass diese nicht unabhängig von Wertentscheidungen des Autors sind. Anmerkungen der Befragungsteilnehmer, die als sinnvoll erachtet wurden und bspw. auch von anderen Teilnehmern in ähnlicher Weise geäußert wurden, wurden umgesetzt. Obwohl es eine Vielzahl von Anpassungen gibt, wurden hierdurch jedoch keine umfassenden Veränderungen vorgenommen, sondern im Wesentlichen die Verständlichkeit verbessert. Darüber hinaus hatten die Befragungsteilnehmer in den folgenden Runden die Möglichkeit, die überarbeiteten Listen wiederum zu kommentieren. Hierbei wurde jedoch keine bedeutende Kritik mehr geäußert.

4.3.4 Ergebnisse der zweiten und dritten Befragungsrunde

4.3.4.1 Bedeutung der Anforderungen und Forschungsbedarfe

In der zweiten Befragungsrunde wurde den Teilnehmern die überarbeiteten Listen mit den Anforderungen und Forschungsbedarfen zur Beurteilung der Bedeutung und somit zur Priorisierung vorgelegt. Obwohl den Befragungsteilnehmern wiederum die Möglichkeit gegeben wurde, allgemeines Feedback zu den Anforderungen (und Forschungsbedarfen) zu geben, wurde von dieser Möglichkeit kaum gebraucht gemacht, was ein Anzeichnen für die Zustimmung zu den Anforderungen und Forschungsbedarfen sein könnte. Erwähnenswert ist lediglich der wiederholte Hinweis auf die Bedeutung von existierenden Rahmenwerken wie COSO. Obwohl im Sinne der Allgemeingültigkeit auf die Erwähnung bestimmter Rahmenwerke verzichtet wurde, wird insbesondere im Rahmen der Anforderungskategorie Management-Systeme hierauf Bezug genommen.

Zur Bestimmung der Bedeutung der Anforderungen und Forschungsbedarfe wurden die Mittelwerte und hierauf aufbauend die Rangfolgen ermittelt. Die entsprechenden Statistiken sowie die überarbeiteten Listen der Anforderungen und Forschungsbedarfe sind in Tab. 36 und Tab. 37 sowie Tab. 38 (Top 10 der Forschungsbedarfe, bzw. in Tab. 71 bis Tab. 75 für alle Forschungsbedarfe)[85] für die Runden 2 und 3 angegeben. Die Rangfolge basiert auf den Mittelwerten der dritten Befragungsrunde. Die Werte basieren, wie bereits dargestellt, auf einer sechsstufigen Likert-Skala (1 = not important; 6 = very important). Die verwendeten Abkürzungen werden in Abschnitt 4.3.1 eingeführt. Auf die weiteren deskriptiven Statistiken, die in den Tabellen dargestellt sind, wird im Rahmen der Diskussion des Konsenses und der Stabilität eingegangen.

Wie der Tab. 36, der Tab. 37, der Tab. 38 sowie Tab. 71 bis Tab. 75 zu entnehmen ist, kann bei der Bewertung der Bedeutung eine ausreichende Streuung beobachtet werden. So weist die Anforderung auf Rang 1 einen Mittelwert von 5,79 auf und die Anforderung auf Rang 19 einen Mittelwert von 4,21. Gleichzeitig kann das Ergebnis so interpretiert werden, dass die Anforderung auf Rang 19 zwar eine relativ geringere Bedeutung als die höher gelisteten Anforderungen hat, jedoch bei einem Mittelwert von 4,21 (Likert-Skala von 1 bis 6, wobei der Wert 4 „eher wichtig“ bedeutet) immer noch von einer relevanten Anforderung für das strategische GRC-Management gesprochen werden kann.

[85] Werte, die außerhalb des Bereichs liegen, der Konsens, Konsensverbesserung bzw. Stabilität anzeigt, sind in den relevanten Tabellen (Tab. 36, Tab. 37, Tab. 38, Tab. 71, Tab. 72, Tab. 73, Tab. 74, Tab. 75, Tab. 78, Tab. 79, Tab. 80, Tab. 81) grau hinterlegt. Für die Forschungsbedarfe ist zudem in Klammern die Anforderungskategorie und das Forschungsziel angegeben (DandE = Beschreiben und Erklären; Design = Gestalten).

Bzgl. des Ranges der einzelnen Anforderungen kann weiterhin festgehalten werden, dass obwohl ein Fokus auf IT-affinen Experten lag, strategischen und verhaltensbezogenen Anforderungen eine besonders hohe Bedeutung von den Experten zugestanden wird. So weisen die Anforderungen auf den ersten vier Rängen eine strategische Komponente auf, obwohl die Anforderungen auf Rang zwei und vier aus der Anforderungskategorie „Human factors" stammen. Gleichzeitig werden jedoch andere Anforderungen aus der Anforderungskategorie strategische Ausrichtung eine relativ niedrige Bedeutung beigemessen (bspw. Anforderung #19). Ebenfalls auf Rang vier sind Anforderungen zur Automatisierung und Integration. Insgesamt weisst dies darauf hin, dass die Experten sich differenziert mit den einzelnen Anforderungen auseinandergesetzt haben. Betrachtet man die Ergebnisse aggregiert nach den Anforderungskategorien (durchschnittliche Bewertung aller Anforderungen in einer Kategorie) zeigt sich, dass Automatisierung am höchsten bewertet wurde und Flexibilität am niedrigsten. Die Kategorie Integration nimmt einen mittleren Platz ein (siehe Tab. 76). Dies zeigt auch, dass Integration zwar ein wichtiger Aspekt ist, jedoch vielfältige Anforderungen existieren, die bei der Umsetzung bzw. Weiterentwicklung von GRC-bezogenen Management-Systemen berücksichtigt werden müssen.

Wie es auch in anderen Delphi-Studien beobachtet werden kann (Niederman et al. 1991, S. 482; Park et al. 2006, S. 424-425), findet eine Polarisierung der Bewertungen bei den Anforderungen statt. Das bedeutet, dass Anforderungen mit einer hohen Bedeutung in der zweiten Befragungsrunde in der dritten Runde noch höher bewertet werden und umgekehrt Anforderungen mit niedriger Bewertung noch niedriger bewertet werden. Im vorliegenden Fall steigt der Mittelwert der ersten 9

Anforderungen. Die niedriger bewerteten Anforderungen werden lediglich teilweise niedriger bewertet.

Tab. 36: Befragungsergebnisse zu den Anforderungen für ein strategisches GRC-Management (1 von 2)

Rang	Anforderung	Runde 2		Runde 3		SD_{Diff}
		M	SD	M	SD	
1	Important for establishing an organizational culture that supports GRC is a commitment and clear communication ("tone at the top") of the top management. (#1)	5,67	0,60	5,79	0,56	-0,04
2	GRC should focus on the strategic objectives of companies to achieve superior performance and thus secure the companies' survivability. (#2)	5,53	0,62	5,71	0,45	-0,17
2	GRC need to ensure that the requirements are clearly communicated to the relevant employees. (#3)	5,33	0,94	5,71	0,45	-0,49
4	GRC should focus on the stakeholders' interests. GRC should support the long-term maximization of the companies' value through balancing out the stakeholders' interests and ensuring the fulfillment of those interests e.g. by control procedures. (#4)	5,27	1,06	5,50	0,63	-0,44
4	In order to realize synergies and to avoid double work, GRC should be integrated across different areas (e.g. compliance requirements like Sarbanes-Oxley and information security) as well as across the GRC disciplines (Governance, Risk and Compliance). (#5)	5,13	0,96	5,50	0,73	-0,22
4	To increase the efficacy and efficiency of organizational procedures of compliance and risk control as well as for reasons of cost reduction, controls should be automated as far as needed. At the same time organizational procedures should complementarily support automated controls. (#6)	5,27	0,93	5,50	0,63	-0,30
7	IT should be used as an enabler for strategic GRC-Management. (#7)	5,13	1,02	5,23	0,58	-0,45
8	In order to achieve sustainable competitive advantage based on a superior approach for strategic GRC management, the focus should be on the establishment of a superior GRC culture ("living" the defined processes of GRC) because cultural aspects cannot be easily copied by other organizations. (#8)	5,20	1,11	5,21	0,67	-0,43

Tab. 37: Befragungsergebnisse zu den Anforderungen für ein strategisches GRC-Management (2 von 2)

Rang	Anforderung	Runde 2		Runde 3		SD_{Diff}
		M	SD	M	SD	
8	The operational activities of GRC should be carried out decentralized and should be integrated into the operational business processes and IT systems. This includes the execution and documentation of the control activities. (#9)	5,00	1,15	5,21	0,56	-0,60
8	Existing management systems in the context of GRC (i.e. internal control system, quality management system, data privacy) need to be harmonized. (#10)	5,27	0,77	5,21	0,77	0,00
11	To influence the compliance behaviour preventive and detective controls should be applied. (#11)	5,20	1,17	5,14	0,74	-0,42
12	GRC should be supported by integrated information systems as well as harmonized management methods. (#12)	5,13	0,88	5,07	0,80	-0,09
13	A process oriented point of view as well as procedures, methods and tools of business process management (BPM) should be adapted to reduce the transaction costs and improve efficacy and efficiency in GRC. (#13)	4,73	1,34	5,00	0,85	-0,49
13	In addition to formal controls like rules and incentive systems, informal controls that are focusing especially on cultural aspects should be established. (#14)	5,00	0,82	5,00	0,76	-0,06
13	The control approach chosen should consider the relationship between certain determinants of compliance behaviour and controls, the relationship between the controls itself as well as situation specific aspects. (#15)	4,87	0,81	5,00	0,78	-0,02
16	A strategic approach of GRC should support strategic decision making by collecting and preparing relevant information. (#16)	4,47	1,09	4,71	0,88	-0,21
16	The management activities being relevant for GRC should be guided by a central strategy and carried out by a central organizational unit (esp. in large organizations). (#17)	4,57	1,35	4,71	1,10	-0,25

Rang	Anforderung	Runde 2		Runde 3		SD_{Diff}
		M	SD	M	SD	
18	The challenge of flexible business processes and IT systems originates from the conflict between achievement of business objectives and regulatory GRC needs. As far as there is freedom of choice between design alternatives (not mandatory requirements coming from a law) GRC should apply risk management techniques to balance out GRC objectives and process flexibility. (#18)	4,80	1,05	4,50	0,73	-0,31
19	The relevant resources of the GRC management should support the achievement of operational benefits like the improvement of business processes. (#19)	4,13	1,20	4,21	1,21	0,00

Tab. 38 zeigt die 10 wichtigsten Forschungsbedarfe für ein strategisches GRC-Management. Alle diese Forschungsbedarfe weisen einen Mittelwert von größer 5 auf, wobei wiederum eine 6-stufige Likert-Skala verwendet wurde. Sieht man sich die Bedeutung aller Forschungsbedarfe an, liegen lediglich die beiden Forschungsbedarfe mit der niedrigsten Bedeutung unter einem Mittelwert von 4. Es kann also auch bei dieser Liste von einer hohen Relevanz für das strategische GRC-Management gesprochen werden. Unter den wichtigsten 10 Forschungsbedarfen sind die Anforderungskategorien Integration, Menschliche Faktoren, Automatisierung und strategische Ausrichtung. Betrachtet man die durchschnittliche Bedeutung je Anforderungskategorie sind ebenso wie bei den Anforderungen Automatisierung und Menschliche Faktoren auf den ersten beiden Rängen (siehe Tab. 76). Berechnet man die durchschnittliche Bedeutung der Forschungsbedarfe nach den Forschungsausrichtungen „Beschreiben und Erklären“ und „Gestalten“ lässt sich kaum ein Unterschied feststellen (siehe Tab. 77). Eine Polarisierung der Bedeutungen zwischen Runde zwei und drei, wie es bei den Anforde-

rungen zu beobachten ist, ist bei den Forschungsbedarfen nicht durchgehend vorhanden.

Tab. 38: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (Rang 1 bis 10) [DandE = „Describe and Explain"]

Rang	Forschungsbedarf (Kategorie / Forschungsziel)	Runde 2		Runde 3		SD_{Diff}
		M	SD	M	SD	
1	Are there "basic controls" being relevant for every compliance system? Are there differences between the industries? (Integration / DandE) [§1]	4,92	1,19	5,36	0,61	-0,58
1	Evaluation method for the consequences of compliance violations including effects on operational business processes (cost-benefit analysis of controls) (Human factors / Design) [§2]	5,50	0,65	5,36	0,72	0,07
3	Understand how organizations adopt existing tools and methods in the context of GRC (Automation / DandE) [§3]	5,00	0,95	5,29	0,70	-0,25
4	Which control types can be automated? (Automation / DandE) [§4]	5,40	0,80	5,21	0,67	-0,13
5	Theoretical and empirical examination of the potential benefits of GRC (Strategic Orientation / DandE) [§5]	5,08	0,76	5,14	0,64	-0,12
5	Development of general and industry specific control models (reference models for control processes) for the integrated fulfillment of GRC requirements (Integration / Design) [§6]	5,17	0,80	5,14	0,64	-0,16
5	Method to derive company specific controls from regulatory requirements (e.g. laws) (Integration / Design) [§7]	5,00	1,00	5,14	0,64	-0,36
5	Examinations of the conditions for the automation approaches (respectively control model used, compliance by design vs. compliance by detection) (Automation / DandE) [§8]	5,00	1,00	5,14	0,64	-0,36
5	Development of techniques and methods to improve the compliance behaviour and the compliance culture (Human factors / Design) [§9]	5,08	0,95	5,14	0,64	-0,31

Rang	Forschungsbedarf (Kategorie / Forschungsziel)	Runde 2		Runde 3		SD_{Diff}
		M	SD	M	SD	
10	Empirical studies on the advantages of alternative coordination approaches for GRC (coordination with a central organizational unit, integration of GRC into the core business processes or a combined approach) (Integration / DandE) [§10]	4,83	0,90	5,07	0,46	-0,44
10	Extension and consolidation of existing empirical examinations of compliance behavior (Human factors / DandE) [§11]	5,17	0,99	5,07	0,59	-0,39

4.3.4.2 Konsens und Stabilität

Zur Analyse des Konsenses und der Stabilität der Bewertungen hinsichtlich der Anforderungen und Forschungsbedarfe eines strategischen GRC-Managements wurden, wie eingangs dargestellt, unterschiedliche Messgrößen verwendet, welche in Tab. 32 und Tab. 33 mit den verwendeten Abkürzungen beschrieben wurden. Die berechneten Werte für die vorliegende Studie sind in Tab. 36, Tab. 37 und Tab. 38 sowie ergänzend im Anhang (Tab. 71, Tab. 72, Tab. 73, Tab. 74 und Tab. 75) angegeben.

Hinsichtlich des Konsenses der Anforderungen lässt sich festhalten, dass basierend auf der Einteilung von Schmidt (1997, S. 767) für Kendall's Konkordanzkoeffizient mit W=0,24 (p=<0.0001) in der dritten Befragungsrunde ein schwacher Konsens erreicht wurde. Für die zweite Befragungsrunde wurde W=0,15 (p=0,0013) berechnet, was bedeutet, dass eine Verbesserung des Konsenses in der dritten Befragungsrunde erreicht wurde. Es wäre zu erwarten gewesen, dass bei einer weiteren Befragungsrunde, unterstellt man, dass das Teilnehmerpanel stabil geblieben wäre, eine Konsensverbesserung hätte erzielt werden können. Die Analyse der Konsensbildung bzgl. einzelner Anforderungen und Forschungsbedarfe, die nachfolgend dargestellt wird, zeigt jedoch, dass für die Mehrheit der Anforderungen und Forschungsbedarfe Konsens erreicht wurde. Des Weiteren ist anzumerken,

dass für die meisten Anforderungen und Forschungsbedarfe, wie noch gezeigt wird, keine signifikanten Änderungen zwischen der zweiten und dritten Befragungsrunde zu beobachten sind. Hiermit wurde also Stabilität erreicht. Des Weiteren wurde den Teilnehmern eine Beendigung nach drei Befragungsrunden zugesagt, um potentielle Teilnehmer nicht durch einen zu hohen Aufwand abzuschrecken. Andere Delphi-Studien zeigen, dass ab der vierten Befragungsrunde Ausfälle unter den Befragungsteilnehmern zu erwarten sind (Singh et al. 2009, S. 420-421). Einige Kommentare zur dritten Befragungsrunde haben zudem gezeigt, dass dies auch für die vorliegende Studie wahrscheinlich gewesen wäre. Schwacher bzw. moderater Konsens ist zudem ein mehrfach beobachtetes Phänomen in Delphi-Studien in der Wirtschaftsinformatik bzw. Information Systems-Forschung (Singh et al. 2009, S. 420-421). Dies liegt in den unterschiedlichen Hintergründen wie Ausbildung und Industriezugehörigkeit der Befragungsteilnehmer begründet, was auch für die vorliegende Delphi-Studie aufgrund der gewollten heterogenen Zusammensetzung des Expertenpanels zutrifft.

Basierend auf den Standardabweichungen kann gezeigt werden, dass für die überwiegende Zahl der Anforderungen jeweils eine Konsensverbesserung mit der dritten Befragungsrunde eingetreten ist. Lediglich für die Anforderungen #10 und #19 hat das Konsensniveau stagniert. Auf der Grundlage des Variationskoeffizienten ergibt sich eine Verbesserung für alle Anforderungen bis auf die Anforderung #10, wofür der Konsens wiederum stagniert, eine Verbesserung des Konsenses. Zieht man einen Schwellwert von 0,2 für den Variationskoeffizienten heran, so wurde für alle Anforderungen bis auf Anforderung #17 und #19 ein Konsens erzielt. Die Analysen auf Grundlage der Standardabweichung und des Variationskoeffizienten führen somit, da beide grundsätzlich auf der Standardabweichung basieren, erwartungsgemäß zu ähnlichen

Ergebnissen. Die Interquartilsabstände weisen in acht Fällen für die dritte Befragungsrunde einen Wert von größer als eins auf, was bedeutet, dass für diese Anforderungen kein Konsens erzielt wurde. Darüber hinaus ist der Interquartilsabstand nur für fünf Anforderungen in der dritten Runde kleiner als in der zweiten Befragungsrunde. Insgesamt sind die Interquartilsabstände somit eine striktere Methode, was die Bewertung der Konsensverbesserung als auch die Messung des erreichten Konsenses in Befragungsrunde 3 anbelangt. Der Interquartilsabstand zeigt hierbei für alle Anforderungen, die auch im Rahmen der Analyse mit Hilfe der Standardabweichung bzw. mit Hilfe des Variationskoeffizienten eine fehlende Konsensverbesserung bzw. einen nicht erreichten Konsens zeigten, ein gleiches Ergebnis. Für die vorliegende Delphi-Studie wird daher geschlussfolgert, dass für die Anforderungen #17 und #19 kein Konsens erzielt wurde (jeweils kein Konsens gemäß Variationskoeffizienten und Interquartilsabstand). Für die Anforderungen #11, #12, #13, #14, #15, #16 ist die Konsensbildung fraglich (Konsens gemäß Variationskoeffizient, jedoch nicht gemäß Interquartilsabstand). Hinsichtlich der Anforderungen #1, #2, #3, #4, #5, #6, #7, #8, #9, #10, #18 kann von einem erreichten Konsens ausgegangen werden (Konsens gemäß Variationskoeffizient und Interquartilsabstand).

Für die Forschungsbedarfe wurde in der dritten Befragungsrunde ein Wert für Kendall's W von 0,25 berechnet, womit Schmidt (1997, S. 767) folgend ein schwacher Konsens erzielt wurde und gegenüber der zweiten Delphi-Runde eine Konsensverbesserung vorliegt (W=0.15). Zur Einordnung dieser Ergebnisse gelten die Überlegungen, die zu den Anforderungen angestellt wurden, analog. Die Standardabweichung zeigt lediglich für sieben Forschungsbedarfe ein verschlechtertes Konsensniveau und für einen Forschungsbedarf ein stagnierendes Kon-

sensniveau in der dritten Befragungsrunde an. Der Variationskoeffizient zeigt für sechs Forschungsbedarfe einen verschlechterten Konsens in der dritten Befragungsrunde, wobei die hierbei identifizierten Forschungsbedarfe größtenteils übereinstimmen. Lediglich Forschungsbedarf §47 zeigt einen verschlechterten Konsens bei der Auswertung der Standardabweichung, jedoch einen leicht verbesserten Konsens bei der Auswertung des Variationskoeffizienten. Aus dem Schwellwert von 0,2 für den Variationskoeffizienten ergeben sich lediglich 6 von 55 Forschungsbedarfen für welche kein Konsens in der dritten Befragungsrunde erreicht wurde. Die Berechnung der Interquartilsabstände zeigt für lediglich sechs der Forschungsbedarfe einen Wert von größer eins. Für vier der Forschungsbedarfe verschlechterte sich des Weiteren der Konsens in Runde drei. In zehn Fällen verzeichnete der Konsens eine Stagnation. Für die Forschungsbedarfe ergibt sich hinsichtlich der Konsensmerkmale gemäß den Methoden des Variationskoeffizienten und der Interquartilsabstände im Gegensatz zu den Anforderungen kein konsistentes Ergebnis. Forschungsbedarf §47 hat gemäß beiden Methoden keinen Konsens erzielt. Für die Forschungsbedarfe §13, §14, §15, §26, §43, §49, §51, §52, §53, §54, §52 ist fraglich, ob ein Konsens erreicht wurde (entweder kein Konsens gemäß Variationskoeffizient oder Interquartilsabstand). Für alle weiteren Forschungsbedarfe, einschließlich aller Forschungsbedarfe auf den ersten zehn Rängen, kann ein Konsens unter den Experten angenommen werden.

Zur Bestimmung der Stabilität der Anforderungen und Forschungsbedarfe wurde der Kruskal-Wallis-Test (Kruskal und Wallis 1952) herangezogen und für alle Anforderungen und Forschungsbedarfe durchgeführt. Für die Anforderungen können hierbei keine signifikanten Änderungen festgestellt werden (Signifikanzniveau $\alpha=0{,}1$). Eine signifikante

Änderung (ebenfalls α=0,1) ergibt sich bei den Forschungsbedarfen lediglich für Forschungsbedarf §55 (p=0,07). Basierend auf dem Kruskal-Wallis-Test kann daher geschlussfolgert werden, dass Stabilität bei den Anforderungen und Forschungsbedarfen erzielt wurde.

Die Analyse der Stabilität kann außerdem mit Hilfe des Vergleichs des Mittelwerts, des Rangs, der Standardabweichung und des Variationskoeffizienten von zwei aufeinanderfolgenden Befragungsrunden bestimmt werden. In der Literatur werden jedoch keine konkreten Grenzwerte genannt, die es ermöglichen würden festzulegen, ob Stabilität für eine bestimmte Anforderung bzw. Forschungsbedarf erreicht wurde. Daher werden im Folgenden die Extremwerte aufgegriffen und diskutiert. Vergleicht man die Ränge aus den Runden 2 und 3 ergeben sich für die Anforderungen #5 (-5), #9 (-4), #10 (+4), #11 (+4) erhebliche Änderungen. Hervorzuheben ist außerdem, dass die ersten beiden Ränge gleichbleiben. Wie bereits angesprochen findet bei den Mittelwerten eine Polarisierung statt. Des Weiteren verzeichnen die Anforderungen #3 (+0,38), #5 (+0,37), #18 (-0,30) besonders große Veränderungen, die jedoch verglichen mit der sechsstufigen Skala moderat erscheinen. Im Rahmen des Vergleichs der Standardabweichungen sticht die Veränderung der Anforderung #9 (-0,6), welche auch eine erhebliche Verbesserung des Ranges verzeichnet, hervor. Die größte Veränderung bei den Variationskoeffizienten ist ebenfalls bei Anforderung #9 mit -0,12 zu verzeichnen. Wiederum ist festzustellen, dass insbesondere die Variationskoeffizienten der ersten beiden Anforderungen mit -0,01 und -0,03 kaum Veränderungen aufweisen.

Bei den Forschungsbedarfen sind die Veränderungen in den Rängen größer, was aufgrund der untersuchten Anzahl an Forschungsbedarfen von insgesamt 55, nicht überraschend ist. Insgesamt weisen 7 Forschungsbedarfe eine Veränderung von mehr als 10 Rängen auf. Die 10

am wichtigsten eingeschätzten Forschungsbedarfe erscheinen wesentlich stabiler. Auffallend ist in diesem Bereich jedoch der auf Rang 1 bewertete Forschungsbedarf, der in Runde 3 eine Verbesserung um 13 Ränge verzeichnet. Die Veränderungen bei den Standardabweichungen zeigen für die Forschungsbedarfe bei den Extremwerten wesentlich größere Veränderungen als dies für die Anforderungen festgestellt wurde. Der größte Wert liegt hier für Forschungsbedarf §36 bei -0,81. Folglich zeigt sich, da ebenfalls eine sechsstufige Skala verwendet wurde, ein ähnliches Bild für die Veränderungen in den Variationskoeffizienten zwischen Befragungsrunde 2 und 3. Betrachtet man lediglich die ersten 10 Ränge zeigen sich wiederum wesentlich geringere Veränderungen in den Standardabweichungen und Variationskoeffizienten zwischen Befragungsrunde 2 und 3. Ausnahme ist hier wiederum der auf Platz 1 bewertete Forschungsbedarf.

Obwohl nur wenige andere Studien die Veränderungen der Standardabweichungen und Variationskoeffizienten explizit darstellen, erscheinen die Veränderungen im Durchschnitt klein (bspw. verglichen mit Wamba und Ngai 2012, S. 2884, die eine fünfstufige Likert-Skala einsetzen). Dies gilt insbesondere für die Anforderungen und die ersten 10 Ränge der Forschungsbedarfe. Zu Bedenken ist, dass durch das Feedback der Mittelwerte in Runde 3 an das Teilnehmerpanel insbesondere extreme Ausreißer eliminiert wurden. Es ist zu vermuten, dass dies ein wesentlicher Einflussfaktor insbesondere auf die Größe der Streuungsmaße (Standardabweichung und Variationskoeffizient) in der dritten Delphi-Runde war. Eine weitere Untersuchung der Anforderungen und Forschungsbedarfe mit auffälligen Werten bzgl. Konsens und Konsensverbesserung sowie Stabilität wäre sinnvoll. Bspw. hätte man in einer weiteren Befragungsrunde lediglich die Anforderungen und Forschungsbedarfe mit großen Abweichungen weiter betrachten

können. Insgesamt kann geschlussfolgert werden, dass die Analyse der deskriptiven Statistiken die Ergebnisse des Kruskal-Wallis-Tests bestätigen und somit größtenteils Stabilität erreicht wurde.

4.4 Grenzen der Studie

Erstens ist als Einschränkung der vorliegenden Delphi-Studie die limitierte Anzahl an Experten zu nennen. Delphi-Studien basieren generell nicht auf einer repräsentativen Stichprobe (Powell 2003; Okoli und Pawlowski 2004, S. 19). In der Literatur wird eine Panelgröße von 10 bis 18 Teilnehmern als optimal angesehen (Okoli und Pawlowski 2004, S. 18), welche in dieser Studie erreicht wurde. Eine solche Panelgröße ist ebenso in vergleichbaren Studien üblich (Okoli und Pawlowski 2004, S. 18-19). Des Weiteren ist anzumerken, dass durch eine heterogene Zusammensetzung des Expertenpanels möglichst viele unterschiedliche Sichtweisen berücksichtigt werden konnten. Wie die Auswertung der demografischen Daten der Experten zeigt, wurde dies erreicht. Trotzdem muss man bei einer Verallgemeinerung von Ergebnissen aus Delphi-Studien grundsätzlich vorsichtig sein. Eine weitere allgemeine Einschränkung von Delphi-Studien ist die Vielzahl an Freiheiten bei der Festlegung des Forschungsdesigns. Wie von Pare et al. (2013, S. 214-215) empfohlen, wurde versucht getroffene Entscheidungen bzgl. des Forschungsdesigns durch ähnliche Studien zu begründen.

Weiterhin ist darauf hinzuweisen, dass die Auswahl der Experten von entscheidender Bedeutung für die Qualität von Delphi-Studien ist (Linstone und Turoff 1975; Powell 2003). Um dem Rechnung zu tragen, wurde ein strukturierter Prozess zur Auswahl der Experten verwendet. Außerdem zeigt die Selbsteinschätzung der Expertise eine durchgehend hohe Kompetenz. Darüber hinaus wurde durch die sequentielle Versendung der Einladungen zur ersten Befragungsrunde

versucht, eine möglichst heterogene Zusammensetzung des Expertenpanels zu erreichen. Naturgemäß kann jedoch die tatsächliche Zusammensetzung nur eingeschränkt beeinflusst werden, und es ist nicht vollständig auszuschließen, dass durch eine Überrepräsentation einzelner Expertengruppen Verzerrungen entstanden sind. Wie jedoch die Diskussion der Ergebnisse zeigt, sind in den Daten keine konkreten Anzeichen für solche Verzerrungen zu finden. Weitere Einschränkungen hinsichtlich des lediglich schwachen Konsenses sowie die Berechnung von Mittelwert und Standardabweichung für Daten aus Likert-Skalen wurden bereits an den entsprechenden Stellen diskutiert.

Abschließend wird darauf hingewiesen, dass zur Bestimmung der Bedeutung der Anforderungen für einzelne Industrien bzw. für bestimmte Gegebenheiten, wie die konkrete Relevanz für IT-Abteilungen, weitere Untersuchungen notwendig sind. Die Studie macht weiterhin keine Aussagen über die Beziehungen und auch Vorbedingungen für die jeweiligen Anforderungen und Forschungsbedarfe. So können einzelne Anforderungen bspw. bei einem geringen GRC-Reifegrad von hoher Bedeutung sein und andere wiederum wichtig zur Weiterentwicklung bereits ausgereifter GRC-Management-Systeme. Auch im Bereich der Forschungsbedarfe kann die Lösung eines Forschungsbedarfs z.B. eine Vorarbeit zur Lösung eines anderen sein.

4.5 Zwischenfazit

Die vorliegende Delphi-Studie hat zwei Ziele verfolgt.

1. Evaluierung der Ergebnisse des Literaturreviews
2. Priorisierung von Anforderungen und Forschungsbedarfen

Ziel 1 wurde insbesondere in der ersten Befragungsrunde adressiert. Insgesamt 19 Teilnehmer mit unterschiedlichen Hintergründen und

hoher Expertise haben in dieser Delphi-Runde die Listen der Anforderungen und Forschungsbedarfen aus dem Literaturreview evaluiert. Hierbei wurden Kommentare zu einzelnen Anforderungen und Forschungsbedarfen gemacht sowie Ergänzungen vorgenommen. Insgesamt wurden die Ergebnisse aus dem Literaturreview bestätigt. Dies wird auch durch die Bewertung der Bedeutung der Anforderungen und Forschungsbedarfe in den Befragungsrunden 2 und 3 ersichtlich.

Das zweite genannte Ziel wurde in den Runden 2 und 3 der Delphi-Studie verfolgt. Obwohl die Studie wie jeder Forschungsansatz mit Einschränkungen verbunden ist, kann angenommen werden, dass die vorliegende Delphi-Studie einer einfachen Expertenbefragung hinsichtlich der Qualität der Befragungsergebnisse überlegen ist. Okoli und Pawlowski (2004, S. 19-20) vergleichen traditionelle Befragungen mit Delphi-Studien anhand unterschiedlicher Kriterien. Hierbei wird deutlich, dass Delphi-Studien, für Forschungssituationen, die eine Qualifizierung von Expertenmeinungen erfordern, überlegen sind. Sie erfordern lediglich die Erfüllung moderater Anforderungen unter anderem hinsichtlich der Panelgröße und sind flexibel hinsichtlich des Designs. Sie bieten weiterhin die Möglichkeit der Evaluierung und Priorisierung innerhalb eines einzigen Forschungsdesigns. Durch ein kontrolliertes Feedback über mehrere Befragungsrunden erzeugen Delphi-Studien reichhaltigere Daten als klassische Befragungen. Hierbei erfolgt zudem eine Stabilisierung und Konsensbildung der Antworten. Dieser Effekt konnte auch für die vorliegende Studie gezeigt werden.

Weitere Forschung zu Anforderungen und Forschungsbedarfen für ein strategisches GRC-Management könnte zuallererst die genannten Einschränkungen der Studie adressieren. So sind ähnliche Studien denkbar, die einzelne Expertenbereiche wie bspw. IT-Leiter adressieren, und so konkretere Hinweise zu einzelnen Anwendungsfällen geben können.

Außerdem könnten weitere Analysen zu einzelnen Anforderungen und Forschungsbedarfen durch persönliche Interviews von GRC-Experten erfolgen, welche tiefergehende Erkenntnisse liefern würden. Letztlich wären auch die Beziehungen zwischen den einzelnen Anforderungen und Forschungsbedarfen zu untersuchen.

Die Anforderungen stellen eine umfassende Strukturierung des Themengebiets strategisches GRC-Management dar und bieten für die Praxis konkrete Anknüpfungspunkte wie GRC-bezogene Management-Systeme aufgebaut oder weiterentwickelt werden können. Obwohl bspw. im Rahmen der Anforderungskategorie Integration Integrationsarten identifiziert wurden, machen die Anforderungen keine Aussagen über konkrete Integrationsbedarfe und -möglichkeiten auf Informationsebene. Diese sind jedoch für die Entwicklung von Informationssystemen für das strategische GRC-Management und damit für die Wirtschaftsinformatik von besonderer Bedeutung. Die Eingrenzung des Themengebietes strategisches GRC-Management macht es aus dem Blickwinkel der Wirtschaftsinformatik erforderlich, die relevanten Informationen zu identifizieren und in Beziehung zu setzen. Im folgenden Kapitel werden daher die für das strategische GRC-Management relevanten Informationen fokussiert und ein datenseitiges Modell entwickelt sowie evaluiert. Hiermit wird ein konkreter Beitrag für die Entwicklung von Informationssystemen für das strategische GRC-Management geleistet.

5 Datenseitiges Modell für das strategische GRC-Management[86]

5.1 Motivation und Ziele

Die bisherige Arbeit zeigt, dass eine einheitliche Terminologie im Kontext von GRC noch nicht oder nur sehr eingeschränkt vorliegt. Es existieren zwar einige Arbeiten, die versuchen die terminologischen Grundlagen zu legen und insbesondere die Begriffe zu definieren sowie in einen Zusammenhang zu bringen, wie noch zu zeigen sein wird, ist dies bislang jedoch nur eingeschränkt gelungen.[87] Des Weiteren lässt das durchgeführte Literaturreview die Beobachtung zu, dass eine Schwerpunktsetzung auf den Managementprozessen von GRC liegt. Hervorzuheben ist hierbei das Rahmenwerk COBIT (ITGI 2007), das im Wesentlichen eine Darstellung der für eine IT-Governance relevanten Prozesse beinhaltet. Aber auch im Kontext von integrierten GRC-Ansätzen stellen sowohl Racz et al. (2010c) als auch das GRC Capability Model von der OCEG (2009) den Prozess des GRC-Managements ins Zentrum ihrer Betrachtungen. Insgesamt zeigt die Analyse der vorhandenen GRC-Ansätze, dass ein Herausarbeiten der Integrationsaspekte sowie eine Eingrenzung des Themengebiets auf der Grundlage eines Modells für die GRC-Management-Prozesse nur eingeschränkt möglich sind.

---

[86] Die Forschungsergebnisse, welche in diesem Kapitel dargestellt werden, wurden bereits in folgenden Veröffentlichungen thematisiert: Marekfia und Nissen (2013); Marekfia und Nissen (2014); Nissen und Marekfia (2014).

[87] Siehe Abschnitt 5.3.1.1.

Es wird daher argumentiert, dass der Ausgangspunkt zur wissenschaftlichen Entwicklung eines GRC-Management-Ansatzes in einer Analyse der strukturellen Zusammenhänge der für GRC relevanten Informationen liegen sollte. Die Identifikation der für GRC relevanten Informationen ist gleichzeitig ein Beitrag zur Eingrenzung des Themengebietes sowie zur Vereinheitlichung der Terminologie. Das in diesem Kapitel behandelte Forschungsziel ist daher die Entwicklung eines fachkonzeptionellen Modells für das strategische GRC-Management, das sich auf die Informationsstruktur beziehen soll.[88] Hiermit sollen zwei Forschungsfragen beantwortet werden.

1. Welches sind die konstituierenden Informationsobjekte eines strategischen GRC-Managements?
2. Welche Beziehungen weisen die Informationsobjekte auf?[89]

Informationsobjekte sind hierbei als informationstechnisch motivierte Abbildung von verschiedenen Informationen zu verstehen. Der Begriff des Informationsobjekts ist somit gleichzusetzen mit den Begriffen Entität (bspw. Entity Relationship Modell, Chen 1976) oder Klasse (bspw. Klassendiagramm der Unified Modeling Language (UML)

[88] Wie in Abschnitt 5.1 und 5.2.1 ausgeführt wird, wird die Entwicklung eines fachkonzeptionellen Datenmodells für ein strategisches GRC-Management angestrebt. Es wird im Weiteren daher auch von einem datenseitigen Modell gesprochen.

[89] Die in diesem Abschnitt bearbeiteten Forschungsfragen behandeln insbesondere den Forschungsbedarf §48. Obwohl diesem Forschungsbedarf in der Delphi-Studie lediglich eine Bedeutung von 4,15 beigemessen wurde, legt das hier entwickelte Modell jedoch essentielle Grundlagen und hat somit einen Einfluss auf vielfältige weitere Forschungsbearfe. So trägt es zur Analyse der Integration der GRC-Disziplinen (insb. Forschungsbedarf §13) bei und leistet hierbei auch einen Beitrag zur Harmonisierung der Terminologie. Des Weiteren stellt das datenseitige Modell einen Ausgangspunkt zur Entwicklung eines Referenzmodells für GRC-Software dar (Forschungsbedarf §40). Insgesamt trägt es somit wesentlich zur Grundlegung eines allgemeinen Verständnisses für ein strategisches GRC-Management bei, welches das Ziel dieser Forschungsarbeit ist.

(OMG 2010a; OMG 2010b)). Dieses Modell soll als Grundlage für das Management von Informationen dienen, die für das strategische GRC-Management relevant sind. Somit kann es sowohl als Grundlage für die Entwicklung von Informationssystemen als auch hinsichtlich der Organisationsgestaltung nützlich sein. Es kann weiterhin als Bezugsrahmen für die Entwicklung unternehmensspezifischer Modelle dienen. Dieses Kapitel ist im Anschluss wie folgt strukturiert. Abschnitt 5.2 führt in die Methodik der Referenzmodellierung ein. In Anlehnung an den Prozess gestaltungsorientierter Forschung (Peffers et al. 2006; Peffers et al. 2007; Österle et al. 2010) wird im Anschluss in Abschnitt 5.3 das Modell entworfen, dargestellt sowie anhand eines Demonstrationsbeispiels illustriert. In Abschnitt 5.4 wird die Evaluierung des Modells betrachtet. Abschnitt 5.5 diskutiert die Grenzen der hier durchgeführten Modellierung. Das Kapitel schließt mit einem Fazit in Abschnitt 5.6.

5.2 Methodik der Referenzmodellierung

5.2.1 Grundlagen und Einordnung

Referenzmodelle sind Modelle[90], die in einer konkreten Modellierungssituation zur Entwicklung von speziellen Modellen verwendet werden können. Sie weisen das Merkmal der Wiederverwendung auf. Dies bedeutet, dass Referenzmodelle entweder mit dem Zweck der Wiederverwendung entworfen oder faktisch wiederwendet werden. Des Weiteren werden Referenzmodelle mit einer gewissen Allgemeingültigkeit, da diese eine Klasse von Anwendungsfällen unterstützen sollen, und einem Empfehlungscharakter in Verbindung gebracht (siehe bspw.

[90] Zur Definition des Begriffs Modell siehe Abschnitt 1.3.

Delfmann 2006, S. 45-47; Fettke 2006b; Thomas 2006, S. 82-95; vom Brocke 2003, S. 31-34).[91] Bekannte Referenzmodelle existieren von Scheer (1997) für Industriebetriebe sowie Becker und Schütte (2004) für Handelsunternehmen. Im Unterschied zu Ontologien, die ebenfalls geeignet wären die Semantik von Konzepten zu definieren und somit die Struktur von GRC zu explizieren (siehe hierzu auch Wolf und Goeken 2010), besitzen Referenzmodelle einen Empfehlungscharakter (zur ausführlichen Abgrenzung der Begriffe siehe Zelewski 1999, S. 11-13).

Referenzmodellierung kann einer prozessorientierten Sichtweise folgend in zwei Prozesse unterteilt werden. Der erste Prozess ist die Konstruktion des Referenzmodells. Der zweite Prozess ist die Konstruktion unternehmensspezifischer Modelle auf Grundlage des Referenzmodells und stellt somit die Anwendung des Referenzmodells in einer konkreten Modellierungssituation dar. Beide Prozesse sind in der Regel sowohl zeitlich als auch personell voneinander getrennt (Fettke und Loos 2002, S. 10; Fettke und Loos 2004b, S. 18-19, vom Brocke 2003, S. 34-37). In die Prozesse der Referenzmodellierung sind demzufolge der Referenzmodellkonstrukteur, der Anwendungsmodellkonstrukteur, welcher gleichzeitig der Referenzmodellnutzer ist, und der Anwendungsmodellnutzer involviert (vom Brocke 2003, S. 34-37). Darüber hinaus sind Konstruktionstechniken relevant, die spezifische Regeln beinhalten und somit die Übernahme, Adaption und Ergänzung von Inhalten von Referenzmodellen ermöglichen. Zu diesen etablierten Techniken gehören die Konfiguration, die Instanziierung, die Aggregation, die Spezialisierung und die Analogie (Delfmann 2006, S. 94-184;

[91] Die forschungsmethodischen Probleme, die mit den genannten Eigenschaften von Referenzmodellen verbunden sind, werden in vom Brocke (2003, S. 31-34) diskutiert.

vom Brocke 2003, S. 269). Für diese Arbeit ist lediglich der erste Prozess, also die Erstellung des Referenzmodells relevant.

Für die Referenzmodellierung existieren verschiedene Methodensysteme, wie ARIS (Scheer 2001; Scheer 2002), MEMO (Frank 1994; Frank 2002), die Enterprise Architecture at Work (ArchiMate) (Lankhorst 2005) oder das semantische Objektmodell (Ferstl und Sinz 1990; Ferstl und Sinz 1991; Ferstl und Sinz 1995), welche die verschiedenen Arten und Perspektiven der Referenzmodellierung hinsichtlich einer umfassenden Organisationsmodellierung strukturieren. Im Folgenden wird ARIS zur Einordnung des eigenen Forschungsvorhabens verwendet. Es ist darauf hinzuweisen, dass hiermit keine Vorfestlegung auf ein bestimmtes Methodensystem erfolgt, sondern die Erweiterung des hier vorgestellten, auf Datenaspekte fokussierenden Modells bspw. um Aspekte der Aufbauorganisation, weiterhin mit allen zuvor genannten Methodensystemen erfolgen kann. ARIS ist ein von Scheer (Scheer 2001; Scheer 2002) entwickeltes Methodensystem, das zwischen der Organisationssicht, der Funktionssicht, der Datensicht sowie der Steuerungssicht als Zusammenführung der vorgenannten Sichten unterscheidet. Jede dieser Sichten wird in den drei Ebenen Fachkonzept, Datenverarbeitungskonzept und Implementierung betrachtet. ARIS ordnet jeder Sichten-Ebenen-Kombination Darstellungstechniken zu. Diese sind für die Ebene des Fachkonzepts die EPK (Keller et al. 1992) in der Steuerungssicht und Entity Relationship (ER) Diagramme (Chen 1976) in der Datensicht. Die UML (OMG 2010a; OMG 2010b) beinhaltet verschiedene objektorientierte Diagrammarten, die sowohl die Struktur, als auch das Verhalten und die Interaktion fokussieren. Klassendiagramme können als Kernbestandteil objektorientierter Modelle betrachtet werden, wobei die Struktur betrachtet wird und hohe Ähnlichkeiten zu fachkonzeptionellen Datenmodellen von ARIS bestehen.

Aktivitätsdiagramme betrachten das Verhalten und dienen ebenso wie EPKs zur Abbildung von Geschäftsprozessen (vom Brocke 2003, S. 121-128). ARIS unterstellt, dass für die vollständige Beschreibung eines Referenzmodells alle Sichten und Ebenen zu betrachten sind. Zum Zweck der Anwendungssystemgestaltung sind die Steuerungssicht und die Datensicht wesentlich. Für die Organisationsgestaltung ist darüber hinaus die Sicht der (Aufbau-)Organisation relevant. Die Funktionssicht kann in beiden Fällen durch die Steuerungssicht substituiert werden (vom Brocke 2003, S. 112).

In dieser Arbeit wird argumentiert, dass ein Referenzmodell für ein integriertes GRC-Management auf dem Verständnis der Struktur im Sinne der konstituierenden Informationsobjekte und Beziehungen aufbauen sollte. Daher wird in dieser Arbeit die Datensicht in den Mittelpunkt gestellt. Es wird zudem keine Implementierung in ein Informationssystem angestrebt, sondern es sollen die relevanten Informationen aus konzeptioneller Sicht betrachtet werden. Das hier zu entwickelnde Modell stellt somit ein fachkonzeptionelles Datenmodell dar. Das Modell soll als Referenz für eine konkrete Modellierungssituation dienen, und es wäre wünschenswert, wenn das Modell vielfältige Anwendungen findet. Für ein umfassendes Referenzmodell des strategischen GRC-Managements sind jedoch weitere Anstrengungen notwendig, welche die hier eingenommene Datensicht unter anderem um Referenz-Managementprozesse von GRC ergänzen. Daher wird in dieser Arbeit das eigene Modell nicht als Referenzmodell bezeichnet. Die Methodik der Referenzmodellierung ist jedoch aufgrund des Forschungsziels anwendbar.

5.2.2 Strukturierung des Forschungsprozesses

Die Referenzmodellierung ist eine in der Wirtschaftsinformatik etablierte Forschungsmethode (Wilde und Hess 2007, S. 282), die dem gestaltungsorientierten Forschungsparadigma (Hevner et al. 2004) zugeordnet werden kann. Grundsätzlich sind somit die allgemeinen Forschungsprozesse der gestaltungsorientierten Forschung einschlägig (Hevner et al. 2004; Hevner und Chatterjee 2010; March und Smith 1995; Österle et al. 2010).[92] Darüber hinaus existieren für die Referenzmodellierung auch spezielle Vorgehensmodelle, die den Forschungsprozess gliedern. Im Wesentlichen erfolgt hierbei eine Konkretisierung der notwendigen Schritte zur Entwicklung und Evaluierung von Referenzmodellen, wobei die Vorgehensweisen zwischen vier bis fünf Phasen umfassen (Fettke 2014, S. 1036). Becker et al. (2002, S. 36) stellen ein Fünf-Phasen-Vorgehensmodell vor, das sich wie folgt gliedert. In Phase 1 soll das Projektziel definiert und hierauf aufbauend die (Referenz-)Modellierungstechnik ausgewählt werden (Phase 2). Anschließend wird das Modell erstellt (Phase 3) und evaluiert (Phase 4). Letztlich ist das Modell zu veröffentlichen und zu vermarkten (Phase 5). Thomas (2006, S. 244) ergänzt diese Schritte um die Identifikation von relevanten Wissensquellen. Es fällt eine hohe Übereinstimmung mit dem allgemeinen Prozess der gestaltungsorientierten Forschung auf. Peffers et al. (2006; 2007) weist darüber hinaus auf die Notwendigkeit einer Demonstration des entwickelten Artefakts hin. Der hier dargestellten Referenzmodellierung liegt in Anlehnung hieran ein Sechs-

[92] Eine Darstellung der Grundlagen gestaltungsorientierter Forschung ist in Abschnitt 1.3 zu finden.

Phasen-Vorgehensmodell zugrunde, das wie in der folgenden Tabelle (Tab. 39) dargestellt, aufgebaut ist.

Tab. 39: Verwendeter Forschungsprozess der Referenzmodellierung in Anlehnung an Becker et al. (2002, S. 36) und Thomas (2006, S. 244)

Nr.	Phase
1	Problem definieren und Projektziel festlegen
2	Adäquate Wissensquellen identifizieren
3	Referenzmodellierungstechnik festlegen
4	Referenzmodell erstellen und demonstrieren
5	Referenzmodell evaluieren
6	Referenzmodell veröffentlichen

Die Problemdefinition und die Festlegung der Projektziele (Phase 1) erfolgte in Abschnitt 5.1. In diesem Abschnitt wird die Identifikation der Wissensquellen (Phase 2) und die Auswahl der Modellierungstechnik (Phase 3) diskutiert. Die Entwicklung, Darstellung und Demonstration des Modells (Phase 4) erfolgt in Abschnitt 5.3. Die Evaluierung (Phase 5) wird in Anschnitt 5.4 dargestellt. Eine Publikation des datenseitigen Modells (Phase 6) wurde bereits durch verschiedene Konferenz- und Journalpublikationen (Marekfia und Nissen 2013; Marekfia und Nissen 2014; Nissen und Marekfia 2014) vorgenommen und erfolgt ebenfalls durch die vorliegende Dissertationsschrift.

5.2.3 Identifikation adäquater Wissensquellen

Im Kontext der Referenzmodellierung existieren zwei grundsätzliche Strategien zur Erkenntnisgewinnung, die sich in Anlehnung an die Unterscheidung in der Wissenschafts- und Erkenntnistheorie in Rationalismus und Empirismus ergeben. Diese sind die deduktive und die induktive Strategie (vom Brocke 2003, S. 31; Fettke 2014, S. 1035; Thomas 2006, S. 93). Beim induktiven Vorgehen werden Modelle ausgehend vom empirischen Fall gewonnen. Deduktiv werden diese aus

grundlegenden Erkenntnissen zum Gegenstand des zu konstruierenden Modells hergeleitet. Hinsichtlich der induktiven Vorgehensweise ist darauf hinzuweisen, dass Referenzmodelle allgemeingültig in dem Sinne sein sollen, dass sie für eine Klasse unternehmensspezifischer Modelle Gültigkeit aufweisen (vom Brocke 2003, S. 31).

Thomas (2006, S. 252-254) unterscheidet im Kontext der Identifikation adäquater Wissensquellen zwischen der strukturellen und sozialen Ebene. Auf struktureller Ebene können Publikationen im Gegenstandsbereich des zu entwickelnden Referenzmodells sowie existierende Informations- und Referenzmodelle als Wissensquellen dienen. Hierzu gehören auch konkrete Unternehmensmodelle aus der Unternehmenspraxis. Außerdem sind in Bezug auf Referenzmodelle für Anwendungssysteme Softwaredokumentationen relevant. Auf sozialer Ebene können Personen- bzw. Personengruppen wie Organisationen oder Unternehmen als Wissensquellen fungieren. Fettke (2014, S. 1035) weist im Kontext der induktiven Strategie zu Recht darauf hin, dass sich die Unternehmensmodellierung zwar vermehrt in der Unternehmenspraxis etabliert hat und somit auch zunehmend unternehmensindividuelle Modelle eine induktive Strategie der Referenzmodellierung ermöglichen würden, jedoch trifft dies hauptsächlich auf Kernprozesse zu, die in Standardsoftware wie ERP-Systemen abgebildet werden. Für innovative Domänen, wie dies auch das strategische GRC-Management ist, existieren solche Modelle nur eingeschränkt. Das in dieser Arbeit vorgestellte Verständnis eines strategischen GRC-Managements ist vielmehr ein normatives Modell, das zukünftig in der Unternehmenspraxis verfolgt werden sollte. Des Weiteren ist der Zugang zu solchen Modellen fraglich, da diese nicht frei zugänglich sind und Unternehmen diese als strategisch relevante Ressource betrachten. In der vorliegenden Arbeit wird davon ausgegangen, dass vorhandene Publikationen im Kontext

von GRC sowie die darin enthaltenen Informations- und Referenzmodelle, die derzeit geeignetste Quelle zur Konstruktion eines datenseitigen Modells für das strategische GRC-Management sind. Dies ist wie folgt begründet.

1. Der bereits dargestellte Literaturreview zeigt, dass obwohl GRC eine neue Forschungsdomäne ist, relevantes Wissen aus den GRC-Teilbereichen existiert und im Sinne einer kumulativen Forschung berücksichtigt werden sollte.
2. Eine Befragung von GRC-Experten ist aufgrund der bislang uneinheitlichen Terminologie aufwendig und schwierig. Insbesondere zu einzelnen Begriffen, die als Bezeichnungen der Entitäten des Modells von besonderer Bedeutung sind, bestehen unterschiedliche Auffassungen.
3. Die für GRC relevanten Publikationen beinhalten eine Reihe von Informations- und Referenzmodellen aus Teilbereichen von GRC, die sich zur Auswertung anbieten. Diese Modelle beinhalten sowohl Ergebnisse aus konzeptionellen Überlegungen sowie Erfahrungswissen, generiert durch empirische Methoden wie die Befragung von Praxisvertretern.

Insgesamt erscheinen existierende Modelle im Kontext von GRC als eine adäquate Quelle. Wie Abschnitt 5.3.1.1 zu entnehmen ist, diskutieren nur wenige Modelle Integrationsaspekte von GRC und vernachlässigen hierbei weitere relevante Anforderungen an ein strategisches GRC-Management. Neben der Auswertung der existierenden Informations- und Referenzmodelle sollen daher die Anforderungen an ein strategisches GRC-Management genutzt werden, da diese das bestehende Wissen hinsichtlich eines strategischen GRC-Management-Ansatzes zusammenfassen. Dies führt zu einer Kombination der induk-

tiven Strategie, als welche die Auswertung der bestehenden Modelle bezeichnet werden kann, sowie der deduktiven Erkenntnisstrategie, die sich aus der Analyse der relevanten Aspekte der Anforderungen an ein strategisches GRC-Management ergibt. Hiermit soll auch der Forderung der Allgemeingültigkeit Rechnung getragen werden, die schwieriger mit einer rein induktiven Strategie zu erfüllen ist (vom Brocke 2003, S. 31).

5.2.4 Festlegung der Modellierungstechnik

Die Festlegung der Modellierungstechnik sollte insbesondere zwei Aspekte beinhalten, die als „way of modeling" und „way of working" bezeichnet werden (Verhoef et al. 1991). Ersteres betrifft die Auswahl der Modellierungssprache. Basierend auf dem dargestellten Projektziel kommen hierfür ER-Diagramme und UML-Klassendiagramme in Frage. Hier werden UML-Klassendiagramme verwendet, da diese mehrheitlich bei den Modellen in der GRC-Literatur eingesetzt wurden. Im Rahmen der hier dargestellten Referenzmodellierung wurden die folgenden Elemente verwendet. Klassen, die im Rahmen dieser Arbeit auch als Informationsobjekte bezeichnet werden, sind durch Rechtecke dargestellt und beinhalten den Klassennamen. Im Rahmen der hier dargestellten fachkonzeptionellen Modellierung wurde auf die Darstellung der Attribute verzichtet. Des Weiteren beinhaltet das Modell Assoziationen und Generalisierungen. Assoziationen werden als Kante zwischen zwei Klassen dargestellt, welche eine Richtung hat und eine Bezeichnung trägt, die jeweils oberhalb bzw. neben der Kante abgebildet sind. Eine Generalisierung ist durch einen Pfeil dargestellt, wobei die Pfeilspitze in die generelle Klasse zeigt. Zur Modellierung wurde Microsoft Visio™ verwendet. Eine datenbankgestützte Modellierung unterstützt durch ein GPM-System war aufgrund der geringen Kom-

plexität des Gesamtmodells nicht notwendig. Eine Modellierung in ER-Diagrammen wäre ebenso angemessen und möglich.

Der „way of working" spricht die Vorgehensweise an, die der Modellerstellung (im engeren Sinne) zu Grunde liegt. Wie bereits ausgeführt werden, um der besonderen Bedeutung von Referenzmodellen Rechnung zu tragen, im vorliegenden Forschungsvorhaben induktive und deduktive Elemente bei der Entwicklung des Modells kombiniert. Daher findet in einem ersten Schritt eine Auswertung von existierenden konzeptionellen Modellen aus der GRC-Literatur statt. In einem zweiten Schritt erfolgt dann ein Abgleich der gefundenen Modellelemente mit den strategischen GRC-Anforderungen. Für die Erstellung des hier thematisierten datenseitigen Modells für ein strategisches GRC-Management sind zwei Aspekte von herausragender Bedeutung.

1. Welches sind die relevanten Informationsobjekte (Klassen bzw. Entitäten) eines strategischen GRC-Managements?
2. Welche Beziehungen existieren zwischen den Informationsobjekten?

Beide Teile der Vorgehensweise zur Referenzmodellerstellung fokussieren auf diese zentralen Aspekte. Hierzu werden die relevanten Elemente und Beziehungen aus existierenden Modellen im Kontext von GRC analysiert. Diese Vorgehensweise ist im Kontext von Methoden zur induktiven Gewinnung aus existierenden (unternehmensindividuellen) Modellen zu sehen (Fettke 2014). Für das hier dargestellte Forschungsvorhaben ist die Erstellung von sogenannten Synsets zentral. Synsets sind ein linguistisches Konzept, das eine Menge von Wörtern mit gleicher Bedeutung erfasst. Fettke (2014, S. 1041) führt zur Herleitung von Referenzmodellen einen sogenannten Abstraktionsparameter sowie einen Konfigurationsparameter ein. Ersterer erfasst inwieweit Beson-

derheiten der analysierten Modelle bei der Referenzmodellerstellung berücksichtigt werden, also bspw. in wie vielen der analysierten Modelle eine Entität vorkommen muss, damit sie im Referenzmodell berücksichtigt wird. Der Konfigurationsparameter legt fest, ab wann die Aufnahme einer Entität obligatorisch ist. Beide Parameter lassen sich nur unter Berücksichtigung des Ziels der Referenzmodellierung festlegen. Im vorliegenden Fall sollen möglichst alle relevanten Informationsobjekte eines strategischen GRC-Managements erfasst werden. Es wird daher bereits ein Begriff in das Modell aufgenommen, wenn dieser in mindestens zwei Modellen vorkommt. Zusätzlich wird die Häufigkeit des Auftretens einer Entität in den zugrundeliegenden Modellen angegeben, so dass eventuelle Anwender diese Information bei der Entwicklung eines unternehmensindividuellen Modells aufgreifen können. Im Rahmen des Abgleichs der Modellelemente und Beziehungen mit den Anforderungen an ein strategisches GRC-Management wird ein argumentativ-deduktiver Ansatz verfolgt.

5.3 Entwicklung des Modells

5.3.1 Auswertung der existierenden Modelle in der GRC-Literatur

5.3.1.1 Identifikation existierender konzeptioneller Modelle im Kontext von GRC

Das datenseitige Modell soll, wie bereits dargelegt, einen Beitrag zur Eingrenzung und Strukturierung des Themengebietes GRC leisten. Die Literaturrecherche identifiziert einige Arbeiten, die versuchen, dieses Ziel natürlichsprachlich zu erreichen (Hardy und Leonard 2011; Klotz 2009; Klotz und Dorn 2008; Krey 2010; Krey 2012; Krey et al. 2012; Menzies 2006; OCEG 2009; Puspasari et al. 2011; PwC 2004; PwC 2007; Racz et al. 2010b; SAP 2009; Schöler und Zink 2008; Tarantino

2007; Teubner und Feller 2008). Hierbei wird im Wesentlichen die Analyse von einem GRC-Bereich wie dem Compliance-Management gestartet und hierauf basierend die Idee eines integrierten GRC-Managements entwickelt. Eine thematische Eingrenzung lässt sich dadurch nur schwierig gewinnen, da über die Begriffe (Corporate) Governance, Risiko- und Compliance-Management hinausgehend, eine Vielzahl weiterer Begriffe genannt werden, die mit GRC in Verbindung stehen sollen (Hardy und Leonard 2011, S. 3-4). So nennen Racz et al. (2010b, S. 8) Strategie, Prozesse, Menschen und Technologie als grundlegende Komponenten von GRC. Vicente und da Silva (2011b, S. 202) bezeichnen basierend auf einer weiteren Studie von Racz et al. (2011c), „Audit Management", „Policy Management", „Issue Management" und „Risk Management" als Kernfunktionalitäten von GRC. Krey et al. (Krey 2010, S. 7-9; Krey et al. 2012, S. 2881-2882) identifizieren insgesamt sechs sogenannte „focus areas", die als relevant für einen GRC-Ansatz erachtet werden. Hierzu gehören „strategic alignment (business-IT-alignment)", „value delivery", „resource management", „performance measurement, „risk management" und „compliance". Es wird deutlich, dass bei Krey neben der Aufzählung der GRC-Teilbereiche Risiko- und Compliance-Management lediglich eine Konkretisierung der Governance-Aspekte stattfindet.

Hinsichtlich der Beziehungen von GRC existieren einfache schematische Darstellungen. Frühe Arbeiten von PwC (2007, S. 15-17) bzw. Menzies (2006, S. 334-336) ordnen die Teilbereiche von GRC entlang der Unternehmenshierarchie. Corporate Governance ist demnach an der Unternehmensspitze angeordnet, das Risikomanagement ist in der Mitte als Aufgabe des mittleren Managements dargestellt und die Compliance wird als operative Aufgabe verstanden. In neueren Arbeiten hat sich das sogenannte GRC-Dreieck durchgesetzt (Klotz 2009, S. 8-11;

Klotz und Dorn 2008, S. 6-10; Kranawetter 2009, S. 24; Puspasari et al. 2011, S. 312; Racz et al. 2010b; SAP 2009, S. 8; Schöler und Zink 2008, S. 17-18)[93], das die GRC-Elemente durch Beziehungen verbindet und teilweise Erläuterungen für die jeweiligen Beziehungen enthält. Darüber hinaus existieren schematische Darstellungen, die unter anderem IT-GRC als Teilbereich der unternehmensweiten GRC darstellen oder die Bedeutung der IT im Kontext von GRC schematisch darstellen (Klotz 2009, S. 8-11; Klotz und Dorn 2008, S. 6-10; Racz et al. 2010b, Teubner und Feller 2008). Racz. et al. (2010b) entwickeln eine Definition für GRC auf der Grundlage eines Literaturreviews sowie eines Online-Fragebogens. Darüber hinaus wird ein Rahmenwerk für GRC entwickelt, welches das GRC-Dreieck um weitere Aspekte ergänzt. Hierbei wird GRC als integrierter, ganzheitlicher und organisationsweiter Ansatz charakterisiert, der die Komponenten Strategie, Prozesse, Menschen und Technologie umfasst. Die Darstellung der Beziehungen von GRC bleibt jedoch schematisch und auf das GRC-Dreieck beschränkt.

Die natürlichsprachlichen Analysen ebenso wie die Versuche GRC durch schematische Darstellungen aufzubereiten geben zwar einen ersten Eindruck von den relevanten Informationen sowie deren Beziehungen, sind jedoch für eine detaillierte Analyse nur eingeschränkt geeignet. Daher wird im Folgenden der Fokus auf existierende konzeptionelle Modelle im Kontext von GRC gelegt. Zur Identifikation von Modellen in der Literatur, die hier von Bedeutung sind, wurde das Ergebnis der Literatursuche herangezogen (siehe Abschnitt 3.1). In den dort für das strategische GRC-Management relevanten Arbeiten wur-

[93] Siehe ebenso Abschnitt 2.6.

den Informations- und Referenzmodelle[94], welche die Datenstruktur betrachten, identifiziert. Die folgenden Tabellen (Tab. 40 und Tab. 41) stellen die Ergebnisse dieses Arbeitsschrittes dar und ordnen den einzelnen Modellen den jeweiligen Gegenstand der Modellierung basierend auf den GRC-Teilbereichen zu. Insgesamt wurden 35 relevante Modelle identifiziert.

[94] Die bei der Auswertung der GRC-Literatur identifizierten Informations- und Referenzmodelle werden im Folgenden auch als Quellmodelle der hier vorgenommenen Modellierung bezeichnet.

Tab. 40: Übersicht der ausgewählten Informations- und Referenzmodelle aus der GRC-Literatur (1 von 2)

Nr.	Titel	Gegenstand	Quelle
1	Interrelationships of COBIT Components	IT-Governance	ITGI 2007, S. 8
2	Relationships between Process Modeling and Control Modeling Concepts	Compliance	Sadiq et al. 2007, S. 5
3	Selected correspondences between business process and risk	Risikomanagement	Sienou et al. 2008, S. 24
4	Conceptual model of the compliance management problem	Compliance	Silveira et al. 2009, S. 5
5	A basic high level model for regulatory compliance	Compliance	El Kharbili et al. 2008b, S. 4; El Kharbili et al. 2008c, S. 180
6	Policy Ontology	Compliance	El Kharbili et al. 2008c, S. 187; El Kharbili und Pulvermüller 2009, S. 72
7	Rule Ontology	Compliance	El Kharbili et al. 2008c, S. 188; El Kharbili und Pulvermüller 2009, S. 73
8	A MOF/UML metamodel of a business protocol model	Compliance	Goedertier und Vanthienen 2006a, S. 562
9	A MOF/UML metamodel of an obligation	Compliance	Goedertier und Vanthienen 2006a, S. 563
10	A MOF/UML metamodel of a conditional commitment	Compliance	Goedertier und Vanthienen 2006a, S. 563
11	Rule ontology (constraints)	Compliance	Weigand et al. 2011, S. 794
12	The upper domain model of the Internal Controls Compliance	Compliance	Namiri und Stojanovic 2007a, S. 62; Namiri und Stojanovic 2007b, S. 63
13	Relationship between an Application Control and a Business Process	Compliance	Namiri und Stojanovic 2007a, S. 62; Namiri und Stojanovic 2007b, S. 63
14	A semi-formalization of the control implementation	Compliance	Namiri und Stojanovic 2007a, S. 63; Namiri und Stojanovic 2007b, S. 69
15	IT Risk Reference Model	Risikomanagement	Sackmann 2008a, S. 4
16	Meta-Referenzmodell zum Compliance-Management	Compliance	Teuteberg und Freundlieb 2009, S. 555

Tab. 41: Übersicht der ausgewählten Informations- und Referenzmodelle aus der GRC-Literatur (2 von 2)

Nr.	Titel	Gegenstand	Quelle
17	A Classification Model for Automating Compliance	Compliance	Sackmann 2008c, S. 41; Sackmann et al. 2008, S. 81
18	Beispielhafter Auszug einer (initialen) Corporate Rule Base	GRC	Menzies 2006, S. 364
19	ISO 27001 Metamodell	Risikomanagement / Compliance	Milicevic und Goeken 2010
20	The oracle corporate analysis flow	Compliance	Pohlman 2008, S. 42
21	The regulatory mandate and compliance framework control domain relationship	Compliance	Pohlman 2008, S. 43
22	Risk Management Concepts	Risikomanagement	Barateiro et al. 2012, S. 3297
23	Meta-Reference Model for Risk and Compliance Management in the Cloud	Risiko- und Compliance-Management	Martens und Teuteberg 2011, S. 4
24	IT GRC application architecture that represents the connectivity between each of these domains	GRC	Puspasari et al. 2011
25	Kontrollmodell	Risiko- und Compliance-Management	Sackmann et al. 2013, S. 32
26	Concept map for audit relevant information	Risiko- und Compliance-Management	Schultz et al. 2012, S. 11
27	Semantic net of key domain concepts as preliminary step towards method design	Risikomanagement	Strecker et al. 2011
28	Excerpt of the RISKML meta model	Risikomanagement	Strecker et al. 2011
29	Key concepts of the business process compliance model	Compliance-Management	Turetken et al. 2011, S. 7
30	The conceptual model for the compliance repository's key elements	Compliance-Management	Turetken et al. 2012, S. 29
31	Integrated GRC Conceptual Model / Conceptual model for GRC	GRC	Vicente und da Silva 2011a, S. 209; Vicente und da Silva 2011b, S. 3
32	Conceptual meta model of the SBPML notation extended by the new risk view	Compliance-Management	Weiss und Winkelmann 2011, S. 4
33	Auszug der Ontologie des URM (Ebene 2 – Verfeinerung (RM-Gegenstandsbereich))	Risikomanagement	Wolf und Goeken 2011, S. 12

Nr.	Titel	Gegenstand	Quelle
34	Ontologisches Metamodell von COBIT	IT-Governance	Alter und Goeken 2009, S. 254
35	Meta-Model Domain Integration	Compliance-Management	Zoet et al. 2011, S. 455

Menzies (2006, S. 362-366) stellt mit der sogenannten „Corporate Rule Base“ einen ersten Ansatz vor, der die für das GRC-Management relevanten Informationen identifiziert und zueinander in Beziehung setzt. Im Rahmen der Publikation wird dieser Ansatz beispielhaft mit Hilfe einer Tabelle eingeführt, wobei darauf verwiesen wird, dass in der Unternehmenspraxis eine Umsetzung mit Hilfe einer Datenbank wünschenswert ist. Im Kern fokussiert dieser Ansatz, obwohl er explizit eine Integration von GRC ermöglichen soll, auf eine strukturierte Herleitung, Dokumentation und Nachverfolgung der Compliance-Kontrollen im Rahmen eines internen Kontrollsystems. Die einzigen im Rahmen der Literatursuche gefundenen Arbeiten, die eine tiefer gehende Analyse der Elemente und Beziehungen von GRC sowie die Modellierung eines fachkonzeptionellen Modells für einen integrierten GRC-Ansatz liefern, stammen von Vicente und da Silva (2011a; 2011b) sowie Puspasari et al. (2011).

Ausgangspunkt des von Vicente und da Silva (2011a; 2011b) entwickelten Modells stellen die sogenannten Hauptfunktionalitäten „Audit Management“, „Policy Management“, „Issues Management“ und „Risk Management“ dar, die basierend auf einer Studie von Racz et al. (2011c) den Funktionsumfang von GRC-Software begründen sollen. Weitere wichtige Funktionalitäten von GRC-Software werden mit den Begriffen Reporting, Dashboards und Monitoring angeführt. Diesen „Funktionalitäten“ werden anschließend Daten zugordnet. Dies erfolgt in zwei Schritten. Zuerst werden einzelne Modelle für die Teilbereiche von GRC entwickelt. Die Integration ergibt sich durch „übereinanderlegen“

der Modelle für die Teilbereiche und einer Identifikation gemeinsamer Informationen. Diese gemeinsamen Informationen namentlich „Control“, „Policies“, „Risks“ und „Processes“ werden als Kernbereich von GRC herausgestellt. Die Modelle für die GRC-Teilbereiche werden argumentativ-deduktiv auf der Grundlage der Definitionen der GRC-Bereiche entwickelt, wobei eine exakte Herleitung der einzelnen Informationen und Beziehungen fehlt und bestenfalls indirekt erschlossen werden könnte. Insbesondere die Wahl der Begriffe erfolgt ohne Begründung. Existierende Modelle für die Teilbereiche werden nicht berücksichtigt. Des Weiteren beschränkt sich die Arbeit auf den Integrationsaspekt. Die weiteren Anforderungen werden vernachlässigt. Die Evaluierung erfolgt lediglich gegen den Ansatz von der OCEG (2009), der von Vicente und da Silva ebenso für die Herleitung verwendet wird.

Das Forschungsziel von Puspasari et al. (2011) ist die Entwicklung eines Modells für ein IT-GRC-Informationssystem. Der Ausgangspunkt hierfür ist das IT-Risikomanagement in Banken. Zu diesem Zweck wird eine Fallstudie durchgeführt und hierbei Anforderungen durch die Befragung von Anwendern gewonnen. Das dargestellte Modell wird in die fünf Prozesse „policy management“, „risk management“, „compliance/audit management“, „business continuity/disaster recovery planning“ und „incident management” aufgeteilt, welche gleichzeitig die Module der Software darstellen sollen. Innerhalb dieser Prozesse werden die relevanten Informationen gemäß dem Prozessablauf dargestellt. Insgesamt erscheint das Modell sehr spezifisch für den betrachteten Fall des Risikomanagements einer Bank zu sein. Eine Herleitung der genannten Prozesse und Modellelemente aus den durch Interviews gewonnenen Benutzeranforderungen ist nicht Teil des Forschungspapiers. Insgesamt wird zwar das IT-Risikomanagement teilweise um Aspekte aus Governance und Compliance erweitert, jedoch

bleibt eine technische Perspektive auf das IT-Risikomanagement als Schwerpunkt erhalten.

Es existieren weitere fachkonzeptionelle Modelle im Kontext von GRC. Zum Teil sollen diese, die in den jeweiligen Arbeiten betrachtete Domäne lediglich konzeptualisieren und basieren nur auf grundlegenden Überlegungen (siehe Tab. 40/Tab. 41: 1, 2, 4, 5, 18, 20, 21, 22, 25, 27), ohne dass hierbei ein systematischer Forschungsprozess einschließlich einer Evaluierung erfolgen würde. Ein anderer Teil der Arbeiten (siehe Tab. 40/Tab. 41: 3, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 19, 23, 24, 26, 28, 29, 30, 31, 32, 33, 34, 35) stellt die Entwicklung des Modells jedoch ins Zentrum der Forschungsanstrengungen, wobei eine Dokumentation des Forschungsprozesses erfolgt und teilweise auch empirische Methoden eingesetzt werden (siehe Tab. 41: 24, 26, 32). Mit der Ausnahme der Arbeit von Vicente und da Silva (2011a; 2011b) und Puspasari et al. (2011) betrachten diese Modelle jedoch lediglich Teilbereiche von GRC. Es ist herauszustellen, dass durchaus auch Integrationsaspekte bspw. hinsichtlich Risiko- und Compliance-Management (Milicevic und Goeken 2010; Martens und Teuteberg 2011; Sackmann et al. 2013; Schultz et al. 2012) betrachtet werden.

Insgesamt lässt sich festhalten, dass bislang keine Arbeit existiert, welche die für ein strategisches GRC-Management relevanten Informationen erfasst und ihre Beziehungen darstellt. Die Modelle von Vicente und da Silva (2011a; 2011b) und Puspasari et al. (2011) stellen zwar einen ersten Versuch hierzu dar, weisen jedoch die genannten Schwächen auf. Insbesondere erfolgt lediglich eine Fokussierung auf den Integrationsaspekt, wobei weitere für einen GRC-Ansatz wichtige Aspekte, wie die strategische Ausrichtung, nicht berücksichtigt werden. Gleichzeitig kann jedoch festgehalten werden, dass die vorgestellten Arbeiten nützliche Wissensquellen zur Entwicklung eines eigenen Mo-

dells für ein strategisches GRC-Management sind. Die identifizierten Modelle decken ein breites Themenspektrum, unterschiedliche GRC-Teilbereiche und sowohl IT-spezifische als auch unternehmensweite Aspekte ab. Auch aufgrund der Vielzahl von Modellen kann davon ausgegangen werden, dass hiermit bzgl. der Informationsobjekte von GRC eine umfassende Wissensquelle zur Verfügung steht.

5.3.1.2 Auswertung der relevanten Informationsobjekte

Eine Zuordnung der Elemente aus den verschiedenen Informations- und Referenzmodellen wurde durch mehrere Arbeitsschritte erreicht (siehe Tab. 42 bis Tab. 45 sowie Tab. 82 für weitere zugeordnete Begriffe). Zuerst wurden gleiche Elemente einander zugeordnet. Anschließend erfolgte eine Zuordnung von Modellelementen, die zwar unterschiedliche Begriffe verwenden, jedoch auf der Grundlage der Definitionen eine gleiche Bedeutung haben. Dies beinhaltete auch deutsch- und englischsprachige Begriffe bzw. Wortvariationen. Danach wurde den unterschiedlichen Abstraktionsgraden der Quellmodelle Rechnung getragen. Modellelemente, die eine Teilmenge eines anderen darstellen und für die konzeptionelle Modellierung des strategischen GRC-Managements nicht zwingend notwendig sind, wurden übergeordneten Begriffen zugeordnet (bspw. Business Goal und IT Goal zu Goal). Fehlende Oberbegriffe für zusammengehörende Modellelemente wurden entwickelt. In diesem Schritt musste auch entschieden werden, welches Abstraktionsniveau und welchen Detaillierungsgrad das Modell haben sollte. Konkret reflektiert dies die Entscheidung, ob ein Modellelement ein eigenes Informationsobjekt (Klasse in der Sprache der UML) oder lediglich ein Attribut darstellt. Abschließend wurde eine sprachliche Vereinheitlichung vorgenommen. Tab. 42 bis Tab. 45 zeigen die Zuordnung der Informationsobjekte nach sprachlicher Vereinheitlichung zu den synonymen sowie untergeordneten Begriffen aus

den Quellmodellen. Des Weiteren sind sonstige zugeordnete Begriffe in Tab. 82 aufgeführt. Diese Begriffe stehen in den Quellmodellen in einem logischen Zusammenhang mit den im Rahmen der Auswertung gefundenen Informationsobjekten und stellen eine mögliche Detaillierung der Informationsobjekte im Sinne von Attributen dar. Eine Zuordnung zu den Quellmodellen erfolgt durch die Modellnummern gemäß Tab. 40 und Tab. 41. Ebenso ist die Anzahl der Modelle, die zugeordnete Elemente zu einem Informationsobjekt aufweisen, dargestellt. Zu beachten ist, dass die Zuordnung der Begriffe maßgeblich vom Verständnis des Begriffs in der Publikation, die das Quellmodell enthält, abhängig ist. Bei einer Zuordnung von Begriffen wurde daher nach Möglichkeit auch die zugrundliegende Definition abgeglichen. Aufgrund unterschiedlicher Begriffsverständnisse, die teilweise auch aus einem unterschiedlichen Gegenstandsbereich der Quellmodelle resultieren, ist es daher möglich, dass identische Begriffe unterschiedlich zugeordnet werden.

Es ist weiterhin zu beachten, dass die analysierten Modelle unterschiedliche Gegenstandsbereiche besitzen und somit auch eine gewisse Diversität aufweisen. Dies führt bei der Auswertung der Entitäten der Quellmodelle dazu, dass es wahrscheinlich ist, dass die gefundenen Begriffe einen großen Teil der für GRC relevanten Begriffe umfassen. Es ist natürlich nicht auszuschließen, dass weitere für GRC relevante Entitäten existieren. Des Weiteren ist anzunehmen, dass oft vorzufindende Entitäten auch von besonderer Bedeutung für GRC sind. Da die Gegenstandbereiche der Modelle jedoch nicht gleichverteilt sind, kann dies jedoch lediglich als Indiz verstanden werden und ist kein exaktes Maß.

Tab. 42: Geordnete Übersicht zu den Modellelementen (1 von 4)

IO	Synonyme Begriffe	Untergeordnete Begriffe	Anz.
Kontrolle	Control Practices (1), Internal Control (2), rule (4), Internal Controls (5), Procedures (5), business rule (11), control (12), Regel (18), Control (19), Business Rule (20), Control (22), Controls/Standards (24), Kontrolle (25), Controls (26), Measure (27), Control (27), Measure (28), Control (29), Control (30), Procedures (31), Internal Controls (31), Maßnahme (33), Control Practice (34), Implementation Mechanism (35)	RiskTreatmentMesure (3), operational business rule (11), declarative business rule (11), CompanyLevelControl (12), ITControl (12), ApplicationControl (12), Control Procedures (24), Remediation Plan (24), Solution Library (24), Desaster Solving Procedures (24), Kontrollprozess (25), Compliance Rule (29), Control Rule (30), Separation of Duty Rule (32), Business Continuity Action (32), Risk Control Action (32), Risk Control (32)	27
Rolle	Responsibility and Accountability Chart (1), PersonProfile (3), OrganisationalUnit (3), FunctionalEntity (3), Actor (4), Role (4), Role (6),Business Function (6), Role (8), Role (9), Role (10), Agent (11), Agent (13), authority (13), Organisationsmodell (Organisationseinheit, Mitarbeiter, Rolle, Ressource, Zugriffsrechte) (16), Verantwortlich (18), Role (19), Corporate / Business Owner (24), Organization (26), Organizational Role (27) OrganisationalRole (28), Accountability / Roles (31), Organizational Unit (32), Organisationseinheit (33), Role (34)	Communication Partner (32), Activity Operator (32)	20
Geschäftsprozess	BusinessProcess (1), Process (2), Business Process (5), ProcessModel (6), BusinessProcess (12), BusinessProcess (13), Business Process (BP) (15), Geschäftsprozess (18), Business Process (20), Process (26), BusinessProcess (28), Business Process (29), Process (30), Processes (31), Process (32), Process (34)	IT Processes (1), Key Activities (1), Task (2), EnterpriseActivity (3), ProcessStructure (3), Activity (4), ProcessFragment (6), ProcessConstruct (6), Activity (6), operation (11), Activity (13), Business Process Element (29), Process element (30), Process Bundle (32), Subprocess (32), Subprocess Variant (32), Variant (32), Process Building Block Chain (32), Process Buildung Block Type (32), Process Building Block (32), Process Model Element (32), Activity (34)	19

Tab. 43: Geordnete Übersicht zu den Modellelementen (2 von 4)

IO	Synonyme Begriffe	Untergeordnete Begriffe	Anz.
Risiko	Risk (2), Risik (3), Risk (4), Risk (11), Risk (12), Risk (22), Risk (26), Risk (27), Risk (28), Risk (30), Risks (31), Risk (32), Risiko (33), Concern (Risk) (35)	Event (3), Vulnerabilities (VN) (15), Threats (TH) (15), Threat (19), Vulnerability (22), Impact (22), Threat (22), Desaster Event (24), Chance (27), Chance (28), (Compliance) Risk (29), Risk Type Hierarchy (32), Risk Type (32), Risk Affiliated Element (32), Restrisiko (33)	19
Kontrollziel	Control Objectives (1), Control Objective (2), Requirement (4), RuleGoal (7), ControlObjective (12), Measures & Directives (16), Control objectives (17), Anforderung/Vereinbarung (18), Control Objective (19), Requirement (19), Directive (20), Control Strategy (24), Kontrollanforderungen (25), Compliance Requirement (29), Compliance Target (29), Compliance requirement / objective (30), Control Objective (34), Business Rule (35), Requirement (35)	ApplicationControlStrategy (13), ApplicationControlStrategy (14), BC/DR Planning (24)	17
GRC-Vorgabe	Source (Law, Standard, Best Practice) (4), Regulation (5), Regulation (6), authority (11), Laws and regulations (17), Gesetzlich (18), Regulation (20), Compliance Regulation (23), Authorative Sources (24), Standards & Regulations (26), Compliance Source (29), Directive (compliance source) (30), Regulations and Standards (31)	Compliance Concern (29)	13
Ressource	asset (3), Resource (3), EnterpriseObject (3), Business subject (Sub-subject) (4), Resource (6), Subject (6), asset (19), asset (22), IT Asset Register (24), Reference Object (27) ReferenceObject (28), Business Object (32), Resource (32), Resource Type (32)	Produktgruppe (18), Data (26), IT-Resource (34)	12
Ziel	objective (3), Goal (6), Goal (11), Goal (20), objective (20), Desired Result (20), Goal (28), Ziel (33), Goal (34), Goal (35)	Business Goals (1), IT Goals (1), Business Objective (26), Organizational Goal (27), Key Objectives (31), IT Goal (34), Process Goal (34), Activity Goal (34), Soft Goal (35), Hard Goal (35)	12

Tab. 44: Geordnete Übersicht zu den Modellelementen (3 von 4)

IO	Synonyme Begriffe	Untergeordnete Begriffe	Anz.
Assessment	Audit (17), Assessment (20), Audit (24)	Control Outcome Tests (1), Control Design Tests (1), RiskAssessment (12), Inspection Method (24), IT Asset Analysis (24), Risk Review (24), Audit Objective (26), Audit Results (26), BP Compliance Assessment (29), Business Continuity Testing Action (32), Business Continuity Test (32), Risk Control Testing Action (32), Risk Control Test (32)	9
Kennzahl	Performance Indicators (1), PerformanceIndicator (3), Kennzahl (Skalenausprägung, Zielwert, Maßeinheit, Merkmal, Merkmal quantitativ, Merkmal qualitativ, Sachverhalt, Methode) (16), KPI (23), Metrics/Indicators (24), KPI (31), Indikator (33), Metric (34)	RiskIndicator (3), Cost (28), KRI (31)	9
Richtlinie	Policy (4), Policy (6), Policy (11), Policies (17), Richtlinie / Arbeitsanweisung (18), Business Policy (20), Policies (31)	Meta-Policy (6), IT Policies (24), Code of Conduct (31)	9
Dokumentation	BusinessProtocol (8), BusinessDocument (13), Dokumentenmodell (Report, Zielgruppe, Layout, Struktur, Symbole) (16), Log/Documentation (24), Evidences (31)	Logs/Incident Event (24), Risk Reports (31), Inquiries / Surveys (31)	7
IT-Komponente	IT Applications /IT Infrastructure (AP) (15), IT-Architekturmodell (IT-Architekturobjekt, Modul, Datenobjekt, Zugriffsart) (16), Datenbankmodell (Datenbank, Tabellen, Spalten, Datentypen, Beziehungen, Kardinalitäten) (16), IT-System (17), Application (21), IS (26), InformationSystem (28)	Packaged Service (21), Cloud Computing Service (23), Software (28)	7

Tab. 45: Geordnete Übersicht zu den Modellelementen (4 von 4)[95]

IO	Synonyme Begriffe	Untergeordnete Begriffe	Anz.
Anwendungsbereich	Domain (3), Jurisdiction (6), Scope (6), Scope (7), Scope (Global, Before, After, Between, AfterUntil) (14), Domain (34)	Control Domain (21)	6
Ausführung	Performance (9), Performance (10), Business Process Instance (29), Process instance (30)	BP Element Instance (29), Process element instance (30), Process Building Block Variant Instance (32)	5
Implementierungslogik	monitor (4), RuleLogic (7), Monitors (17)	---	3
Rahmenwerk	Rahmenwerk (18), Compliance Frameworks (21), Controls/Standards (24)	---	3
Strategie	Strategy (6), Strategiemodell (Strategie, Ziele, Maßnahmen) (16), Strategy (31)	---	3
Stakeholder	Stakeholder (3), Stakeholder (18), Stakeholder (35)	Indirekte Stakeholder (18)	3
Reifegrad	Maturity Models (1), Reifegradmodell (Reifegrade, Anforderungen, Kriterien, Implementierungsdauer, Reifegradbewertung, Methoden, Erhebungsmethoden, Analysemethoden) (16), Maturity Model (34)	Maturity Level (34)	3
Verletzung	Violation (4)	Security Breach (19)	2

5.3.1.3 Auswertung der Beziehungen zwischen den Informationsobjekten

Zur Analyse der Beziehungen zwischen den Informationsobjekten sind die Quellmodelle nur eingeschränkt geeignet, da die Modelle überwie-

[95] Es sei darauf hingewiesen, dass die Tabellen lediglich die Ergebnisse der Auswertung der Quellmodelle darstellen. Die Ergebnisse der Evaluierung sind noch nicht berücksichtigt. Daher sind die in den Tabellen enthaltenen Informationsobjekte nicht identisch mit dem in Abb. 9 dargestellten Modell.

gend nicht explizit eine Integration von GRC auf strategischer Ebene betrachten. Grundsätzlich mögliche Beziehungen konnten jedoch identifiziert werden. Hierzu wurden auf Basis der Konsolidierung der Modellelemente Beziehungen in den Modellen identifiziert. Folgende Einschränkungen sind zu beachten. Der Fokus und die Abstraktionsebene des jeweiligen Modells haben wesentlichen Einfluss auf die dort enthaltenen Beziehungen. So steht das Informationsobjekt Rolle, welches die Verantwortlichkeit ausdrückt, in den ausgewerteten Modellen fast zu jedem anderen Informationsobjekt in Beziehung. Hier ist jedoch insbesondere die Verantwortlichkeit der Kontrollen und Geschäftsprozesse relevant. Ist keine Unterscheidung zwischen einzelnen Informationsobjekten in einem Quellmodell gegeben, wurden mehrere Beziehungen aufgenommen. So wird Kontrollziel und Kontrolle jeweils zu Geschäftsprozess in Beziehung gesetzt, da zwischen Kontrollziel und Kontrolle nicht immer unterschieden wird. Teilweise haben die Quellmodelle einen unterschiedlichen Fokus (unternehmensweite vs. IT-bezogene Modelle), wodurch logische Beziehungen mehrfach aufgenommen wurden. Bspw. werden Kennzahlen entweder IT-Komponenten oder Geschäftsprozessen zugeordnet. Zur Ableitung der Beziehungen wurden daher weitere Regeln eingeführt. Es wurden Beziehungen auch mittelbar, d.h. über andere Informationsobjekte hinweg, dargestellt. Außerdem wurde nicht versucht, jede mögliche Beziehung darzustellen, sondern besonders verbreitete, die zu einem konsistenten Modell führten, wurden identifiziert und übernommen. Hierzu hat insbesondere die im folgenden Abschnitt dargestellte Analyse mit Hilfe strategischer GRC-Anforderungen beigetragen.

Bei der Herleitung der Beziehungen für das datenseitige Modell wurde auf mehrere Quellen zurückgegriffen. Erstens wurden auf Basis der Konsolidierung der Modellelemente in den Modellen mögliche Bezie-

hungen identifiziert. Diese grundlegenden Beziehungen wurden in einem zweiten Schritt mit Hilfe der strategischen GRC-Anforderungen verfeinert. Ebenfalls liefert die durchgeführte Evaluierung relevante Informationen bzgl. der Beziehungen der Modellentitäten des datenseitigen Modells. Die folgende Tab. 46 liefert eine Übersicht zur Herleitung der Modellbeziehungen. Hierbei werden Quellmodelle zugeordnet, die eine gleiche Beziehung aufweisen (mit Referenz zu den Modellnummern aus Tab. 40 und Tab. 41). Außerdem wird die Herleitung aus den Anforderungen für ein strategisches GRC-Management referenziert (Referenz gemäß Tab. 47). Letztlich werden weitere Begründungen angeführt bzw. auf eine Unterstützung der Beziehung durch die Evaluierung verwiesen. Im Rahmen der Darstellung des datenseitigen Modells wird die Analyse in der Weise aufgegriffen, dass die identifizierten Beziehungen in den Quellmodellen an den entsprechenden Stellen zur Begründung der Beziehungen im entwickelten Modell referenziert sind.

Tab. 46: Begründung der Beziehungen zwischen den Entitäten des Modells

Von	Zu	Zugeordnete Modelle	Herleitung aus strat. GRC-Anforderungen	Weitere Begründung
Strategie	Entscheidung	-	-	Evaluierung
Strategie	Ziel	6, 16	-	-
Stakeholder	Strategie	-	B3	-
Stakeholder	GRC-Vorgabe	18	-	-
Stakeholder	Ziel	-	B3	-
Ziel	Kontrollziel	1, 35	B1	-
GRC-Vorgabe	Kontrollziel	4, 5, 17, 18, 29, 30	B5	-
Kontrollziel	Risiko	2, 4, 12, 24, 29, 30	B5	-
Kontrollziel	Richtlinie	4, 5, 17, 18, 20	-	-
Rahmenwerk	Richtlinie	4, 18, 24	-	-
Rahmenwerk	GRC-Vorgabe	18, 24	-	-

Von	Zu	Zugeordnete Modelle	Herleitung aus strat. GRC-Anforde-rungen	Weitere Begründung
Richtlinie	Kontrolle	4, 5, 6, 11, 18, 20, 31	-	-
Richtlinie	Anwendungs-bereich	6	-	-
Risiko	IT-Komponente	15, 23, 26, 28	B13	-
Risiko	Ziel	11, 26, 27, 28, 33, 35	-	Evaluierung
Risiko	Geschäftspro-zess	3, 12, 15, 19, 26, 28, 31	-	-
Kennzahl	Ziel	1, 3, 16, 31, 34	B2	-
Kennzahl	Entscheidung	-	-	Evaluierung
Kennzahl	Geschäftspro-zess	1	B2, B6, B10	-
Assessment	Reifegrad	-	-	Reifegrad wird als eine Form des Assess-ments ver-standen, jedoch auf-grund der Bedeutung als eigenständiges Informations-objekt model-liert.
Assessment	Risiko	12, 26	-	-
Assessment	Geschäftspro-zess	1, 12, 26, 32	B6, B10	-
Assessment	Schwachstelle	-	-	Evaluierung
Assessment	Entscheidung	-	-	Evaluierung
IT-Komponente	Geschäftspro-zess	15, 26	-	-
Verletzung	Kontrolle	4, 19	-	-
Kontrolle	Kontrolle	6, 11, 19, 28	-	-
Kontrolle	IT-Komponente	26	B11, B12	-
Kontrolle	Rolle	11, 26, 28, 33	B14	-
Dokumenta-tion	Geschäftspro-zess	13	-	-
Rolle	Geschäftspro-zess	1, 4, 6, 11, 13, 18, 26, 32, 34	B9	-
Geschäfts-prozess	Ziel	3, 20, 26, 31, 34	B2	-

Von	Zu	Zugeordnete Modelle	Herleitung aus strat. GRC-Anforde-rungen	Weitere Begründung
Geschäfts-prozess	Schwachstelle	-	-	Evaluierung
Geschäfts-prozess	Ressource	3, 6, 18, 28, 32, 34	-	-
Geschäfts-prozess	Kontrolle	2, 3, 5, 6, 11, 12, 13, 18, 26, 29, 30, 32	B7, B8	Evaluierung

5.3.2 Abgleich der Modellobjekte mit den Anforderungen an das strategische GRC-Management

5.3.2.1 Vorüberlegungen

In diesem Abschnitt werden die Anforderungskategorien und Anforderungen, die das vorhandene Wissen im Kontext des strategischen GRC-Managements strukturieren, angewendet um die Konstruktion des datenseitigen Modells zu unterstützen. Diese Vorgehensweise liegt darin begründet, dass die existierenden konzeptionellen Modelle im Kontext von GRC, nicht auf die Unterstützung eines strategischen GRC-Managements abzielen. Die Anforderungen werden also verwendet, um die bisherigen Überlegungen auf die Unterstützung eines strategischen GRC-Managements auszurichten. Nachfolgend werden daher die für das Modell relevanten Aspekte der Anforderungskategorien diskutiert. Tab. 47 fasst die Ergebnisse hinsichtlich der Informationsobjekte und Beziehungen zusammen.

Tab. 47: Herleitung von Informationsobjekten und Beziehungen aus den strategischen GRC-Anforderungen

Anforderungs-kategorie	Relevante Informationsob-jekte	Abgeleitete Beziehungen
Strategische Ausrichtung	Strategie, Ziel, Richtlinie, Kontrolle, Kennzahl, Stakeholder	(B1) Kontrollziele sind abgestimmt mit den Zielen.
		(B2) Geschäftsprozesse unterstützen Ziele, welche durch Kennzahlen gemessen werden.
		(B3) Strategie und Ziele werden ausgerichtet an den Stakeholdern.
		(B4) Stakeholderinteressen spiegeln sich in GRC-Vorgaben wider.
Integration	Kontrollziel, Risiko, GRC-Vorgabe, Kennzahl, Assessment, Geschäftsprozess, Kontrolle	(B5) Kontrollziele ergeben sich aus Risiken und GRC-Vorgaben.
		(B6) Kennzahlen und Assessments messen Conformance und Performance der Geschäftsprozesse.
		(B7) Kontrollen werden in den operativen Geschäftsprozessen umgesetzt (operative Integration).
Geschäftsprozess-orientierung	Kontrolle, Geschäftsprozess, Implementierungslogik, Rolle	(B8) Kontrollen werden in Geschäftsprozessen implementiert und mit Hilfe der Implementierungslogik mit dem Geschäftsprozess automatisiert.
		(B9) Über Geschäftsprozesse wird die verantwortliche Rolle (Ownership) determiniert.
Management-Systeme	Assessment, Kennzahl, Geschäftsprozess	(B10) Geschäftsprozesse werden durch Assessments und Kennzahlen im Hinblick auf GRC gesteuert.
Automatisierung	Kontrolle, Geschäftsprozess, IT-Komponente, Implementierungslogik	(B11) IT-Komponenten sind direkt durch Kontrollen betroffen.
		(B12) Kontrollen werden mit Hilfe der Implementierungslogik in IT-Komponenten automatisiert.
Flexibilisierung	Alle insb. Geschäftsprozess, IT-Komponente, GRC-Vorgabe, Risiko	(B13) Eine direkte Beziehung zwischen IT-Komponenten und Risiken ist notwendig, um eine Überwachung der Risiken bei IT-bezogenen Anpassungen zu ermöglichen.
Menschliche Faktoren	Kontrolle, Geschäftsprozess, Rolle	(B14) Kontrollen haben eine direkte Beziehung zum Informationsobjekte Rolle.

5.3.2.2 Strategische Ausrichtung

Die Anforderungskategorie strategische Ausrichtung betont die strategische Bedeutung von GRC, wobei GRC als strategische Chance und nicht lediglich als Kostentreiber und Hindernis für das Geschäft betrachtet wird. Hierbei wird die Ausrichtung von GRC an der Geschäftsstrategie, die Berücksichtigung möglicher Zielkonflikte zwischen Normerfüllung und strategischer Zielerreichung, die Verfolgung von Nutzenpotentialen und die Ausrichtung an den Stakeholdern gefordert. Somit werden Informationsobjekte wie Strategie und Ziel angesprochen. GRC, d.h. konkret die Kontrollziele, sollten demnach an den geschäftlichen Zielen ausgerichtet werden, wodurch auch der Zielkonflikt zwischen GRC und strategische Zielerreichung berücksichtigt wird.

Hervorzuheben für die strategische Ausrichtung ist außerdem die Governance, die das strategische Management bei der Strategie- und Zieldefinition unterstützten sollte. Hierbei ist die integrierte Steuerung von „Performance" und „Conformance" (ISO 2008) in den Mittelpunkt zu rücken. Für diese Aufgabe haben Kennzahlen eine besondere Bedeutung. Diese sollten die Zielerreichung der Geschäftsprozesse hinsichtlich der Conformance und Performance messen. Durch verbesserte Kontrollen können Performance-Verbesserungen der Geschäftsprozesse erzielt und die Erreichung von Geschäftszielen durch GRC unterstützt werden, was der Forderung der Verfolgung von Nutzenpotentialen entspricht. Berücksichtigt werden diese Punkte als Beziehung zwischen Kennzahlen und Zielen.

Die Stakeholder-Orientierung fordert eine Ausrichtung der Strategie und Ziele und somit mittelbar auch der Kontrollziele an den Stakeholderinteressen. Letztlich beeinflussen die Stakeholderinteressen die GRC-Vorgaben, da Stakeholderinteressen auf normativer Ebene regula-

tive Vorgaben bspw. hinsichtlich von Kontroll- und Offenlegungspflichten im Rahmen der Rechnungslegung abbilden.

5.3.2.3 Integration

Die Integration von GRC wird in der Literatur unter inhaltlichen, methodischen bzw. informationstechnischen Aspekten diskutiert. Inhaltliche Aspekte sind die integrierte Erfüllung mehrerer GRC-Vorgaben und die Integration der GRC-Disziplinen. Außerdem wird eine Integration der Kontrollen in die operativen Geschäftsprozesse sowie eine Integration von IT-bezogenen und unternehmensweiten Ansätzen gefordert. Für das mit dem datenseitigen Modell verfolgte Forschungsziel ist die Integration der GRC-Disziplinen als Teil der inhaltlichen Integration und die Integration der Kontrollen in die operativen Geschäftsprozesse besonders relevant. Die Beziehungen von GRC, welche für die Integration der GRC-Disziplinen von entscheidender Bedeutung sind, wurden bereits ausführlich dargestellt und sollen daher hier lediglich hinsichtlich der für das Modell relevanten Bereiche wieder aufgegriffen werden.

Wie bereits ausgeführt können sich Kontrollziele bzw. Kontrollen zum einen aus GRC-Vorgaben und zum anderen aus Risiken ergeben. Kontrollziele für risikosteuernde Maßnahmen, die aus Risikoanalysen gewonnen werden, sollen hierbei die Erreichung der Ziele sicherstellen. Ein weiterer wichtiger Aspekt der Integration ist die integrierte Betrachtung von Performance und Conformance (ISO 2008). Da Kontrollen wiederum gemäß der operativen Integration in den Geschäftsprozessen umgesetzt werden, beziehen sich Kennzahlen und Assessments auf Geschäftsprozesse.

5.3.2.4 Geschäftsprozessorientierung

Ein geschäftsprozessorientierter Ansatz wird in der Literatur aufgrund der Bedeutung der Geschäftsprozesse für das GRC-Management gefordert. Außerdem wird die Bedeutung eines geschäftsprozessorientierten Ansatzes für die Automatisierung der Compliance-Sicherung betont und eine Integration von GRC- und GPM vorgeschlagen. Die Integration von GRC und Enterprise Architecture Management erweitert diesen Aspekt zusätzlich um weitere relevante Informationen des Unternehmens.

Geschäftsprozesse stehen in einem direkten Zusammenhang mit Risiken (Sackmann 2008b, S. 1137) und sollten im Sinne einer operativen Integration (siehe Anforderungskategorie Integration) die Kontrollen beinhalten. Da Geschäftsprozesse Ausgangspunkt der Automatisierung sind, gibt es eine Beziehung zur Implementierungslogik. Folgt man dem Grundgedanken eines geschäftsprozessorientierten Ansatzes und der Überlegung, dass auch Kontrollen direkter Bestandteil der Geschäftsprozesse sind, dann kann das Informationsobjekt Geschäftsprozess als ein zentrales Element des GRC-Managements aufgefasst werden. Die Verantwortlichkeit (Informationsobjekte Rolle) an Geschäftsprozessen kann somit die Verantwortlichkeit für eine Reihe weiterer Informationsobjekte determinieren.

5.3.2.5 Management-Systeme

Relevante Management-Systeme, die mit GRC abzustimmen sind, sind solche, die unter GRC zu subsumieren sind (bspw. Interne Revision, Datenschutz, Qualitätsmanagement) und sonstige, die im Kontext von GRC relevant sind (bspw. Controlling, IT-Management) (Bhimani 2009; Klotz 2009, S. 13-16). Management-Systeme, die unter GRC zu subsumieren sind, beschäftigen sich im Wesentlichen mit der Prüfung der ihr anvertrauten Verantwortungsbereiche. Besonders betont wird

dies in der Aufgabenstellung der Internen Revision, die unabhängige Prüfungs- und Beratungsleistungen erbringt (Deutsches Institut für Interne Revision 2011, S. 5). Mit einer ähnlichen Aufgabenstellung ist auch das Controlling konfrontiert, das eine Managementunterstützung durch Planung, Kontrolle und entsprechende Informationsversorgung erbringt und Kennzahlensysteme eingesetzt (Horvath 2011). Neben dem GPM verfolgen auch das IT-Management, bei der geschäftsprozessorientierten Einführung von Informationssystemen und das Qualitätsmanagement sowie die Interne Revision geschäftsprozessbasierte Ansätze. Somit sind neben Assessments und Kennzahlen auch Geschäftsprozesse als Gegenstand von Interesse. Geschäftsprozesse werden hierbei durch Assessments und Kennzahlen gesteuert.

5.3.2.6 Automatisierung

Die IT ist Gegenstand und Unterstützer von GRC (Klotz und Dorn 2008, S. 9-10; Teubner und Feller 2008, S. 401). Aus Sicht der IT als Unterstützer von GRC ist die Automatisierung der Compliance-Sicherung und Risikosteuerung relevant. Hinsichtlich der Bedeutung der IT als Gegenstand von GRC sind zwei Formen zu unterscheiden. Einerseits ist die IT direkt Gegenstand von Compliance-Vorgaben und Risiken. Beispiele hierfür sind Anforderungen zur Informationssicherheit und technische Risiken. Andererseits ist die IT mittelbar durch ihre Rolle als Unterstützer von Geschäftsprozessen Gegenstand von GRC. Bspw. müssen Kontrollen zur Sicherstellung der Richtigkeit der Finanzberichterstattung, unter anderem festgeschrieben durch den SOX, in IT-Systemen umgesetzt werden. Relevante Informationsobjekte sind daher Kontrollen, Geschäftsprozesse sowie IT-Komponenten als auch die Implementierungslogik. Kontrollen werden als Teil der Geschäftsprozesse durch eine Implementierungslogik, wie einen Monitor, in IT-Komponenten automatisiert. Es können jedoch nicht alle Kontrollen

automatisiert werden, sondern sind teilweise manuell auszuführen (Sackmann 2008a), was dann die Aufgabe der an den Geschäftsprozessen beteiligten Rollen ist.

5.3.2.7 Flexibilität

In der Literatur wird die Flexibilisierung hinsichtlich der Geschäftsprozesse und IT-Systeme als Herausforderung für GRC dargestellt. Als weitere relevante Aspekte, die eine Flexibilisierung in Aussicht stellen und relevant für GRC sind, werden in der Literatur SOA und Cloud-Computing angeführt.

Veränderungen können sowohl an den Kontrollen als auch den Geschäftsprozessen oder IT-Komponenten ausgelöst werden und vielfältige Auswirkungen haben. Menzies (2006, S. 359) identifiziert in diesem Zusammenhang Treiber des GRC-Managements wie neue Geschäftsprozesse, neue Produkte oder Märkte, M&A-Aktivitäten, neue IT-Systeme, neue Geschäftspartner und neue bzw. veränderte regulatorische Vorgaben. Flexibilisierung kann Auswirkungen auf nahezu alle Informationsobjekte des Modells haben, insbesondere auf Strategien und Ziele, Geschäftsprozesse und andere Ressourcen (bspw. modelliert als Teil der Enterprise Architecture), Risiken sowie Kontrollen. Von Sackmann (2008b) werden im Kontext der Flexibilisierung die Beziehungen zwischen Risiken und IT-Komponenten sowie direkt von den Risiken zu den Geschäftsprozessen betont. Die direkte Beziehung zwischen IT-Komponenten und Risiken ist notwendig, da Änderungen in den IT-Komponenten, bspw. im Rahmen von SOA, unmittelbar Auswirkungen auf die Risikosituation haben, diese jedoch nicht notwendigerweise auch den Ablauf des Geschäftsprozesses tangieren.

5.3.2.8 Menschliche Faktoren

Die Berücksichtigung von Faktoren des menschlichen Verhaltens wird in der Literatur hinsichtlich des Mitarbeiter-Verhaltens, der GRC-bezogenen Kultur sowie einer effizienten Unternehmenskommunikation im Sinne eines „tone at the top" gefordert. Der verantwortliche Mitarbeiter, welcher in seiner Rolle Geschäftsprozesse und die hierin enthaltenen Kontrollen ausführt, ist somit von besonderer Bedeutung. Es sollten daher auch Kontrollen wie Schulungen oder Awareness-Kampagnen durchgeführt werden, welche die Mitarbeiter in ihrer Rolle zu GRC-konformen Verhalten befähigen und ermutigen. Solche Maßnahmen können auch als Kontrollen aufgefasst werden, um die die operativen Geschäftsprozesse als auch Management-Prozesse zu ergänzen sind. Kontrollen haben somit eine direkte Beziehung zum Informationsobjekte Rolle.

5.3.3 Darstellung des Modells

Das in diesem Abschnitt dargestellte Modell basiert auf den Analysen aus den vorgegangenen Abschnitten. Die Darstellung nimmt außerdem bereits die Ergebnisse der Evaluierung vorweg.

Abb. 9 zeigt somit das datenseitige Modell für ein strategisches GRC-Management nach der Evaluierung. Informationsobjekte, die im Rahmen der Evaluierung nicht bestätigt wurden, sind am oberen linken Rand dargestellt. Informationsobjekte, die durch die Evaluierung hinzugefügt wurden, sind mit nicht durchgezogenem Rand dargestellt (Schwachstelle und Entscheidung). Die Beziehungen zwischen den Informationsobjekten werden aus den vorhandenen Modellen sowie den strategischen GRC-Anforderungen hergeleitet. Die Beziehungen können aus Tab. 46 entnommen werden. Zur Nachvollziehbarkeit wird die Begründung an den relevanten Stellen wiederholt. Hierzu werden

die Nummern der Modelle, welche die Beziehung unterstützen, referenziert (Modelle 1 bis 35 gemäß Tab. 40 und Tab. 41). Für die Herleitung der Beziehungen aus den strategischen GRC-Anforderungen werden die Bezeichnungen (B1 bis B14) gemäß Tab. 47 referenziert. Aufgrund der Komplexität des Modells wurde eine weitere Untergliederung in die strategische, konzeptionelle und operative Ebene vorgenommen, die lediglich die Lesbarkeit des Modells erhöhen soll und nicht Gegenstand der Herleitung bzw. Evaluierung ist. Diese Gliederung ist daher lediglich als Vorschlag zu verstehen und ist im Modell mit Hilfe von „swim lanes" dargestellt. Definitionen hinsichtlich der speziellen Bedeutung der Informationsobjekte im Rahmen des Modells sind in Tab. 83 dargestellt. Die dortigen Definitionen führen im Wesentlichen die Definitionen, die den Quellmodellen aus der GRC-Literatur zu Grunde liegen, zusammen. Daher wurde auf weitere Literaturverweise verzichtet. Das Modell wird nachfolgend von oben nach unten gelesen.

Auf strategischer Ebene sollte GRC an Ergebnissen des strategischen Managements ansetzen, diese für die Governance sowie zur strategischen Ausrichtung des Risiko- und Compliance-Managements nutzbar machen und andererseits durch relevante Informationen den Strategieprozess unterstützen. Ausgangspunkt sind die Stakeholder, deren Interessen gesamtwirtschaftlich Einfluss auf die GRC-Vorgaben (18) und unternehmensbezogen, wie in der Analyse der Anforderungskategorie „strategische Ausrichtung" gezeigt, Einfluss auf Strategie und Ziele (B3) haben. Strategien beinhalten Ziele (6, 16) und beeinflussen die Entscheidungsfindung (siehe Evaluierung).

Die konzeptionelle Ebene beinhaltet die Management-Aktivitäten von GRC. Hier sind die Kontrollziele aus den GRC-Vorgaben (4, 5, 17, 18, 29, 30, B5) und den Risiken (2, 4, 12, 24, 29, 30, B5) zu entwickeln. Die Anforderungskategorie „strategische Ausrichtung" legt außerdem nahe,

dass die Kontrollziele mit den Zielen der strategischen Ebene abzustimmen sind (1, 35, B1). Aus den Kontrollzielen werden die Richtlinien abgeleitet (4, 5, 17, 18, 20), die einen eingeschränkten Anwendungsbereich haben (6). Zur Herleitung unternehmensspezifischer Richtlinien können Rahmenwerke in Form von Standards und Best Practices herangezogen werden (4, 18, 24), welche die Erfüllung von GRC-Vorgaben unterstützen (18, 24). Geschäftsprozesse sind an den Unternehmenszielen auszurichten (3, 20, 26, 31, 34, B2). Der Fokus dieses Modells legt es nahe, Assessments hinsichtlich der Risiken (12, 26) sowie der „Conformance" und „Performance" (B6) auf der Ebene der Geschäftsprozesse durchzuführen (1, 12, 26, 32, B6, B10). Hierfür können auch Reifegradmodelle verwendet werden, die eine Spezialform des Assessments darstellen. Assessments unterstützen Entscheidungen auf strategischer Ebene (siehe Evaluierung). Geschäftsprozesse sind wiederum mit den Kontrollen (2, 3, 5, 6, 11, 12, 13, 18, 26, 29, 30, 32, B7, B8) und Risiken (3, 12, 15, 19, 26, 28, 31) verknüpft. Risiken können sich weiterhin auch unmittelbar aus den IT-Komponenten ergeben (15, 23, 26, 28, B13), ohne dass hierbei die Geschäftsprozesse betroffen sind. Risiken beziehen sich außerdem auf Ziele und gefährden die Zielerreichung (11, 26, 27, 28, 33, 35). Kennzahlen messen Geschäftsprozesse (1, B2, B6, B10) hinsichtlich der Erreichung der Ziele (1, 3, 16, 31, 34, B2) und unterstützen hierdurch, ebenso wie Assessments, Entscheidungen auf strategischer Ebene (siehe Evaluierung). Es ist darauf hinzuweisen, dass das Non-Compliance-Risiko als Teil der Beziehung zwischen Kontrollziel und Risiko verstanden wird. Dieses Verständnis ist in Übereinstimmung mit den bestehenden Modellen aus der GRC-Literatur (siehe Modelle 4, 29, 30). Daher wird keine Beziehung zwischen Risiko und GRC-Vorgabe in das Modell aufgenommen.

Auf operativer Ebene werden Kontrollen, die in den Richtlinien formuliert sind (4, 5, 6, 11, 18, 20, 31), im Sinne einer operativen Integration in den Geschäftsprozessen implementiert (2, 3, 5, 6, 11, 12, 13, 18, 26, 29, 30, 32, B7, B8). Zwischen den Kontrollen selbst können Abhängigkeiten bestehen (6, 11, 19, 28). Kontrollen können weiterhin durch Verletzungen gefährdet werden (4, 19) und neben Geschäftsprozessen auch direkt die IT-Komponenten betreffen (B11), welche die Geschäftsprozesse unterstützen (15, 26). IT-Komponenten dienen darüber hinaus zur Automatisierung der Kontrollen (B12). Geschäftsprozesse werden als Unternehmensressourcen betrachtet, wobei auch weitere Gegenstände wie Produkte, Projekte oder Informationen für GRC relevant sind (3, 6, 18, 28, 32, 34). IT-Komponenten und Kontrollen sind im Rahmen der Geschäftsprozesse zu dokumentieren (13). Das Modell definiert die Verantwortlichkeiten mittels der Rollen, die an den Geschäftsprozessen beteiligt sind (1, 4, 6, 11, 13, 18, 26, 32, 34, B9). Kontrollen können, wie die Analyse der verhaltensspezifischen Aspekte zeigt, auch direkt Mitarbeiter betreffen (11, 26, 28, 33, B14). Letztlich sind Schwachstellen relevant, die sich auf die Geschäftsprozesse beziehen und im Rahmen der Assessments auf konzeptioneller Ebene aufzudecken sind (siehe Evaluierung).

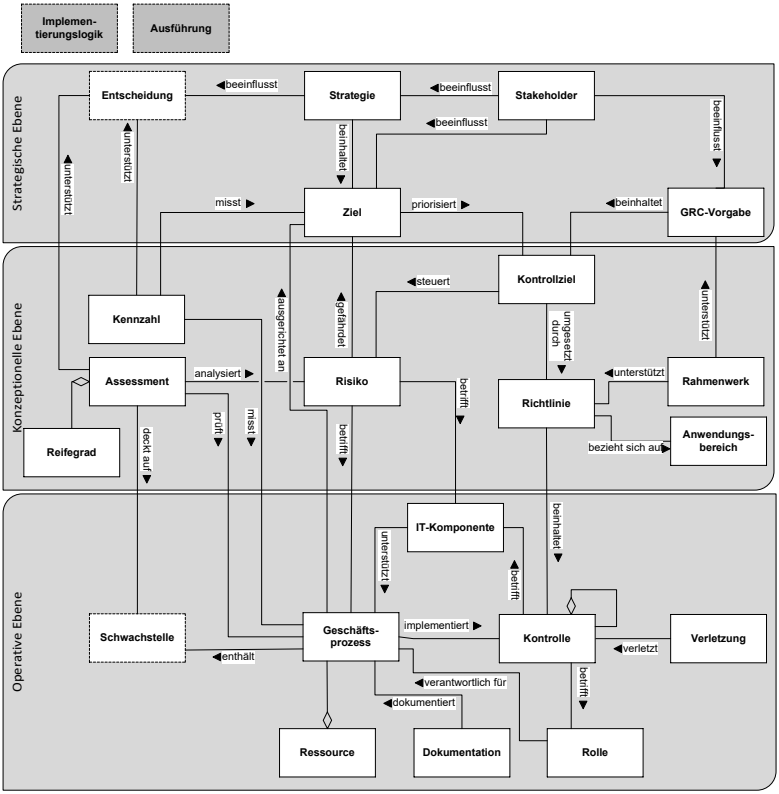

Abb. 9: Datenseitiges Modell für das strategische GRC-Management

5.3.4 Demonstration des Modells

Zur Veranschaulichung des datenseitigen Modells für das strategische GRC-Management soll nachfolgend ein fiktives Demonstrationsbeispiel dargestellt werden. Es wird ein Beispielprozess herausgegriffen und hierauf aufbauend die Informationsobjekte beispielhaft hergeleitet. Die Demonstration soll insbesondere das entwickelte Modell veranschaulichen und somit die Nachvollziehbarkeit erhöhen. Es ist selbst-

verständlich, dass im Rahmen eines solchen fiktiven Demonstrationsbeispiels nicht alle Einflussfaktoren einer realen Anwendung adäquat berücksichtigt werden können (siehe bspw. Riege et al. 2009, S. 79). Trotzdem erscheint das Demonstrationsbeispiel als Möglichkeit die intendierte Anwendung zu plausibilisieren. Es ist darauf hinzuweisen, dass das vorliegende Modell in seiner derzeitigen Form die relevanten Informationen und Zusammenhänge von GRC auf konzeptioneller Ebene aufzeigt, was dem verfolgten Forschungsziel entspricht. Zur Implementierung im Rahmen eines Informationssystems sind weitere Detaillierungen hinsichtlich der Attribute und der Kardinalitäten zwischen den Entitäten des Modells notwendig. Auch sind weitere Schritte erforderlich um einen umfassenden Ansatz für ein strategisches GRC-Management verfügbar zu machen. Die Anwendung des Modells in einer konkreten Unternehmenssituation würde jedoch einen solchen Ansatz erfordern, da zur Spezifizierung der einzelnen Informationsobjekte Methoden bspw. für die Verknüpfung der Unternehmensstrategie mit den GRC-Vorgaben, für die integrierte Erfüllung von GRC-Vorgaben und der damit verbundenen Nutzung von Synergieeffekten sowie der Verwirklichung von Nutzenpotentialen durch GRC erforderlich sind. Solche Methoden liegen derzeit, wie ausführlich dargestellt, noch nicht vor. Es ist zudem anzumerken, dass für die einzelnen Informationsobjekte lediglich Beispiele angegeben werden, die obwohl sie bspw. real existierende GRC-Vorgaben beinhalten, keinen Anspruch auf Vollständigkeit erheben.

Das Demonstrationsbeispiel stellt auf die IT-Abteilung eines Pharmaunternehmens ab. Hierbei wird konkret der IT-Change-Management-Prozess betrachtet. Es wird somit keine unternehmensweite Sichtweise gewählt, sondern es findet eine Beschränkung auf IT-Aspekte statt. Es ist zu beachten, dass das Modell sowohl für unternehmensweite als

auch IT-bezogene Szenarien anwendbar ist und eine unternehmensweite Perspektive analog eingenommen werden könnte. Die Pharmaindustrie stellt ebenso wie die Finanzdienstleistungsindustrie eine hochregulierte Branche dar. Es ist daher anzunehmen, dass sich diese besonders als Grundlage für ein Demonstrationsbeispiel im Kontext des strategischen GRC-Managements eignet. Relevanz und Eignung des Falls werden auch im Rahmen der Fallstudienmethode (Yin 2009) als Auswahlkriterien herangezogen (Mayring 1993, S. 28).

Unter pharmazeutischen Unternehmen werden solche Unternehmen verstanden, die Arzneimittel im Sinne des §2 Arzneimittelgesetz (AMG) herstellen. Bedeutende regulatorischen Vorgaben existieren in der Pharmaindustrie im Bereich der „Guten Herstellungspraxis" (engl. „Good Manufacturing Practice"), womit Vorgaben an das Qualitätsmanagement im Kontext der pharmazeutischen Produktion gemeint sind (European Commission Health and Consumers Directorate 2010). Ziel dieser Vorgaben ist im Kern die Herstellung qualitativ einwandfreier Produkte und somit die Patientensicherheit. Soweit die IT Geschäftsprozesse, die Einfluss auf die Qualität der Produkte haben, unterstützt, finden diese Vorgaben auch für die IT Anwendung. In diesem Zusammenhang wird von „Validierung" bzw. „Computersystemvalidierung" gesprochen, womit der dokumentierte Nachweis gemeint ist, dass die IT gemäß den definierten Anforderungen fehlerfrei funktioniert. Der „validierte Zustand" ist über den gesamten Lebenszyklus, also von der Entwicklung über den Betrieb bis zur Stilllegung des IT-Systems aufrecht zu erhalten (ISPE 2008; Nissen 2006). Als regulatorische Quellen für diese Vorgaben sind in Europa der GMP-Leitfaden der Europäischen Union (EU) und hier für IT-Systeme insbesondere der Annex 11 (European Commission Health and Consumers Directorate 2010) und in den USA der Code of Federal Regulations (CFR)

Title 21 insbesondere Part 11, 210, 211 und 820 (FDA 2013) zu nennen.

Das IT-Change-Management bezieht sich auf Änderungen an IT wie Software oder Hardware und wird als IT-Prozess in ITIL (siehe bspw. OGC 2007a; OGC 2007b) dargestellt. IT-Service-Management nach ITIL versucht die IT hinsichtlich Administration und Betrieb in einer Weise zu organisieren, dass die Dienste (engl. Services), die mit den internen oder externen Kunden vereinbart wurden, bestmöglich erbracht werden können. ITIL nennt verschiedene Auslöser von Änderungen. So können Änderungen aus Initiativen zur Verbesserung von Geschäftsprozessen resultieren oder zur Reduzierung von Kosten dienen. Ebenso können zur Behebung von Fehlern Änderungen notwendig sein. Ziel des IT-Change-Managements ist eine strukturierte Durchführung dieser Änderungen. Zum IT-Change-Management-Prozess gehören die Schritte Stellen des Änderungsantrags, Bewertung der Änderung, Freigabe bzw. Ablehnung der Änderung, Koordination der Umsetzung der Änderung, Überprüfung der Änderung und Abschluss der Änderung (OGC 2007b, S. 42).

Die Beispiele für die Informationsobjekte sind für die strategische, die konzeptionelle und die operative Ebene getrennt in Tab. 48, Tab. 49 und Tab. 50 dargestellt. Es ist darauf hinzuweisen, dass lediglich eine Beschreibung der Beispiele je Informationsobjekt angegeben wird, die zur Nachvollziehbarkeit ausreichend sind. Würde man das Datenmodell in einem Informationssystem abbilden wollen, wäre eine Spezifikation der Attribute je Informationsobjekt notwendig, die jedoch sehr individuell je Anwendungsfall wäre. Des Weiteren zeigt das Modell die Beziehungen zwischen den Informationsobjekten, die im Beispiel um die Beziehungen der jeweiligen Ausprägungen der Informationsobjekte zu

ergänzen ist. Diese Beziehungen werden innerhalb der folgenden Darstellung an einigen Beispielen aufgezeigt.

Wie in Tab. 48 dargestellt, wird angenommen, dass die IT-Abteilung des Pharmaunternehmens sich als strategischer Partner der Geschäftsfunktionen (siehe bspw. Venkatraman 1999) positionieren möchte und hiermit den Fokus auf die Generierung von Wertbeitrag durch die IT legen möchte. Als relevante Stakeholder, die im Rahmen von GRC für den IT-Change-Management-Prozess relevant sind, wurden Anteilseigner (Aktionäre), Konsumenten, wobei es sich im Kontext eines Pharmaunternehmens insbesondere um Patienten handelt, und Vertragspartner bzw. Kunden, womit für die IT-Abteilung insbesondere interne Kunden wie die geschäftliche Funktionen Einkauf, Produktion oder Finanzen gemeint sind, für welche IT-Dienstleistungen erbracht werden sollen, identifiziert. Aus der Strategie ergibt sich die Entscheidung, dass die IT-Änderungen stärker an den Geschäftsanforderungen auszurichten sind. Aus einem Assessment war hierzu ersichtlich, dass dies bislang nicht ausreichend der Fall war. Aus der strategischen Zielsetzung wurden mehrere Ziele abgeleitet, wobei zwischen geschäftlichen und IT-bezogenen Zielen unterschieden wird. Als geschäftliche Ziele sind die kontinuierliche Verbesserung der Geschäftsprozesse und die schnelle Reaktion auf geschäftliche Änderungen relevant. Aus diesen Geschäftszielen werden die IT-Ziele Liefern von IT-Lösungen, welche die Geschäftsanforderungen erfüllen und einen Wertbeitrag aufweisen und schnelle Reaktion auf geänderte geschäftliche Anforderungen und Umsetzung von IT-Änderungen gemäß den Vorgaben für Zeit, Qualität und Budget abgeleitet. Im Kontext des IT-Change-Managements sollen im Rahmen des Beispiels GRC-Vorgaben aus drei Bereichen betrachtet werden. Im Bereich Compliance mit Bezug zur Finanzberichterstattung ist für ein international agierendes Unternehmen, das an

der US-amerikanischen Börse gelistet ist oder Tochterunternehmen eines solchen Unternehmens ist, der SOX (SEC 2002) relevant. Hier sind insbesondere die Abschnitte 302 und 404 relevant. Des Weiteren hat das Unternehmen verpflichtend die Vorgaben im Bereich Qualitätsmanagement zu berücksichtigen. Im Rahmen des Beispiels soll insbesondere der Annex 11 des EU-Leitfadens (European Commission Health and Consumers Directorate 2010) betrachtet werden. Zudem hat die IT-Abteilung entschieden, ein Informationssicherheitsmanagementsystem (ISMS) aufzubauen, wobei der ISO 27001 Standard (DIN 2008a) als Grundlage verwendet werden soll. Die Strukturierung der GRC-Vorgaben könnte alternativ zur Strukturierung in GRC-Bereiche auch von den Quelldokumenten, wie den einzelnen Gesetzen ausgehen, und die Zuordnung zu dem jeweiligen GRC-Bereich als Attribut dokumentieren. Darüber hinaus erscheint bei der Ausarbeitung des Informationsobjekts GRC-Vorgabe sinnvoll, bereits grob einzelne Vorgaben innerhalb der Bereiche oder Quelldokumente zu identifizieren und in Form von Attributen zu dokumentieren. In Tab. 48 ist dies jeweils beispielhaft angedeutet.

Tab. 48: Beispiele zu den Informationsobjekten auf strategischer Ebene

Informationsobjekt	Beispiel
Strategie	(1) Positionierung der IT als strategischer Partner mit Fokus auf Generierung von Wertbeitrag durch die IT
Stakeholder	(1) Anteilseigner (Aktionäre)
	(2) Konsumenten (Patienten)
	(3) Vertragspartner / Kunden (geschäftliche Funktionen wie Einkauf, Produktion, Vertrieb, Finanzen usw.)
Entscheidung	(1) Stärkere Ausrichtung der IT-Änderungen an den Geschäftsanforderungen
Ziel	Geschäftsziele: (1) Kontinuierliche Verbesserung der Geschäftsprozesse (2) Schnelle Reaktion auf geänderte geschäftliche Änderungen
	IT-Ziele: (1) Liefern von IT-Lösungen, welche die Geschäftsanforderungen erfüllen und einen Wertbeitrag aufweisen (2) Schnelle Reaktion auf geänderte geschäftliche Anforderungen und Umsetzung von IT-Änderungen gemäß den Vorgaben für Zeit, Qualität und Budget
GRC-Vorgabe	(1) Compliance mit Bezug zur Finanzberichterstattung (SOX – Section 302 „Corporate Responsibility for Financial Reports" und Section 404 „Management Assessment of Internal Controls" (SEC 2002))
	(2) Qualitätsmanagement (Annex 11 – „10. Change and Configuration Management" (European Commission Health and Consumers Directorate 2010))
	(3) Informationssicherheit (ISO/IEC 27001:2005 – „A.12.5 Security in development and support processes" (DIN 2008a)

Auf der konzeptionellen Ebene sind die strategischen Aspekte zu analysieren und hinsichtlich einer operativen Umsetzung vorzubereiten. Hierbei sind insbesondere die Herleitung von konkreten Kontrollzielen,

die Analyse der Risiken und die Spezifikation der Richtlinien relevant. Eine Übersetzung der Ziele und der GRC-Vorgaben in konkrete Kontrollziele ist keine triviale Aufgabe. Gesetzliche Vorgaben sind in der Regel unkonkret und können nicht direkt übersetzt werden, was bei den betroffenen Unternehmen eine hohe Unsicherheit hervorruft (Nissen 2006, S. 79; Bretz 2007, S. 3). Der SOX (SEC 2002) fordert in Section 404 bspw. ein internes Kontrollsystem, macht aber keine konkreten Vorgaben für Kontrollen, die im Zuge des IT-Change-Managements zu berücksichtigen wären. Der Annex 11 des EU-Leitfadens (European Commission Health and Consumers Directorate 2010) führt zu IT-Change-Management lediglich das folgende aus. „Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure" (Annex 11 – „10. Change and Configuration Management"). Das Modell schlägt daher vor, die GRC-Vorgaben mit Rahmenwerken zu verknüpfen, die detailliertere Ausführungen beinhalten, wie die jeweiligen Vorgaben umzusetzen sind. Für den Bereich Qualitätsmanagement ist mit Bezug zur IT insbesondere der GAMP (ISPE 2008) in der Version 5 sowie ITIL im Bereich der Service Transition (OGC 2007b) und COBIT (ITGI 2007) relevant. Die jeweiligen relevanten Passagen sind in Tab. 49 wiedergegeben.

Risiken gefährden dem Modell folgend Ziele und können sich auf Geschäftsprozesse sowie auch direkt auf IT-Komponenten beziehen. Die Risiken sind ebenfalls in Tab. 49 beispielhaft dargestellt, wobei eine Analyse hinsichtlich Eintrittswahrscheinlichkeit und Schadenshöhe, die eine Priorisierung der Kontrollziele ermöglichen würde, nicht dargestellt ist. Es ist zudem darauf hinzuweisen, dass sich die Risiken zum Teil direkt aus den GRC-Vorgaben und den hieraus abgeleiteten Kontrollzielen ergeben. Eine Ausnahme stellt das Risiko „Änderungen ent-

sprechen nicht den Geschäftsanforderungen und liefern keinen Wertbeitrag", das sich aus den Zielen ergibt. Das Informationsobjekt Kontrollziel ermöglicht eine Integration in mehrfacher Hinsicht. Zum einen werden, wie bereits angesprochen, sowohl Risiken, die sich aus den Zielen als Teil der Governance-Aufgabe ergeben abgebildet und auch Kontrollziele aus den GRC-Vorgaben berücksichtigt. Zum anderen können anhand der Rahmenwerke überlappende Kontrollziele identifiziert werden (siehe Angaben zu Informationsobjekt Kontrolle in Tab. 50). Im Beispiel beziehen sich ein oder mehrere Kontrollziele auf ein Risiko. So wird das Risiko „Änderungen entsprechen nicht den Geschäftsanforderungen und liefern keinen Wertbeitrag" durch die Kontrollziele „Verhinderung von nicht-autorisierten Änderungen", „Umsetzung von Änderungen gemäß Geschäftsanforderungen" und „Kontrolle über IT-Änderungen" gesteuert. Des Weiteren wurde im Beispiel entschieden je GRC-Vorgabe, die hier in GRC-Bereiche strukturiert sind, eine Richtlinie und darüber hinaus eine Richtlinie für das IT-Change-Management auszufertigen, welche die Kontrollen für das IT-Change-Management zusammenfasst. Zudem existiert ein Service Level Agreement zwischen den Geschäftsbereichen und der IT-Abteilung, das die Support- und Reaktionszeiten und die Kostenstruktur für die Dienstleistungen der IT-Abteilung regelt. Der Anwendungsbereich der Richtlinien ist jeweils unterschiedlich und für das Beispiel in Tab. 49 dokumentiert. Das Risiko-Assessment wird ebenso wie das Geschäftsprozess-Assessment jährlich für den IT-Change-Management-Prozess durchgeführt. Aus dem Geschäftsprozess-Assessment ergibt sich ein Reifegrad für das IT-Change-Management, der im Beispiel auf COBIT (ITGI 2007, S. 18-19) basiert. Als Kennzahlen können die Anzahl von Störungen durch fehlerhafte Änderungen und der Prozentsatz an Änderungen, welche dem definierten IT-Change-Management folgen, genannt werden.

Tab. 49: Beispiele zu den Informationsobjekten auf konzeptioneller Ebene

Informationsobjekt	Beispiel
Kontrollziel	(1) Verhinderung von nicht-autorisierten Änderungen
	(2) Umsetzung von Änderungen gemäß Geschäftsanforderungen
	(3) Kontrolle über IT-Änderungen
	(4) Minimierung von Risiken für Patientensicherheit, Produktqualität und Datenintegrität
	(5) Verhinderung von fehlerhaften Änderungen
	(6) Gewährleistung einer adäquaten Dokumentation
	(7) Aufrechterhaltung der Sicherheit von Applikationen und Informationen
Risiko	(1) Änderungen entsprechen nicht den Geschäftsanforderungen und liefern keinen Wertbeitrag.
	(2) Änderungen gefährden die Patientensicherheit, Produktqualität und Datenintegrität.
	(3) Der Systemzustand hinsichtlich Konfiguration und Eigenentwicklungen ist unklar.
	(4) Änderungen beeinträchtigen die Sicherheit von Applikationen und Informationen.
Richtlinie	(1) IT-Change-Management-Richtlinie
	(2) Qualitätsmanagement-Richtlinie
	(3) Informationssicherheitsrichtlinie
	(4) Richtlinie zu Compliance mit Bezug auf Finanzberichterstattung
	(5) Service Level Agreement – IT-Abteilung mit Geschäftseinheiten
Rahmenwerk	(1) ITIL – Service Transition (OGC 2007b)
	(2) GAMP 5 – „4.3.4 Change Management" GAMP 5 – „Operation Appendices O6 Operational Change and Configuration Management" (ISPE 2008)
	(3) COBIT – „AI6 Manage Changes" (ITGI 2007)
Anwendungsbereich	(1) Alle IT-Änderungen (für die IT-Change-Management-Richtlinie)
	(2) Service Level Agreement (für die gesamte IT-

Informa-tionsobjekt	Beispiel
	Abteilung)
	(3) Qualitätsmanagement-Richtlinie / Informationssicherheitsrichtlinie / Richtlinie zu Compliance mit Bezug auf Finanzberichterstattung (unternehmensweit)
Kennzahl	(1) Anzahl von Störungen durch fehlerhafte Änderungen
	(2) Prozentsatz an Änderungen, welche dem definierten IT-Change-Management folgen
Assessment	(1) Risiko-Assessment IT-Change-Management 2014
	(2) Geschäftsprozess-Assessment IT-Change-Management 2014
Reifegrad	(1) Level 3 – Defined Process

Kernaufgabe auf operativer Ebene ist die Übertragung der Kontrollziele in konkrete Kontrollen, die dann in die Geschäftsprozesse eingebunden werden müssen. Die für das Beispiel relevanten Informationsobjekte auf operativer Ebene sind in Tab. 50 dargestellt. Jedes Kontrollziel kann durch eine oder mehrere Kontrollen, die in den Richtlinien spezifiziert sind, umgesetzt werden. Bspw. kann das Kontrollziel „Verhinderung von fehlerhaften Änderungen" durch die Kontrollen „Alle Prozessbeteiligten müssen bzgl. des Prozesses geschult sein" (3), „Vor Freigabe der Änderung für die produktive Verwendung muss ein dokumentierter Nachweis erbracht werden, dass die Änderung die intendierten Anforderungen erfüllt" (5) und „Es muss eine formale Freigabe für die Änderung erfolgen" (7) umgesetzt werden. Es ist wieder anzumerken, dass Kontrollen entweder aus Vorgabedokumenten und unter Einbeziehung von Rahmenwerken abgeleitet werden können oder Ergebnis der Risikoanalyse sind und somit die Erreichung der definierten Ziele unterstützen sollen. Ein Beispiel für letzteres ist die Kontrolle „Jede Änderung, die nicht der Behebung eines Fehlers dient und eine Kostenschätzung von mehr als 20.000 Euro aufweist, muss durch das Change Advisory Board freigegeben werden" (8). Die für das IT-

Change-Management relevanten Dokumentationen sind der Änderungsantrag, die Testdokumentation sowie System-Lebenszyklus-Dokumentation. Unterstützt wird der IT-Change-Management-Prozess durch das IT-Service-Management-System und ein Dokumentenmanagement-System, welches für die Verwaltung der System-Lebenszyklus- und Testdokumentation verwendet wird. Für die Kontrollen ist zudem zu entscheiden, ob sie automatisiert bzw. durch IT unterstützt werden sollen oder ob eine manuelle Ausführung erfolgt. Für einige Kontrollen wie die Anpassung der System-Lebenszyklus-Dokumentation (Kontrolle (4)) oder die Notwendigkeit von Schulungen erscheint eine Automatisierung (Kontrolle (3)) fraglich. Trotzdem könnten diese durch Konsistenzprüfungen unterstützt werden. Als Ressourcen sind im Beispiel Daten relevant, die unter anderem als Gegenstand der Informationssicherheit angesehen werden können. Die relevanten Rollen sind der Antragssteller, der Change Manager, das Change Advisory Board bzw. deren Teilnehmer, der Entwickler, der Tester und die Qualitätssicherung. Diese Rollen sind direkt durch die Kontrolle (3) betroffen und müssen demnach geschult sein. Im Beispiel wurde Kontrolle (4) verletzt, da in einigen Änderungen die betroffene System-Lebenszyklus-Dokumentation nicht angepasst wurde. Im Rahmen des Assessments wurde hierzu ebenfalls eine Schwachstelle festgestellt.

Tab. 50: Beispiele zu den Informationsobjekten auf operativer Ebene

Informationsobjekt	Beispiel
Kontrolle	(1) Für jede Änderung muss eine Risikoanalyse hinsichtlich des Einflusses auf Patientensicherheit, Produktqualität und Datenintegrität erfolgen (GAMP 5 O6).
	(2) Vor Realisierung der Änderung muss die Änderung auf ihre Auswirkungen bewertet, priorisiert und autorisiert werden (COBIT AI6.2, GAMP 5 O6).
	(3) Alle Prozessbeteiligten müssen bzgl. des Prozesses geschult sein (GAMP 5 O6).
	(4) Die durch die Änderung betroffene Dokumentation muss angepasst werden (COBIT AI6.5, GAMP 5 O6).
	(5) Vor Freigabe der Änderung für die produktive Verwendung muss ein dokumentierter Nachweis erbracht werden, dass die Änderung die intendierten Anforderungen erfüllt (ISO/IEC 27001:2005 A.12.5.2, GAMP 5 O6).
	(6) Es muss eine formale Freigabe für die Änderung erfolgen (COBIT AI6.2, GAMP 5 O6).
	(7) Änderungen sollten durch einen formalen IT-Change-Management-Prozess kontrolliert werden (COBIT AI6.1; ISO/IEC 27001:2005 A.12.5.1, GAMP 5 O6).
	(8) Jede Änderung, die nicht der Behebung eines Fehlers dient und eine Kostenschätzung von mehr als 20.000 Euro aufweist, muss durch das Change Advisory Board freigegeben werden.
Ressource	(1) Daten
Dokumentation	(1) Änderungsantrag
	(2) Testdokumentation
	(3) System-Lebenszyklus-Dokumentation
IT-Komponente	(1) IT-Service-Management-Werkzeug
	(2) Dokumentenmanagement-System
Verletzung	(1) Betroffene System-Lebenszyklus-Dokumentation wurde nicht vor Freigabe der Änderung für die produktive Verwendung überarbeitet.
Rolle	(1) Antragsteller
	(2) Change Manager

Informa-tionsobjekt	Beispiel
	(3) Change Advisory Board
	(5) Entwickler
	(6) Tester
	(7) Qualitätssicherung
Geschäfts-prozess	(1) IT-Change-Management
Schwach-stelle	(1) Keine (automatische) Prüfung, dass die betroffene System-Lebenszyklus-Dokumentation vor Freigabe der Änderung für die produktive Nutzung angepasst wurde.

Das dargestellte Demonstrationsbeispiel verfolgte das Ziel, die Informationsobjekte und Beziehungen des datenseitigen Modells für das strategische GRC-Management an einem fiktiven Beispiel zu erläutern. Darüber hinaus kann anhand des Beispiels die grundsätzliche Konsistenz des Modells verdeutlicht werden. Wie bereits erwähnt, kann das Beispiel nur einen kleinen Ausschnitt betrachten, und es bleiben Aspekte der Realität unberücksichtigt. Obwohl das Beispiel lediglich das IT-Change-Management betrachtet und sogar in diesem Bereich nur einen Ausschnitt, wird die Komplexität der zu erfassenden und zu verwaltenden Informationen deutlich. Dies zeigt, dass eine strukturierte Herangehensweise, wie sie von dem Modell unterstützt werden soll, notwendig ist. Des Weiteren sind zwei konkrete Anmerkungen zu den Informationsobjekten Entscheidung und Assessment und deren Beziehungen zu machen. Entscheidungen werden nach dem Modell grundsätzlich durch die Strategie beeinflusst und werden durch Assessments und Kennzahlen mit Informationen versorgt. Sie können jedoch auf nahezu alle anderen Informationsobjekte Auswirkungen haben. So kann z.B. die Entscheidung getroffen werden Ziele anzupassen oder Geschäftsprozesse bzw. unterstützende IT-Systeme zu verändern. Unternehmen müssen sich zudem bei der Anwendung des Modells überlegen, wie

Entscheidungen durch entsprechende Maßnahmen umgesetzt werden können, womit ein kontinuierlicher Verbesserungsprozess eingeleitet werden kann. Assessments beziehen sich dem Modell folgend neben Risiken auf die Geschäftsprozesse, was auch in Übereinstimmung mit COBIT (ITGI 2007, S. 18-20) ist. Im Kontext von GRC ist jedoch insbesondere die Beurteilung der Durchführung und Wirksamkeit der Kontrollen zu prüfen, die in den Geschäftsprozessen implementiert sind. COBIT schlägt in diesem Kontext die Berücksichtigung von verschiedenen Eigenschaften der Geschäftsprozesse vor, zu welchen unter anderem die Kommunikation, die Richtlinien und somit auch die Kontrollen, die unterstützendenden Werkzeuge sowie die Definition der Verantwortlichkeiten gehören.

5.4 Evaluierung

5.4.1 Grundlagen und Vorgehensweise der Evaluierung

Die Evaluierung des entwickelten Artefakts ist ein wichtiger Bestandteil gestaltungsorientierter Forschung, wofür verschiedene Evaluierungsmethoden eingesetzt werden können (Hevner et al. 2004; Riege et al. 2009). Pfeiffer und Niehaves (2005) unterscheiden Evaluierungskriterien und -methoden hinsichtlich der von Hevner et al. (2004) beschriebenen Typen von Artefakten. Hinsichtlich der Evaluierungsmethoden für (Referenz-)Modelle wird ein Forschungsdefizit festgestellt (Pfeiffer und Niehaves 2005, S. 11). Als Evaluierungskriterien für Modelle werden beispielhaft die Grundsätze ordnungsmäßiger Modellierung (GoM, Schütte 1997) genannt. Diese führen den Grundsatz der Konstruktionsadäquanz, den Grundsatz der Sprachadäquanz, den Grundsatz der Wirtschaftlichkeit, den Grundsatz des systematischen Aufbaus, den Grundsatz der Klarheit und den Grundsatz der Vergleichbarkeit ein, können jedoch nur als ein Vorschlag neben anderen betrachtet werden.

Fettke und Loos (2004a) betrachten ebenfalls Evaluierungsmethoden für Referenzmodelle und fordern eine multiperspektivische Evaluierung, da einzelne Evaluierungsmethoden nicht alle möglichen Evaluierungskriterien abdecken können.

Da weder allgemeingültige Evaluierungskriterien noch Evaluierungsmethoden für (fachkonzeptionelle Referenz-)Modelle bekannt sind, wird hier eine Evaluierung gegen das Forschungsziel vorgenommen. Ziel war es explizit nicht bestehende Management-Ansätze abzubilden, sondern ein Sollmodell für das strategische GRC-Management zu entwickeln. Gleichwohl sollte dieses Modell in der Lage sein, die relevanten Informationsobjekte hinsichtlich einer Integration von GRC auf strategischer Ebene adäquat abzubilden. Die Evaluierung adressiert daher die Adäquanz der Informationsobjekte insbesondere hinsichtlich des Abstraktionsniveaus und der verwendeten Begrifflichkeiten, die Vollständigkeit der Informationsobjekte sowie die Modellierung der Beziehungen zwischen den Informationsobjekten. Des Weiteren soll eine Detaillierung der Informationsobjekte durch Attribute basierend auf Praxisanforderungen erfolgen.

Da die GRC-Integration auf strategischer Ebene in der Forschung bislang nur wenig betrachtet wurde, werden dem Vorschlag von Gericke et al. (2009a) folgend Praxisbeschreibungen aus den GRC-Teildisziplinen zur Evaluierung des datenseitigen Modells eingesetzt. Praxisbeispiele werden hierbei als Darstellungen von erfolgreichen Implementierungen verstanden. Die Auswertung von Fallbeispielen bietet die Möglichkeit, ein relativ großes Spektrum an unterschiedlichen Fällen mit ausreichender inhaltlicher Tiefe zu erreichen. Der Forderung nach einer multiperspektivischen Evaluierung (Fettke und Loos 2004a) folgend wären weitere Evaluierungen bspw. mit Hilfe des Metamodells hinsichtlich der korrekten Syntax denkbar. Eine Anwendung des Mo-

dells bei der Herleitung eines unternehmensspezifischen Modells in der Praxis wäre ebenfalls wünschenswert um weitere Erkenntnisse hinsichtlich der Nützlichkeit zu erhalten. Der Erfolg der Anwendung ist jedoch auch von einer Reihe weiterer Faktoren abhängig. So stellt eine Anwendung Anforderungen an den Reifegrad des GPM des Unternehmens, die Verfügbarkeit von Management-Methoden wie der Risikoanalyse und das zur Unterstützung verwendete Informationssystem. Für die Implementierung des vorliegenden Modells in einem Informationssystem muss zudem neben der hier definierten Struktur auch die Verhaltenssicht im Sinne der Geschäftsprozesse eines solchen Management-Ansatzes festgelegt werden.

5.4.2 Übersicht der publizierten Fallbeispiele

Um Praxisbeschreibungen zu finden wurde praxisnahe Literatur in der durchgeführten Literaturrecherche und durch die Suche in allgemeinen Suchmaschinen wie Google und GoogleScholar sowie in praxisnahen Publikationsorganen wie der Zeitschrift für Controlling & Management oder der Zeitschrift für IT-Governance der ISACA identifiziert. Es wurden Praxisbeispiele zu integrierten GRC-Ansätzen und aus den Teilbereichen von GRC berücksichtigt, die basierend auf den Anforderungen für das strategische GRC-Management, eine thematische Relevanz für das datenseitige Modell aufweisen. Die gefundenen Fallbeispiele wurden weiterhin anhand ihrer inhaltlichen Qualität im Sinne einer ausreichenden inhaltlichen Tiefe ausgewählt. Hierbei wurde geprüft, ob die Praxisbeispiele die Beantwortung der im Folgenden formulierten Forschungsfragen für die Evaluierung unterstützen. Insgesamt wurden 21 relevante Praxisbeispiele berücksichtigt. Im Anschluss wurden die wichtigsten Begriffe hinsichtlich der Informationsobjekte je Fallbeispiel aufgenommen und anhand der Entitäten des entwickelten Modells zugeordnet. Hierbei wurden folgende Aspekte berücksichtigt.

1. Können die Informationsobjekte aus dem entwickelten Modell bestätigt werden?
2. Ist der Abstraktionsgrad angemessen?
3. Können die Beziehungen zwischen den Informationsobjekten bestätigt werden?
4. Gibt es Hinweise auf die Integration und strategische Ausrichtung des GRC-Managements?

Die konkrete Vorgehensweise zur Auswertung der Praxisbeispiele ist angelehnt an die qualitative Inhaltsanalyse (Bohnsack et al. 2006; Mayring 2008). In einem ersten Schritt wurden wichtige Begriffe aus den Praxisbeispielen extrahiert und auch verschiedene Begriffe, die innerhalb eines Textes gleiche Konzepte benennen, zugeordnet. Hierbei wurde bewusst auch auf wichtige Begriffe geachtet, die in dem zu diesem Zeitpunkt erreichten Stand des Modells nicht vorkamen. In einem zweiten Schritt wurden die in den Praxisbeispielen gefundenen wichtigen Begriffe den Informationsobjekten des Modells zugeordnet. Begriffe, die nicht den bisherigen Informationsobjekten zugeordnet werden konnten, wurden separiert gesammelt und vereinheitlicht. Zusätzlich wurden die Texte nochmals bzgl. einer Bestätigung dieser zusätzlichen Begriffe durchsucht. Neben den dargestellten Evaluierungszielen werden nachfolgend auch allgemeine Beobachtungen, die im Rahmen der Auswertung gemacht wurden, dargestellt. Die nachfolgenden Tabellen (Tab. 51, Tab. 52, Tab. 53 und Tab. 54) geben einen Überblick zu den Fallbeispielen.

Tab. 51: Übersicht der zur Evaluierung verwendeten Praxisbeispiele (1 von 2)

Nr.	Quelle	Beschreibung des Fallbeispiels
1	Bamberg und Kaven 2006	Der Beitrag stellt die Vorgehensweise der Deutschen Telekom zur Erfüllung der Vorgaben aus dem SOX (insbesondere Section 404) vor.
2	Eckert et al. 2004	Der Beitrag beschreibt die Umsetzung eines Risikomanagementsystems bei der DÜRR AG unter Berücksichtigung von regulatorischen Vorgaben und auf Grundlage des COSO-Standards.
3	Fröhlich und Glasner 2007b	In diesem Beitrag wird die Etablierung einer zentralen Service-Organisation für das Rechnungswesen eines global tätigen Konzerns dargestellt.
4	Fröhlich und Glasner 2007c	Der Beitrag beschreibt den IT-Governance-Ansatz bei PricewaterhouseCoopers.
5	Fröhlich und Glasner 2007a	Der Beitrag beschreibt das Projekt zur Einführung einer IT-Governance bei einem IT-Service-Provider innerhalb eines Konzerns.
6	Gigerl et al. 2007	Der Beitrag beschreibt am Beispiel von ALTANA Pharma den Aufbau und die Einführung eines integrierten IT-Compliance-Rahmenwerks auf Basis von COBIT 3.0.
7	Heydkamp und Ostrowski 2006	Der Beitrag beschreibt das Projekt zur Umsetzung der Anforderungen aus dem SOX und die darauf aufbauende Etablierung eines regelmäßigen Management-Ansatzes bei IBM.
8	Joachim 2006	Das Praxisbeispiel beschreibt das Projekt zur Umsetzung von Anforderungen an „rechnungslegungsrelevante Aussagen“ insbesondere im Rahmen der Section 404 des SOX bei E.ON.
9	Just und Tami 2007	Der Beitrag stellt ein IT-Governance-Projekt bei einem Finanzdienstleistungsinstitut dar.
10	Kley 2011	Der Beitrag beschreibt das integrierte Risiko- und Chancenmanagement bei der MAN SE.
11	Kremer und Haase 2011	Der Beitrag beschreibt die Einführung einer IT-Governance bei der Deutschen Bahn AG unter Verwendung des COBIT-Frameworks.

Tab. 52: Übersicht der zur Evaluierung verwendeten Praxisbeispiele (2 von 2)

Nr.	Quelle	Beschreibung des Fallbeispiels
12	Kurz und Woltering 2008	Der Beitrag beschreibt verschiedene Aspekte der ITK-Governance bei der Deutschen Bahn AG im Bereich Personenverkehr.
13	Michels und Krzeminska 2006	Der Beitrag beschreibt den Ansatz zum Organisations-Controlling bei der AXA Konzern AG, wobei auf die Ziele Conformance und Performance eingegangen wird.
14	Morgenthaler 2011	Der Beitrag stellt das Datenschutzmanagementsystem im Active Global Support der SAP AG dar.
15	Mucic 2006	Der Beitrag beschreibt die Umsetzung der Vorgaben aus dem SOX an interne Kontrollsysteme für die Finanzberichterstattung und die hierauf aufbauende Einführung eines ganzheitlichen Risikomanagement-Ansatzes bei der SAP AG.
16	Riegler 2001	Der Beitrag beschreibt Umsetzungserfahrungen eines wertorientierten Management-Ansatzes im DaimlerChrysler Konzern.
17	Ritschel et al. 2006	Der Beitrag beschreibt das Projekt der IT von Novartis zur Umsetzung der Anforderungen aus dem SOX.
18	Ritzmann 2006	Der Beitrag stellt die freiwillige Einführung eines an die Anforderungen des SOX angelehnten internen Kontrollsystems bei den Schweizerischen Bundesbahnen (SBB) dar.
19	Saalfeld 2006	Der Beitrag stellt den Aufbau der konzernweiten Organisation des internen Kontrollsystems hinsichtlich der Finanzberichterstattung der Bayer AG dar.
20	Tüllner 2012	Der Beitrag stellt ein Projekt zur Verbesserung von GRC durch Integration und Verbesserung der Berichtserstattung dar.
21	Vogler und Lelke 2006	Der Beitrag beschreibt die Konzeption und Umsetzung eines IT-Governance-Ansatzes in der RAG Coal International.

Tab. 53: Charakteristika der Fallbeispiele (1 von 2)[96]

Nr.	Quelle	Gegenstand	GRC-Vorgaben	Standards / Best Practices	Branche
1	Bamberg und Kaven 2006	Compliance-Management	SOX	COSO	Telekommunikation
2	Eckert et al. 2004	Risikomanagement	KonTraG, DCGK, TransPuG, SOX Sec. 404	IDW PS 340, DRS 5, COSO	Automobilindustrie
3	Fröhlich und Glasner 2007b	IT-Governance	IFRS	---	nicht bekannt
4	Fröhlich und Glasner 2007c	IT-Governance	---	ITIL	Unternehmensberatung
5	Fröhlich und Glasner 2007a	IT-Governance	SOX, SAS 70	COBIT, ITIL	IT-Service-Provider
6	Gigerl et al. 2007	IT-Compliance-Management	SOX, GxP, Basel II	COBIT, ITIL, ISO/IEC 20000, ISO 17799, GAMP	Pharmaindustrie

[96] Die Tabelle verwendet die nachfolgend aufgelösten Abkürzungen. Sarbanes-Oxley-Act (SOX), Sarbanes-Oxley-Act Section 404 (SOX Sec. 404), Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), Deutscher Corporate Governance Kodex (DCGK), Transparenz- und Publizitätsgesetz (TransPuG), International Financial Reporting Standards (IFRS), Service Organization Auditing Standards (SAS 70), Gute Arbeitspraxis (GxP), Public Company Accounting Oversight Board (PCAOB), Bundesdatenschutzgesetz (BDSG), Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), Committee of Sponsoring Organizations of the Treadway Commission (COSO), Institut der Wirtschaftsprüfer in Deutschlane e.V. (IDW), Prüfungsstandard (PS), Deutscher Rechnungslegungsstandard (DRS), International Organization for Standardization (ISO), Capability Maturity Model (CMM), Good Automated Manufacturing Practice (GAMP), Control Objectives for Information and Related Technology (COBIT), IT Infrastructure Library (ITIL).

Tab. 54: Charakteristika der Fallbeispiele (2 von 2)

Nr.	Quelle	Gegenstand	GRC-Vorgaben	Standards / Best Practices	Branche
7	Heydkamp und Ostrowski 2006	Compliance-Management / Controlling	SOX	COSO	Informationstechnologie
8	Joachim 2006	Compliance-Management	PCAOB Auditing Standard (AS) No. 2	---	Energieindustrie
9	Just und Tami 2007	IT-Governance	---	COBIT, ITIL, CMM	Finanzdienstleistungen
10	Kley 2011	Risikomanagement	---	---	Automobilindustrie
11	Kremer und Haase 2011	IT-Governance	BDSG, KonTraG, GDPdU, SOX	COBIT, ITIL	Mobilitäts- und Logistikdienstleistung
12	Kurz und Woltering 2008	IT-Governance	---	COBIT	Mobilitäts- und Logistikdienstleistung
13	Michels und Krzeminska 2006	Compliance-Management / Controlling	SOX	Six Sigma	Versicherungsbranche
14	Morgenthaler 2011	IT-Compliance-Management	BDSG	---	Softwareindustrie
15	Mucic 2006	Compliance-Management	SOX	COSO II	Softwareindustrie
16	Riegler 2001	Wertorientierte Unternehmensführung	---	---	Automobilindustrie
17	Ritschel et al. 2006	IT-Compliance-Management	SOX	COBIT	Pharmaindustrie
18	Ritzmann 2006	Compliance-Management	freiwillige Umsetzung von SOX	COSO	Mobilitäts- und Logistikdienstleistung
19	Saalfeld 2006	Compliance-Management	SOX	---	Pharmaindustrie
20	Tüllner 2012	GRC	---	---	Produktionsunternehmen
21	Vogler und Lelke 2006	IT-Governance	Basel II, SOX	COBIT, ITIL	Bergbau/Chemie

Die Fallbeispiele decken ebenso wie die zur Entwicklung des Modells ausgewerteten Quellmodelle die verschiedenen Gegenstandsbereiche von GRC ab. Hierbei wurde darauf geachtet, dass alle GRC-Teildisziplinen sowie unternehmensweite als auch IT-bezogene Ansätze adäquat berücksichtigt wurden. Ebenso werden von den Fallbeispielen unterschiedliche GRC-Vorgaben, Standards bzw. Best Practices und Branchen diskutiert. Dies wird ebenfalls als Stärke angesehen, da das Modell im Sinne einer Allgemeingültigkeit einen möglichst großen Anwendungsbereich umfassen soll. Tab. 53 und Tab. 54 und geben einen Überblick zu den Charakteristika der ausgewerteten Texte. Es ist anzumerken, dass hinsichtlich des Gegenstandsbereiches die in der Publikation getroffene Zuordnung berücksichtigt wurde. Außerdem liegt eine gewisse Dominanz des SOX vor, die mit der großen Bedeutung dieses Gesetzes für die Unternehmenspraxis begründet werden kann.

5.4.3 Ergebnisse der Evaluierung

5.4.3.1 Allgemeine Beobachtungen

Grundsätzlich zeigt sich auch bei der Auswertung der Praxisbeispiele, dass eine einheitliche Terminologie in der Praxis fehlt. Dies unterstreicht, dass die Schaffung und Etablierung einer einheitlichen Terminologie, wozu das Modell beitragen soll, notwendig ist. Teilweise werden unterschiedliche Begriffe für gleiche Sachverhalte verwendet bzw. nur unzureichend gegeneinander abgegrenzt. Zwischen den GRC-Teildisziplinen sowie verschiedenen Branchen lassen sich in den Praxisbeispielen kaum Unterschiede bzgl. der Informationsobjekte feststellen. Vielmehr sind jeweils Kernbegriffe wie Kontrolle, Geschäftsprozess, Risiko und verschiedene Begriffe zu den GRC-Vorgaben auszumachen. Aufgrund der hohen branchenübergreifenden Bedeutung des SOX hat Finanzberichterstattung insgesamt eine hohe Bedeutung. Wei-

terhin wird die Involvierung des Top-Managements für viele Aufgaben als wichtig angesehen. Ebenfalls wird explizit auf die Unsicherheit in der Praxis hinsichtlich der Management-Methoden für GRC hingewiesen (Joachim 2006, S. 445; Menzies 2006, S. 445). Rahmenwerke, wie COSO und COBIT, werden als zu abstrakt bewertet und lassen sich nicht immer eindeutig von den eigentlichen regulatorischen Vorgaben unterscheiden.

5.4.3.2 Adäquanz und Vollständigkeit der Informationsobjekte

Tab. 55 und Tab. 56 beinhalten die Zuordnung der in den Praxisbeispielen identifizierten relevanten Begriffe zu den Entitäten des Modells. Der Verweis auf die zu Grunde liegenden Fallbeispiele ist in Klammern gemäß den Nummern aus Tab. 51 bzw. Tab. 52 angegeben. Darüber hinaus wird die Anzahl der Praxisbeispiele, aus denen sich Begriffe zu den Entitäten des Modells zuordnen lassen, aufgeführt.

Es zeigt sich eine Übereinstimmung von Begriffen und eine ähnliche Verteilung wie bei der Auswertung der Quellmodelle. Es ist jedoch anzumerken, dass keines der Beispiele alle Informationsobjekte bestätigt, was darauf zurückzuführen ist, dass lediglich von Tüllner (2012) ein integrierter GRC-Ansatz betrachtet wird. Die Modelle aus der GRC-Literatur sind oftmals mit dem Ziel der Automatisierung entwickelt worden, was nicht Gegenstand der Praxisbeispiele ist, obwohl auch hier die IT-Unterstützung eine wichtige Rolle einnimmt. Das Informationsobjekt Implementierungslogik wird daher nicht bestätigt. Das Informationsobjekt Ausführung wurde nur in einem Fallbeispiel bestätigt und wird daher mit Geschäftsprozess zusammengefasst.

Das Abstraktionsniveau des Modells erscheint insgesamt angemessen, da die ähnlichen verwendeten Begrifflichkeiten auch ein ähnliches Abstraktionsniveau signalisieren. Hinsichtlich der Ausprägung der Attribute zu den Informationsobjekten ist jedoch eine weitere Detaillierung er-

forderlich. Bezüglich des Informationsobjekts Kontrolle wird festgestellt, dass Kontrollen auf unterschiedlichen Ebenen relevant sind. So unterscheiden Bamberg und Kaven (2006, S. 435) Company Level Controls sowie Business und IT Controls. Darüber hinaus wird auf Wirkungszusammenhänge zwischen den Kontrollen hingewiesen (Bamberg und Kaven 2006, S. 437-438). Eine weitere Beobachtung ist die Fokussierung auf „key controls" in der Praxis. Hiermit soll sich GRC auf bestimmte kritische Bereiche konzentrieren, die entweder zeitlich priorisiert werden oder auf die sich GRC sogar gänzlich beschränkt. Geschäftsprozessen wird eine hohe Bedeutung zuteil und Prozess oder ähnliche Begriffe werden ausnahmslos in allen Praxisbeispielen genannt. Unter Geschäftsprozessen werden hierbei explizit auch die Führungs- und Management-Prozesse von GRC verstanden. Außerdem findet teilweise eine Unterscheidung zwischen Kern- und Unterstützungsprozessen zur Priorisierung von Aktivitäten statt. Rollen und Verantwortlichkeiten werden auf unterschiedlichen Hierarchieebenen betont. Geschäftsdokumente werden in den Praxisbeispielen im Wesentlichen hinsichtlich der Dokumentation des Kontrollsystems und hinsichtlich eines internen und externen Berichtwesens verstanden. Im Bereich der Risiken wird eine Unterteilung in Risikofelder bzw. Risikokategorien vorgeschlagen (Kley 2011). Des Weiteren findet eine Erweiterung des Risikos um Chancen statt. Anhand der Fallbeispiele wird außerdem deutlich, dass eine Unterscheidung zwischen einer GRC-Quelle und Rahmenwerken im Sinne von Standards und Best Practice, welche GRC unterstützen sollen, nicht immer eindeutig möglich ist. Die Praxisbeispiele zeigen deutlich, dass neben der Bewertung der Compliance auch finanzielle Kennzahlen wie Rentabilität, Ertrag und Kosten von hoher Bedeutung für GRC sind. Ebenso ist eine Planung im Sinne einer Budgetvorgabe relevant und muss mit Hilfe von Kennzahlen gemessen werden. Letztlich zeigt sich auch die Bedeutung der

Begriffe Wert bzw. Wertbeitrag. Diese werden entweder direkt auf die Kontrollen angewendet oder meinen den Wertbeitrag der durch die Steuerung von Geschäftsprozessen oder IT-Komponenten erbracht werden soll.

Tab. 55: Zuordnung von wichtigen Begriffen aus den Fallbeispielen zu den Entitäten des Modells (1 von 2)

IO	Zugeordnete Begriffe	Anz.
Kontrolle	Maßnahme (1), Kontrolle (2), Control/Kontrolle (3), Kontrolle (4), Kontrolle/Risk Response/Control Activities (5), Control/Key Control (6), interne Kontrolle/Kontrollmechanismus/Risk Response/Control Activity (7), SOX-Kontrolle/IT-Kontrolle/Regel (8), (interne) Kontrolle (9), Kontrollsystem/Kontrollen/interne Kontrollen/Kontrollaktivitäten/Gegenmaßnahme (zur Bewältigung der Risiken)/Verhaltensregel (10), Kontrollmaßnahme/Steuerungsmaßnahme (11), Regel (12), Gegenmaßnahme (13), IT-Control (15), Regel (17), (technisch-organisatorische) Maßnahme (18), Kontrolle/ITK-Governance-Maßnahme (19), (Prozess)kontrolle/Key Control/Maßnahme (21)	18
Rolle	Abteilung (2), Beteiligter (3), verantwortliche Managementebene (4), Verantwortlichkeit (5), Funktionsbereich/Verantwortlichkeit (7), IT-Verantwortlicher/GxP-Verantwortlicher (8), Prozessverantwortlicher/Zuständigkeit (9), Prozesseigner (10), Verantwortlichkeit (11), Stelle/GRC-Verantwortlicher (13), Rolle (15), Verantwortlicher (16), Verantwortungsbereich (18), Rolle/Verantwortlichkeit/Geschäftsprozessverantwortlicher (19), Rolle (20), Verantwortlichkeit (21)	16
Geschäftsprozess	Führungsprozess (1), Geschäftsprozess (2), Prozess (3), Prozess (4), Geschäftsprozess (5), Risikomanagement-Prozess (5), Führungsprozess/Geschäftsprozess/Supportprozess (6), Ablauf/Risikomanagementprozess/Prozess (7), Prozess (8), (Kern)Prozess (9), Prozess (10), Prozess (11), Prozess (12), Prozess (13), Prozess (14), IT-Prozess (15), Prozess (16), IT-Aktivitäten (17), Prozess (18), (ITK-)Prozess (19), Unternehmensarchitektur (19), Risikomanagementprozess (19), ITK-Prozess (20), Prozess(domäne) (21)	21
Risiko	Risiko (2), Risiko (4), Risiko (5), Risiko (7), Chance (7), Risiko (8), Risiko (9), Risiko (10), Risiko (11), Chance (11), IT-Risiko (12), Risiko (13), Risiko (15), Risiko (19), Risiko (21)	13
Kontrollziel	S-OX404-Anforderung (3), Kontrollziel (3), Kontrollziel (4), SOX-Anforderung (6), Anforderung (7), Kontrollziel/Anforderung (8), Anforderung (9), (SOX-)Anforderung (10), (regulatorische) Anforderung (13), Kontrollziel (15), IFRS Requirement (16), Anforderung (18), Anforderung/Kontrollziel (19), Vorschrift/Anforderung/Kontrollziel (21)	13
GRC-Vorgabe	Regularien (5), Gesetz (7), Richtlinie (hier als Standard/Best Practice gemeint) (7), Gesetz/Norm (8), geltendes Recht (9), Gesetz (10), Vertrag (18)	6
Ressource	Finanzdatum (9), (Finanz)Daten (10), Produkt (11), IT-Ressource (12), Daten (13), Daten (16), Daten (18)	7
Ziel	Ziel (1), Geschäftsziel (5), Ziel/Geschäftsziel (7), Ziel (8), Ziel (9), Ziel (11), Strategisches Unternehmensziel (12), geschäftsprozessbedingten Anforderungen (Geschäftsziele) (14), Ziel (15), Geschäftsziel (17), Unternehmensziel/ITK-Ziel (19), Unternehmensziel/ITK-Ziel (20)	12

Tab. 56: Zuordnung von wichtigen Begriffen aus den Fallbeispielen zu den Entitäten des Modells (2 von 2)

IO	Zugeordnete Begriffe	Anz.
Assessment	Prüfung/Management Assessment (2), Reviewtätigkeit/Testverfahren/Bewertungsverfahren/Checkliste (3), Design Assessment/Testing/Risk Assessment (5), Beurteilung/Test (6), Überwachung (7), Revision/Audit/Risiko-Assessment/(Kontroll-)Tests (8), Test/Revision/Messung/Prüfung (9), Testing/Risiko Assessment/Überwachung/Monitoring/Zertifizierung (der Regeleinhaltung) (10), Audit (14), Audit/Prüfung (15), Messen der SLA (16), Prüfung/Review/Audit/Zertifikat/Risikoanalyse (18), Audit/Prüfung/IT-Revision (19), Test/Audit/Review (21)	14
Kennzahl	Kennzahl (1), Werttreiber/Wert (1), Added Value (6), Kennzahl (7), Ertrag/Rentabilität (7), Wert (7), Messgröße (8), Wirtschaftlichkeit/Kosten (12), Kennzahl (12), IT-Kostenstruktur (14), Kennzahl (15), Kosten (17), Messkriterium/Kennzahl (19), Wertbeitrag (19), Budget/Planung (20), Business Value (21)	12
Richtlinie	Richtlinie (5), Policy (7), Arbeitsanweisung (Standard Operating Procedure (8), Organisationsrichtlinie/Arbeitsrichtlinie (9), (Konzern)Richtlinie (10), Richtlinie (im Sinne von internen Policies und Best Practices) (12), Arbeitsanweisung/Verfahrensdokumentation/Policy (15), Richtlinie/Policy (17), Policy (18), Richtlinie (19), Richtlinie (20), Standard Operating Procedure/Arbeitsanweisung (21)	12
Dokumentation	Bericht (1), Kontrolldokumentation (3), Bericht (3), Bericht/Report (4), Dokumentation (5), Report (5), Dokumentation (6), Dokumentation (8), Dokumentation (9), Dokumentation (10), Bericht (11), Dokument (12), Bericht (13), Dokumentation (15), Reporting (15), Reporting (16), Bericht/Report (17), Dokument (18), DSMS-Handbuch (18), Dokument (21)	16
IT-Komponente	IT (2), IT System (3), IT System (4), IT (5), IT-Infrastruktur/IT-Anwednungen/IT-System (8), IT-System (9), Informationstechnologie/IT/Applikation (10), IT (12), IT (als Gegenstand) (14), Software (zur Unterstützung der IT-Governance) (15), IT (15), Tool (16), ITK-Anwendung/ITK-Plattform/ITK-Infrastruktur (19), ITK-Landschaft (20), Anwendung/Infrastruktur (21)	14
Anwendungsbereich	Scope (9), Scope (15), Geltungsbereich (18), Domäne (19), Geltungsbereich (21)	5
Ausführung	Geschäftsvorfall (4)	1
Implementierungslogik	---	0
Rahmenwerk	Standard/Best-Practice (8), Rahmenwerk (10), Richtlinie (im Sinne von internen Policies und Best Practices) (12), Standard/Best Practice (15), Standard (18), Standard/Framework (19), Standard (20)	7

IO	Zugeordnete Begriffe	Anz.
Strategie	Strategie (1), Strategie (5), Unternehmensstrategie (7), Strategie (11), Unternehmensstrategie (13), Strategie (14), Strategie (16), IT-Strategie (17), strategische Ausrichtung (19), ITK-Startegie (20)	10
Stakeholder	Stakeholder (1), externe Anspruchsgruppe (8), Shareholder (12), Stakeholder (17), Auftraggeber/Auftragnehmer (18), Stakeholder (19)	6
Reifegrad	Reifegrad (14), Reifegrad (19), Reifegradmodell (21)	3
Verletzung	Abweichung (7), Datenschutzvorfall (18)	2

Die Praxisbeispiele beinhalten außerdem weitere Begriffe, die für GRC als relevant erachtet werden. Diese sind in gleicher Weise wie die den Entitäten des Modells zugeordneten Begriffe in Tab. 57 dargestellt. In vielen Praxisbeispielen wird die Komplexität der Organisationsstruktur internationaler Konzerne deutlich (siehe Begriff Struktureinheit). Hierbei muss festgelegt werden, welche Verantwortung innerhalb des Konzerns, bspw. im Rahmen einer Holding, liegt und welche Verantwortung die einzelnen Divisionen des Konzerns haben. Des Weiteren können auch innerhalb der Divisionen, in einzelnen Ländern und Werken, Abstimmungsbedarfe hinsichtlich der Verantwortung auftreten. Hierbei müssen auch global entwickelte Kontrollmodelle an lokale (gesetzliche) Gegebenheiten angepasst werden. Insgesamt zeigt sich, dass das Modell die diversen in international agierenden Konzernen vorhandenen Elemente der Organisationsstruktur nur durch mehrere Modelle auf unterschiedlichen Ebenen abbilden kann. Ein auf globaler Ebene ausgeprägtes Modell könnte somit lokal als Vorlage dienen. Wie bereits schon für IT-bezogene und unternehmensweite Modelle angemerkt wurde, wird hierbei kein wesentlicher Unterschied hinsichtlich der Informationsobjekte und Beziehungen angenommen, sondern lediglich die Ausprägung der auf den lokalen GRC-Vorgaben basierenden Kontrollzielen und Kontrollen ändert sich. Vielmehr ist auch anhand der Praxisbeispiele zu vermuten, dass das hier entwickelte Modell sowohl auf Konzernebene, als auch auf Divisions-, Landesgesellschafts- bzw. Werksebene, bis hin zu einzelnen Abteilungen anwendbar ist. Strukturelemente stellen somit

kein eigenes Informationsobjekt dar, sondern müssen durch eine Kaskadierung des Modells berücksichtigt werden.

Der Begriff „Projekt“ hat in den Praxisbeispielen eine zweifache Bedeutung. Zum einen stellen die Praxisbeschreibungen oftmals Projekte zur Umsetzung von GRC-Vorgaben dar. Andererseits werden heutzutage in der Praxis viele Geschäftsinitiativen, insbesondere auch im IT-Bereich, durch Projekte umgesetzt und sind somit Gegenstand der Steuerung eines Governance-Ansatzes. Projekte werden somit im Rahmen des Modells als Ressourcen betrachtet und unter das entsprechende Informationsobjekt subsumiert.

Mehrere Praxisbeispiele stellen die Durchführung von Schulungen dar. Schulungen sind eine besondere Art von Kontrollen (siehe auch Anforderungskategorie „Faktoren des menschlichen Verhaltens“), die eine direkte Beziehung zu den Mitarbeitern, abgebildet durch das Informationsobjekt Rolle, haben.

Gerade der Begriff Steuerung ist in den Praxisbeschreibungen von herausragender Bedeutung. GRC soll demnach nicht nur eine Steuerung von GRC-Vorgaben und Risiken ermöglichen, sondern der im IT-Governance-Standard der ISO (2008) geforderte Zweiklang aus „Performance“ und „Conformance“ lässt sich auch in der Praxis als gewünschter Ansatz finden.

Ein weiterer wichtiger Begriff der ausgewerteten Praxisbeispiele ist Schwachstelle bzw. Schwäche, der im Sinne von Kontrollschwächen verwendet und im Wesentlichen durch Assessments festgestellt wird. Da dies bislang nicht berücksichtigt ist, wird Schwachstelle dem Modell als weiteres Informationsobjekt hinzugefügt. Insbesondere IT-Governance und Risikomanagement soll Entscheidungen unterstützen. Hierzu müssen neben den Informationen zur Performance auch In-

formationen zum GRC-Status zur Verfügung gestellt werden. Entscheidung wird dem Modell daher ebenfalls als Informationsobjekt hinzugefügt.

Ein weiterer Begriff, der im Zusammenhang mit dem SOX genannt wird, ist Konto. Dieser Begriff stellt einen Gegenstand von Kontrollen dar und kann im Modell daher ebenfalls unter das Informationsobjekt Ressource subsumiert werden.

Die Festlegung einer Meeting-Struktur, die als Entscheidungsgremien und Kommunikationsmittel dienen sollen, wird in der Praxis ebenfalls als wichtig erachtet. Die Begriffe Service Level Agreement und Service sind speziell für die IT-Governance von Relevanz. Sie stellen die Bedeutung von Services als Gegenstand von Kontrollen heraus. Außerdem wird hiermit die Bedeutung von Verträgen als eine Form von GRC-Vorgaben herausgestellt. Weitere Begriffe aus den Praxisbeispielen sind Anreiz, Änderungsanfrage und Datenschutzanfrage. Die zuletzt diskutierten Begriffe Meeting, Service, Anreiz, Änderungsanfrage und Datenschutzanfrage sind nicht spezifisch für GRC bzw. fokussieren im Falle der Datenschutzanfrage lediglich einen sehr speziellen Aspekt und werden lediglich in maximal zwei Praxisbeispielen thematisiert. Daher werden diese Begriffe nicht als weitere Informationsobjekte in das Modell aufgenommen.

Tab. 57: Weitere relevante Begriffe aus den Fallbeispielen, die nicht den Entitäten des entwickelten Modells zugeordnet werden konnten

Oberbegriff	Zugeordnete Begriffe aus den Fallbeispielen	Anz.	Berücksichtigung
Struktureinheit	Konzern/Geschäftsbereich/Werk, Werttreiber (1), Konzern/Teilkonzerngesellschaft (2), Geschäftseinheit (5), Business Unit (7), Konzern/Muttergesellschaft/Tochtergesellschaft (9), Ländergesellschaft (10), Konzern/Tochtergesellschaft/Geschäftsbereich (12), IT-Einheit (15), Konzern/Landesgesellschaften (16), Organisationstruktur/IT-Abteilung (17), Geschäftsfeld (19), Business Unit/Konzern/Land (21)	12	Möglichkeit einer lokalen Ausprägung des globalen Modells
Projekt	Projekt (1), Projekt (3), Projekt (5), Projekt (9), Projekt (10), IT-Projekt (12), IT-Projekt (14), Projekt (15), Projekt (17), Projekt (19), IT-(Projekt-)Portfolio/ITK-Großprojekt (20), Projekt (21)	12	Betrachtung von Projekten als Ressourcen im Rahmen des Modells
Schulung	Schulungs-, Qualifizierungs- und Kommunikationsmaßnahmen (1), Ausbildung/Training (2), Training (3), Schulungsmaßnahmen (12), Schulung (13), Schulung(skonzepte) (14), Schulung (15), Schulung (18), Training(sunterlagen) (21)	9	Schulung als besondere Art der Kontrolle mit direktem Bezug zum Mitarbeiter
Steuerung	Steuerung (5), Steuerung (7), Steuerung (11), Steuerung (12), Steuerung (13), Steuerung (14), Steuerung (16), Steuerung (19)	8	Steuerung von „Conformance“ und „Performance“ verwirklicht durch integrativen Ansatz des Modells
Schwachstelle	Kontrollschwäche (3), Schwachstelle (4), Kontrollschwäche (5), Schwachstelle (6), Schwachstelle (15), Defizit (von Kontrollen) (21)	6	hinzugefügt
Entscheidung	Entscheidung (11), Entscheidung (12), Entscheidung (13), Entscheidung (17), Entscheidung (20)	5	hinzugefügt
Service Level Agreement	Service-Level-Agreement (SLA) (15), Service Level Agreement (SLA)/Operational Level Agreement (OLA) (16), Service Level Agreement (17)	3	Als Teil von Verträgen berücksichtigt im IO GRC-Vorgabe.

Oberbegriff	Zugeordnete Begriffe aus den Fallbeispielen	Anz.	Berücksichtigung
Konto	Konto (3), Konto/Kontengruppe (4), Abschlussposition (4), rechnungslegungsrelevante Aussage/Financial Statement Assertion (4)	2	Als Gegenstand von Kontrollen im IO Ressource berücksichtigt.
Meeting	Meeting (12), Gremium (17)	2	Meeting-Struktur bzw. Entscheidungsgremien als Träger von Entscheidungen
Service	Service (16), IT-Service (17)	2	Berücksichtig als Ressource, da Gegenstand von Kontrollen.
Anreiz	Incentive (1)	1	Lediglich spezieller Aspekt und daher nicht berücksichtigt
Änderungsanfrage	Änderungsanfrage (16)	1	Lediglich spezieller Aspekt und daher nicht berücksichtigt
Datenschutzanfrage	Datenschutzanfrage (18)	1	Lediglich spezieller Aspekt und daher nicht berücksichtigt

5.4.3.3 Beziehungen der Informationsobjekte

Hinsichtlich der Beziehungen zwischen den Informationsobjekten muss angemerkt werden, dass diesen in den Praxisbeispielen allgemein wenig Beachtung entgegengebracht wird. Außerdem wird die Identifikation von Beziehungen durch die teilweise sehr ungenaue Terminologie, wobei unterschiedliche Begriffe auch innerhalb eines Fallbeispiels für gleiche Sachverhalte verwendet oder nur unzureichend gegeneinander abgegrenzt werden, erschwert. So wird mehrmals von Scoping gesprochen, jedoch nicht deutlich, ob sich dies auf GRC-Vorgaben, Kontrollziele, Kontrollen oder Risiken bezieht. Teilweise werden die Beziehungen selbst aber auch sehr allgemein gehalten. Bspw. sollen Abteilungen allgemein an den Unternehmenszielen ausgerichtet werden (Fröhlich und Glasner 2007c, S. 282). Lediglich das Praxisbeispiel von Tüllner (2012) diskutiert explizit die Integration von GRC, fokussiert hierbei jedoch nicht auf die Informationsobjekte, sondern auf die Or-

ganisationsstruktur und Berichterstattung. Die Unterscheidung zwischen den Informationsobjekten Kontrollziel und Kontrolle wird nicht in allen Praxisbeispielen explizit getroffen. Daher werden Kontrollen wie in Bamberg und Kaven (2006, S. 440) nicht immer den Kontrollzielen zugeordnet, sondern teilweise direkt den Risiken (Joachim 2006, S. 443, Ritzmann 2006, S. 467). Weiterhin werden die Beziehungen zwischen Kontrollen in Form von kompensierenden Kontrollen (Bamberg und Kaven 2006, S. 440; Gigerl et al. 2007) und die Beziehungen zwischen Kontrollen und Prozessen (Joachim 2006, S. 443) genannt. Die Beziehungen zwischen Kontrollen (Menzies 2006, S. 440, Gigerl et al. 2007), Kontrollen und Prozessen (Menzies 2006, S. 443), Risiken und Zielen (Kley 2011, S. 106) sowie Prozessen und Assessments (Just und Tami 2007, S. 236; FG07, S. 268) können als bestätigt angesehen werden.

5.5 Grenzen der Modellierung

Referenzmodelle werden in der Literatur mit zwei wesentlichen Charakteristika in Verbindung gebracht. Diese sind die Allgemeingültigkeit und der Empfehlungscharakter (siehe vom Brocke 2003, S. 31-32 und dort verwiesene Literatur). Bzgl. der Allgemeingültigkeit wird gefordert, dass Referenzmodelle, die bei der Entwicklung von Unternehmensmodellen angewendet werden sollen, für eine Klasse von Fällen anwendbar sein sollen. Von Brocke (2003, S. 31-32) folgert grundsätzlich, dass Allgemeingültigkeit nicht erreicht werden kann, sondern vielmehr von einer wahrgenommenen Adäquanz gesprochen werden sollte. Gerade in innovativen Kontexten definieren Referenzmodelle ihren Anwendungsbereich und somit auch Gültigkeitsbereich selbst. Das datenseitige Modell für das strategische GRC-Management stellt ein normatives Modell zur Weiterentwicklung bestehender Management-Ansätze im

Kontext von GRC dar. Es ist nicht das Ziel empirisch existierende Ansätze möglichste exakt abzubilden. Hinsichtlich des Empfehlungscharakters als wichtiges Merkmal von Referenzmodellen ist anzumerken, dass das hier dargestellte Modell explizit eine Vorbildfunktion einnehmen möchte. Jedoch weißt vom Brocke (2003, S. 32) auch hier darauf hin, dass der Empfehlungscharakter nur schwer überprüfbar ist und nicht festgelegt ist, welche Bedingungen hierfür erfüllt sein müssen, damit ein Referenzmodell als Empfehlung bezeichnet werden kann.

Es ist weiterhin anzumerken, dass das Modell lediglich ein Datenmodell darstellt, welches darüber hinaus Erweiterungsbedarf hinsichtlich der Attribute zu den Entitäten und der Kardinalitäten der Beziehungen zwischen den Entitäten (bspw. 1:1; 1:n; n:n) aufweist. Diese Erweiterungsbedarfe sind nicht relevant für die Erreichung der mit dem Modell verfolgten Forschungsziele, die insbesondere in der Explikation der relevanten Informationsobjekte und deren Beziehungen bestehen. Wie bereits ausgeführt wurde, wird das Datenmodell als Grundlage für die Entwicklung weiterer Modelle gesehen, die unter anderem den Prozess des GRC-Managements sowie die Aufbauorganisation berücksichtigen sollten.

Weitere spezifische Einschränkungen der hier vorgestellten Modellkonstruktion werden nachfolgend diskutiert. Die Entwicklung des datenseitigen Modells folgt bei der Auswertung der Entitäten und Beziehungen der bestehenden konzeptionellen Modelle sowie im Rahmen der Evaluierung einem qualitativen Forschungsansatz und leidet daher unter den bekannten Problemen qualitativer Forschung. Insbesondere wird qualitativen Methoden eine mangelnde Objektivität vorgeworfen. Wie bereits im Rahmen des Literaturreviews angesprochen, wurde daher der Forschungsprozess möglichst transparent dokumentiert und einzelne Entscheidungen des Forschers möglichst offengelegt (Brühl und Buch

2006, S. 37; Wrona 2006, S. 207). Außerdem wurde vorliegend einem strukturierten und etablierten Prozess zur Referenzmodellierung gefolgt, wobei auch die Entscheidungen zur Strukturierung des Forschungsprozesses bspw. hinsichtlich der verwendeten Wissensquellen, diskutiert und offengelegt wurden. Insgesamt ist somit darauf hinzuweisen, dass die vorgenommenen Interpretationen nicht vollkommen unabhängig von den Sichtweisen des Forschers sind. Da das Forschungsprojekt als Dissertationsvorhaben angelegt war, bestand zudem nicht die Möglichkeit, die Kodierung, die im Zuge der Evaluierung vorgenommen wurde, auch unabhängig von weiteren Forschern vornehmen zu lassen und somit die Intercoder-Reliabilität zu bestimmen (Atteslander 2010, S. 206). Es wäre sinnvoll dies in zukünftigen Forschungsvorhaben zu adressieren.

Bei der Herleitung der Entitäten des Modells aus den bestehenden Modellen gab es zwangsläufig Interpretationsspielräume. Auch ist darauf hinzuweisen, dass nicht alle Entitäten der Quellmodelle hinreichend definiert sind. Eine Zuordnung der Begriffe, auch wenn es sich hierbei um Synonyme bzw. Wortvarianten handelt, ohne Kenntnis der zugrundeliegenden Definition, ist inhärent mit der Möglichkeit von Fehlinterpretationen verbunden. Um möglichst alle relevanten Informationen für ein strategisches GRC-Management zu berücksichtigen, wurde außerdem versucht, alle Entitäten der Quellmodelle einem Informationsobjekt zuzuordnen. Insbesondere die „sonstigen zugeordneten Begriffe“ (siehe Tab. 57), welche als mögliche Attribute der Informationsobjekte des Modells interpretiert werden, sollten durch weitere Forschung abgesichert werden. Es ist nicht davon auszugehen, dass hierbei alle relevanten Attribute, insbesondere auch hinsichtlich einer technischen Umsetzung des Modells in ein Informationssystem, entdeckt wurden.

Auf die Schwierigkeit der Herleitung der Beziehungen aus den Quellmodellen wurde bereits eingegangen. Insbesondere besteht hierbei die Einschränkung, dass die Beziehungen teilweise indirekt, nach der Zuordnung der eigentlichen Begriffe des Quellmodells zu den neu gebildeten Entitäten des entwickelten Modells, erfolgt sind. Des Weiteren ist anzumerken, dass die Quellmodelle zwar ein weites inhaltliches Spektrum und hiermit alle GRC-Teildisziplinen abdecken, jedoch nur eingeschränkt eine Integration von GRC auf strategischer Ebene betrachten.

Mehrere Charakteristika der Modellierung lassen jedoch die Einschätzung zu, dass diese Einschränkungen keine zu großen Auswirkungen auf die Qualität des entwickelten Modells haben. Zum einen ist darauf zu verweisen, dass von einer guten Datenbasis gesprochen werden kann. So wurden insgesamt 35 bestehende Modelle berücksichtigt, die überwiegend selbst Gegenstand eines Forschungsvorhabens waren. Einzelne, mögliche Fehlinterpretationen hatten somit nur geringen Einfluss auf das endgültige Modell. Zum anderen wurde neben den bestehenden Modellen auch allgemeines Wissen, in Form der Anforderungen an das strategische GRC-Management berücksichtigt. Das Demonstrationsbeispiel zeigt die grundsätzliche Konsistenz des Modells. Im Rahmen der Evaluierung wurde darüber hinaus praxisbezogenes Datenmaterial, in Form von dokumentierten Praxisbeispielen, zur Absicherung des Konstruktionsprozesses herangezogen.

5.6 Zwischenfazit

In diesem Kapitel wurde ein fachkonzeptionelles Modell für ein strategisches GRC-Management entwickelt, das die konstituierenden Informationsobjekte und die strukturellen Zusammenhänge aufzeigt. Das Modell wurde unter Berücksichtigung existierender Modelle in der Literatur und allgemeiner Anforderungen an ein strategisches GRC-

Management entwickelt und mit Hilfe von Praxisbeispielen evaluiert. Das Modell soll explizit als Empfehlung verstanden werden und es ist zu hoffen, dass es im Sinne eines Referenzmodells wiederverwendet wird.

Es besteht naturgemäß weiterer Forschungsbedarf. Weitere Evaluierungen des Modells könnten insbesondere die Anwendung des Modells in einer realen Situation beinhalten. Darüber hinaus könnten weitere Wissensquellen, wie die zugrundeliegenden Informationsmodelle bestehender Softwarelösungen im Kontext von GRC sowie implizite bzw. explizit dokumentierte Informationsmodelle real existierender GRC-Management-Ansätze in der Unternehmenspraxis genutzt werden. Eine Befragung möglicher Anwender könnte zudem eine weitergehende Absicherung der Adäquanz des Modells liefern. Auf die Probleme dieser möglichen Forschungsansätze wurde bereits in Abschnitt 5.2.3 eingegangen.

Weiterer Forschungsbedarf besteht außerdem hinsichtlich der Anwendbarkeit des Modells in unterschiedlichen Branchen sowie IT-bezogenen und unternehmensweiten Anwendungsszenarien, wofür die Evaluierung nur erste Hinweise liefert. Ziel des hier dargestellten Forschungsvorhabens ist es, auf fachkonzeptioneller Ebene die Informationsstruktur eines strategischen und integrierten GRC-Managements herauszuarbeiten. Für eine Implementierung in einem Informationssystem ist eine weitere Detaillierung des Modells notwendig.

6 Schlussbetrachtungen

6.1 Zusammenfassung der Ergebnisse

In dieser Arbeit wurde der initialen Idee eines integrierten und strategisch ausgerichteten GRC-Managements gefolgt. Forschungsziel war die Grundlegung eines allgemeinen Verständnisses für ein strategisches GRC-Management. Zur Erreichung dieses Forschungsziels wurden konkret die im Folgenden wiederholten Forschungsfragen beantwortet.

- Welche Anforderungen sind an einen strategischen GRC-Management-Ansatz zu stellen?
- Welcher Forschungsstand existiert und welcher weitere Forschungsbedarf ist evident?
- Wie kann der Forschungsbedarf strukturiert werden?
- Welche Informationen sind für GRC relevant und welche Beziehungen existieren zwischen diesen Informationen?

Um die Forschungsfragen adäquat beantworten zu können, wurden in Kapitel 2 die Grundlagen zu Governance, Risiko- und Compliance-Management gelegt. Hierzu wurde eine Einführung in die GRC-Teildisziplinen gegeben und die Beziehungen der Einzelkonzepte diskutiert. Hierdurch konnte aufgezeigt werden, dass aufgrund von Überschneidungen, Berührungspunkten und Ergänzungsmöglichkeiten ein gemeinsames Management von GRC erforderlich ist. Hierauf aufbauend wurde in das Konzept des strategischen GRC-Managements eingeführt. Dieses betont neben dem Integrationsaspekt auch die strategische Bedeutung von GRC. Strategisches GRC-Management bezieht sich insbesondere auf eine umfassende Steuerung des GRC-Status, die Integration der Teilaspekte, die Ausrichtung der GRC-Aktivitäten an

den strategischen Zielen des Unternehmens sowie eine kontinuierliche Verbesserung von GRC und grenzt sich von der operativen Normerfüllung und Durchführung der risikosteuernden Maßnahmen ab.

Die vorliegende Forschungsarbeit ist das erste Forschungsvorhaben, das auf der Grundlage eines fundierten Forschungsprozesses, Anforderungen an einen integrierten und strategisch ausgerichteten GRC-Management-Ansatz formuliert. Auf Basis einer systematischen und umfassenden Literaturrecherche, die 282 Publikationen berücksichtigt, werden in Kapitel 3 unter Rückgriff auf die qualitative Inhaltsanalyse Anforderungskategorien hergeleitet. Demnach sind für ein strategisches GRC-Management neben der strategischen Ausrichtung und Integration, die Geschäftsprozessorientierung, die Berücksichtigung weiterer Management-Systeme, die Automatisierung, die Herausforderung der Flexibilität sowie die Berücksichtigung menschlicher Faktoren von Bedeutung. Auf Grundlage zuvor identifizierter relevanter theoretischer Perspektiven wurde eine argumentativ-deduktive Analyse der Anforderungskategorien vorgenommen, die in der Herleitung von insgesamt elf konkreten Anforderungen für das strategische GRC-Management resultierte.

Die Anforderungen werden im weiteren Forschungsprozess auf vielfältige Weise aufgegriffen. Zuerst wurde der Forschungsstand systematisch aufgearbeitet. Hierbei wurden zum einen bestehende GRC-bezogene Management-Ansätze anhand der Anforderungen bewertet. Hierdurch konnte gezeigt werden, dass bislang kein adäquater Ansatz, der alle Anforderungen erfüllen würde, für das strategische GRC-Management existiert. Zum anderen wurde der Forschungsstand zu den Anforderungskategorien dargestellt und auf dieser Grundlage der weitere Forschungsbedarf abgeleitet. Die Beantwortung der aufgezeigten Forschungsbedarfe, die im Rahmen der Forschungsagenda auch

hinsichtlich der Bearbeitungsreihenfolge und Bedeutung systematisiert wurden, kann zur Entwicklung eines geeigneten GRC-Management-Ansatzes führen.

Da es sich bei den Anforderungen und Forschungsbedarfen nicht um empirisch beobachtbare Wahrheiten handelt, sondern der Idee gestaltungsorientierter Forschung folgend um einen Gestaltungsvorschlag, der zukünftig zur Weiterentwicklung von GRC-bezogenen Management-Systemen dienen soll, wurde eine Delphi-Studie eingesetzt, die durch mehrfache Befragung von GRC-Experten, die Evaluierung und Priorisierung der Anforderungen und Forschungsbedarfe ermöglichte (siehe Kapitel 4). Durch diese Studie konnte die Struktur der Anforderungskategorien bestätigt werden. Die Anforderungen wurden teilweise umstrukturiert und weiter konkretisiert, wobei insbesondere jede Anforderung nur einen Aspekt abdecken sollte. Dies führt zu einer finalen Liste von insgesamt 19 Anforderungen. Die Forschungsbedarfe wurden ebenfalls leicht verändert. Es ist davon auszugehen, dass hierdurch die Verständlichkeit der gemachten Vorschläge ebenso wie die Akzeptanz in der Forschungsgemeinschaft und das Evidenzniveau gesteigert werden konnte.

Abschließend wurde der Fokus auf die für GRC relevanten Informationen gelegt, die für die Entwicklung von Informationssystemen für das strategische GRC-Management von besonderer Bedeutung sind und insbesondere eine tiefere Analyse der Integrationsaspekte von GRC ermöglichen (siehe Abschnitt 5). Im Rahmen der Entwicklung eines datenseitigen Modells für das strategische GRC-Management, wurde ein erster Schritt zu einem einheitlichen Begriffsverständnis für ein strategisches GRC-Management gemacht. Das Modell ordnet wichtige Begriffe, welche die für GRC relevanten Informationen darstellen, und setzt sie in Beziehung. Hierfür werden einerseits bestehende Modelle

ausgewertet und andererseits die strategischen GRC-Anforderungen eingesetzt. Neben der Demonstration des Modells anhand eines fiktiven Beispiels erfolgte eine Evaluierung durch einen Abgleich der relevanten Informationen und Beziehungen mit in der Literatur existierenden Fallbeispielen. Insgesamt kann somit das gesetzte Forschungsziel als erreicht angesehen werden.

6.2 Kritische Würdigung der Arbeit

Wie jedes Forschungsvorhaben weist auch die vorliegende Forschungsarbeit Grenzen auf. Diese Grenzen wurden jeweils in den einzelnen Kapiteln diskutiert, wobei sowohl methodische Defizite als auch Ergänzungsbedarf aufgezeigt wurden. Im Allgemeinen ist zudem anzumerken, dass die vorliegende Arbeit generische Ergebnisse, in dem Sinne erzielt, dass diese eine Anwendbarkeit unabhängig von Branche oder Unternehmensgröße haben sollen. Die verfolgte Idee ist, dass die Forschungsergebnisse unter Berücksichtigung situativer Aspekte[97] an die jeweilige Unternehmenssituation anzupassen sind. Ein solcher allgemeiner Ansatz wird ebenso in gängigen Best Practice-Rahmenwerken wie COBIT (ITGI 2007) verfolgt. Trotzdem ist anzunehmen, dass Unterschiede in der Ausgestaltung des GRC-Managements bestehen können. Große, international tätige Unternehmen müssen durch ihre Ländergesellschaften unterschiedliche lokale Normen berücksichtigen und werden wohl andere Strukturen und Prozesse aufbauen als kleinere, nur lokal tätige Unternehmen. Auch könnte ein Unterschied zwischen stark regulierten Branchen, wie dem Finanzsektor und eher schwach regulierten Branchen bestehen. Des Weiteren könnten Unter-

[97] Siehe hierzu auch die Ausführungen zur Kontingenztheorie in Abschnitt 3.3.1.

schiede durch die Art der Regulierung in der produzierenden Industrie wie der Pharmabranche, die eher auf Qualitätsmanagement abzielt und Dienstleistungsunternehmen, wie auch der Finanzbranche, bestehen.

An dieser Stelle soll nochmal darauf hingewiesen werden, dass die Forschungsarbeit im Wesentlichen einem qualitativen Forschungsansatz folgt, der mit den bekannten Problemen qualitativer Forschung verbunden ist. Insbesondere ist in diesem Zusammenhang darauf hinzuweisen, dass die Forschungsergebnisse nicht vollständig unabhängig vom Standpunkt, Hintergrund und Einstellungen des Autors sind.

Die vorliegende Forschungsarbeit erzielt trotzdem wissenschaftlich belastbare Ergebnisse. Hierzu tragen insbesondere die im Folgenden dargestellten Richtlinien bei, die im gesamten Forschungsprozess stringent angewendet wurden. Erstens basiert der Forschungsprozess auf dem etablierten Prozess gestaltungsorientierter Forschung (Hevner et al. 2004; Hevner und Chatterjee 2010; March und Smith 1995; Österle et al. 2010), der im Rahmen dieser Forschungsarbeit zur Erreichung der Forschungsziele zweifach durchlaufen wurde.[98] Insbesondere wurde zur Erhöhung der Qualität der Forschungsergebnisse eine unabhängige Konstruktion und Evaluierung vorgenommen. Des Weiteren wurden etablierte Forschungsmethoden für die einzelnen Forschungsschritte angewendet. Die einzelnen Forschungsmethoden und Forschungsschritte sind jeweils in den einzelnen Kapiteln transparent dokumentiert, was die Nachvollziehbarkeit der Forschungsergebnisse erhöht. Außerdem findet eine Triangulation (Flick et al. 2008, S, 309; Brühl und Buch 2006, S. 3) von unterschiedlichen Forschungsmethoden und Datenquellen statt. So basieren die Anforderungen und Forschungsbedarfe

[98] Siehe Abschnitt 1.4.

sowohl auf einem systematischen Literaturreview und der Anwendung von einschlägigen Theorien als auch auf der Befragung von GRC-Experten im Rahmen einer mehrstufigen Delphi-Studie.

An gestaltungsorientierte Forschung werden zudem die folgenden Prinzipien gestellt, an welchen die vorliegende Arbeit kritisch gewürdigt werden soll (Österle et al. 2010, S. 5).

- „**Abstraktion:** Ein Artefakt muss auf eine Klasse von Problemen anwendbar sein.
- **Originalität**: Ein Artefakt muss einen innovativen Beitrag zum publizierten Wissensstand leisten.
- **Begründung:** Ein Artefakt muss nachvollziehbar begründet werden und validierbar sein.
- **Nutzen:** Ein Artefakt muss heute oder in Zukunft einen Nutzen für die Anspruchsgruppen erzeugen können." (Österle et al. 2010, S. 5)

Eine Abstraktion wird durch die vorliegende Arbeit in mehrfacher Hinsicht vorgenommen. So sind die Ergebnisse weder auf bestimme Branchen noch auf bestimmte Unternehmensgrößen beschränkt. Des Weiteren sind die Ergebnisse sowohl für den unternehmensweiten als auch den IT-Kontext relevant. Außerdem wird bewusst von bestimmen Compliance-Vorgaben oder Risikobereichen abstrahiert.

Hinsichtlich der Originalität ist anzumerken, dass die GRC-Forschung sich noch in einem frühen Stadium befindet. Die Literatursuche erfasst die existierenden Arbeiten, die im Kontext des GRC-Managements

relevant sind. Die identifizierten Anforderungskategorien, Anforderungen sowie die Forschungsagenda wurden in dieser Form noch in keiner anderen Arbeit betrachtet.[99] Das datenseitige Modell berücksichtigt im Gegensatz zu ähnlichen in der Literatur existierenden Modellen[100] alle hergeleiteten Anforderungen an das strategische GRC-Management und basiert auf einer systematischen Auswertung der Informationsobjekte und Beziehungen vorhandener Modelle. Demnach ist auch hier von einem innovativen Artefakt auszugehen.

Das Prinzip Begründung wird dadurch erfüllt, dass alle Forschungsschritte auf einer zuvor festgelegten Forschungsmethode basieren. In diesem Zusammenhang sei auf die zuvor in diesem Abschnitt gemachten Erläuterungen hingewiesen. Auf den Nutzen für die Forschung und Praxis wird in den nachfolgenden Abschnitten eingegangen.

6.3 Nutzen für Forschung und Praxis

6.3.1 Nutzen für die Forschung

Diese Arbeit versucht einen ganzheitlichen Zugang für das strategische GRC-Management zu ermöglichen. Im Gegensatz zu anderen wissenschaftlichen Arbeiten, die primär den Integrationsaspekt von GRC betrachten, versucht diese Arbeit das Blickfeld auf die verschiedenen Anforderungsbereiche zu erweitern, die für das GRC-Management relevant sind. Durch diesen umfassenden Forschungsansatz trägt die vorliegende Arbeit wesentlich dazu bei, das Themengebiet zu erfassen,

[99] Siehe Abschnitt 3.2 zur Diskussion von existierenden Literaturreviews im Kontext von GRC.

[100] Siehe Abschnitt 5.3.1.1 zur Diskussion existierdender konzeptioneller Modelle im Kontext von GRC.

einzugrenzen, zu strukturieren und somit für weitere Forschungsanstrengungen zugänglich zu machen. Der Nutzen für die Forschung ergibt sich in allen Bereichen der vorliegenden Forschungsarbeit. Hierzu gehören die Anforderungen bzw. Anforderungskategorien, die Diskussion des Forschungsstandes zu den Anforderungskategorien und die hiermit verbundene Entwicklung der Forschungsagenda sowie das datenseitige Modell für ein strategisches GRC-Management.

Die Anforderungskategorien und Anforderungen ermöglichen eine erste Strukturierung und Eingrenzung des Themengebietes strategisches GRC-Management. Die Anforderungskategorien sowie deren Unterkategorien können aus Sicht der Forschung herangezogen werden, um Bereiche zu identifizieren, die von Relevanz für GRC sind. Der Idee einer Designtheorie (Fischer et al. 2010) folgend, die aus Anforderungen und Designkomponenten besteht, ermöglichen die Anforderungen eine systematische Entwicklung von Designkomponenten für das strategische GRC-Management. Durch die Offenlegung der Anforderungen können Designentscheidungen transparenter in zukünftigen Forschungsvorhaben begründet und hinsichtlich der Unterstützung der Anforderungen evaluiert werden.

In diesem Zusammenhang ist auch darauf hinzuweisen, dass aufgrund des frühen Stadiums der GRC-Forschung, diese Arbeit vorwiegend beschreibenden und erklärenden Charakter hat.[101] In Anlehnung an Cushing (1990) stellen die Anforderungskategorien und Anforderungen sowie das datenseitige Modell ein Rahmenwerk dar, welches es Forschern ermöglicht, die komplexen Zusammenhänge strukturiert zu erfassen. Diese Forschungsarbeit suggeriert verschiedene kausale Zu-

[101] Siehe die in Abschnitt 3.3.1 angesprochenen Theorietypen nach Gregor (2006, S. 620).

sammenhänge, die in den einzelnen Anforderungen enthalten sind. So wird bspw. angenommen, dass eine Integration über die GRC-Disziplinen sowie mehrere GRC-Vorgaben und Risikobereiche sinnvoll ist. Hierdurch wird zumindest ein Zusammenhang von Integration und GRC-Kosten angenommen. Die Anforderungen stellen somit für weitere Forschung einen Startpunkt zur Explikation und Operationalisierung der kausalen Zusammenhänge von GRC dar, die zu testbaren Hypothesen führen könnten. Solche Hypothesen ermöglichen sowohl quantitativ-empirische Primäruntersuchungen als auch strukturierte Meta-Reviews von vorliegenden empirischen Arbeiten. Wie in den vorliegenden Reviews von empirischen Arbeiten (Abraham 2011; Aurigemma und Panko 2012; Lebek et al. 2013; Milicevic und Goeken 2012; Milicevic und Goeken 2013a; Milicevic und Goeken 2013b) zum Compliance-Verhalten zu Recht herausgestellt wird, haben solche Arbeiten einen hohen Nutzen für die gestaltungsorientierte GRC-Forschung. Bspw. sind adäquate methodische Ansätze zur strategischen Ausrichtung von GRC nur dann zu erwarten, wenn ein tiefgreifendes Verständnis der GRC-spezifischen Faktoren und kausalen Zusammenhänge, die den Unternehmenserfolg beeinflussen, verfügbar ist. Insgesamt befinden sich die hier zu den Anforderungen vorgenommenen Analysen noch auf einem recht hohen Abstraktionsniveau. Dies ist in Übereinstimmung mit dem hier verfolgten Forschungsziel, welches das GRC-Management als übergreifendes Forschungsfeld im Blick hat. Dies bedeutet für die Forschung, dass hinsichtlich der Anforderungskategorien noch weitere detaillierte Analysen denkbar sind. Die Diskussion des Forschungsstandes kann in weiteren Forschungsvorhaben als Referenz dienen, um einen schnellen Einstieg in den Forschungsbereich zu erlangen und eigene Forschungsvorhaben in den Gesamtkontext des GRC-Managements einzuordnen.

Das datenseitige Modell für ein strategisches GRC-Management geht noch einen Schritt weiter. Durch die gegenseitige Zuordnung von bestehenden Begriffen wird eine Vereinheitlichung der GRC-bezogenen Terminologie ermöglicht. Dies ist eine wichtige Grundlage für jegliche weitere Forschung im Bereich GRC. Die Explikation der Beziehungen zwischen den für GRC relevanten Informationen liefert insbesondere ein tieferes Verständnis der relevanten Aspekte von Integration und strategischer Ausrichtung, was die Entwicklung von spezifischen Methoden für diese Aspekte unterstützt. Das datenseitige Modell ist zudem Ausgangspunkt für die Entwicklung GRC-bezogener Informationssysteme und eines GRC-Management-Ansatzes. Eine systematische Erweiterung des datenseitigen Modells auch um prozessuale Aspekte könnte insgesamt zu einem Referenzmodell für das strategische GRC-Management führen.

Die Forschungsagenda zeigt den relevanten Forschungsbedarf hinsichtlich der Entwicklung eines strategischen GRC-Management-Ansatzes auf. Durch die Strukturierung der Forschungsbedarfe innerhalb der Forschungsagenda sowie die Zurverfügungstellung weiterer relevanter Informationen, wie mögliche Theorien, können Forscher wertvolle Hinweise für eigene Forschungsvorhaben erhalten. Die Forschungsagenda versteht sich somit als Aufruf zu weiterer Forschung, die zu einer Entwicklung eines umfassenden Ansatzes für das strategische GRC-Management führen soll. Die Priorisierung der Forschungsbedarfe ermöglicht der Forschungsgemeinschaft knappe Ressourcen auf besonders bedeutende Forschungsbedarfe, die einen hohen Nutzen versprechen, zu konzentrieren.

Die hier erzielten Forschungsergebnisse können auch als Referenz dienen um Einschränkungen des Gegenstandsbereichs bspw. auf bestimmte hochregulierte Industrien wie die Finanzdienstleistungsbranche

oder auf bestimmte GRC-Bereiche wie Vorgaben zum Qualitätsmanagement oder zur Finanzberichtserstattung vorzunehmen. Auch könnte der Fokus auf IT-Abteilungen und deren Prozesse beschränkt werden.

6.3.2 Nutzen für die Praxis

Für die Praxis ergibt sich aus den Anforderungen sowie dem datenseitigen Modell ein ähnlicher Nutzen wie für die Forschung, da auch die Praxis aus der Strukturierung und Abgrenzung des Themengebiets sowie einer Vereinheitlichung der Terminologie und einem Aufzeigen der Zusammenhänge insbesondere hinsichtlich strategischer Ausrichtung und Integration profitiert.

Die Anforderungen dienen zudem zur Bewertung und Weiterentwicklung von existierenden GRC-bezogenen Management-Systemen sowie zur Entwicklung von neuen GRC-Management-Systemen in der Unternehmenspraxis. Die Anforderungen zeigen hierbei die relevanten Aspekte für solche Management-Systeme auf. Sie dienen somit zur Aufdeckung von Lücken in den bestehenden Ansätzen. Die Priorisierung durch GRC-Experten im Rahmen der Delphi-Studie ermöglicht zudem eine Konzentration auf besonderes wichtige Bereiche, die möglicherweise zuerst betrachtet werden könnten und das größte Verbesserungspotential versprechen. In diesem Zusammenhang könnten die Anforderungen unter Berücksichtigung unternehmensspezifischer Aspekte zu einer Art Checkliste weiterentwickelt werden. Ein solcher Ansatz könnte auch von Beratungsunternehmen aufgegriffen werden.

Jede Anforderungskategorie hat Anknüpfungspunkte für die Unternehmenspraxis. Im Rahmen der strategischen Ausrichtung sollten Unternehmen den Zusammenhang zwischen dem GRC-Ansatz und der Unternehmensstrategie sowie den strategischen Zielen untersuchen.

Aufgrund der ad-hoc umgesetzten und isoliert auf einzelne GRC-Vorgaben abzielenden Initiativen, die in der Praxis vorherrschen, kann nicht immer davon ausgegangen werden, dass die Ansätze systematisch aus den strategischen Zielen entwickelt wurden. Des Weiteren legt diese Anforderungskategorie den Fokus auf operative Nutzenpotentiale nahe, die gezielt verfolgt werden sollten. In diesem Zusammenhang würde sich eine schrittweise Weiterentwicklung des GRC-Ansatzes anbieten, die für jeden Schritt einen definierten Business Case basierend auf den Nutzenpotentialen aufweisen. Die Ergebnisse zur Anforderungskategorie Integration können von Unternehmen konkret aufgegriffen werden um eigene Schwächen zu analysieren. Doppelarbeiten und Lücken sollten vermieden und Synergien genutzt werden. Existierende Arbeiten, wie die von Menzies (2006) bieten an dieser Stelle detaillierte Empfehlungen für mögliche Projektvorgehensweisen. Die Geschäftsprozessorientierung zeigt auf, dass die seit längerem eingesetzten Methoden des GPM auch für das GRC-Management genutzt werden können. Unternehmen sollten in diesem Zusammenhang die eingesetzten Methoden und Informationssysteme bspw. zur Prozessmodellierung auf eine Erweiterung um GRC-Aspekte überprüfen. Die Kategorie Management-Systeme legt es Unternehmen nahe, die Zusammenhänge zwischen einer GRC-Initiative und etablierten Management-Systemen wie der Internen Revision und dem Qualitätsmanagement zu untersuchen. Die Verantwortungs- und Aufgabenverteilung sollte übergreifend abgestimmt werden. Die Forschungsergebnisse zur Anforderungskategorie Automatisierung ermöglichen es Unternehmen zu verstehen, für welche Kontrolltypen eine Automatisierung sinnvoll ist und welche Kostenvorteile grundsätzlich möglich sind. Gleichzeitig werden Methoden aufgezeigt, die innerhalb des Unternehmens eine Automatisierung unterstützen können. Im Rahmen der Kategorie Flexibilität werden verschiedene Themen, die bislang eher unabhängig betrachtet wor-

den sind, wie vertrauensbasierte Organisationsgestaltung, SOA und Cloud-Computing in den allgemeinen Zielkonflikt zwischen Flexibilität und GRC-Erfordernissen eingeordnet. Unternehmen wird hiermit ein allgemeiner Zugang zu der Problematik ermöglicht. Außerdem werden existierende Ansätze aufgezeigt, die insbesondere durch Rückgriff auf situationsspezifische Aspekte eine Auflösung dieses Konflikts ermöglichen. Im Rahmen der Anforderungskategorie menschliche Faktoren werden Unternehmen die Einflussfaktoren aufgezeigt, die bei der Ausgestaltung von Einflussmaßnahmen auf das Compliance-Verhalten berücksichtigt werden sollten. Unternehmen können hiermit die eigenen Maßnahmen auf Vollständigkeit prüfen. Die vorliegenden Meta-Reviews von empirischen Arbeiten (Abraham 2011; Aurigemma und Panko 2012; Lebek et al. 2013; Milicevic und Goeken 2012; Milicevic und Goeken 2013a; Milicevic und Goeken 2013b) zeigen, welche Faktoren einen signifikanten Einfluss auf das Compliance-Verhalten haben und somit in der Praxis besonders berücksichtigt werden sollten und zu welchen Faktoren noch keine eindeutigen Ergebnisse vorliegen.

Das datenseitige Modell ermöglicht ebenso wie die Anforderungen eine Strukturierung des Themengebiets. Es zeigt ähnlich wie die Anforderungen Lücken bzgl. der Bereitstellung von Informationen für das strategische GRC-Management in existierenden Management-Systemen auf. Es ermöglicht darüber hinaus die Auswahl und Entwicklung bzw. Weiterentwicklung von GRC-bezogenen Informationssystemen in der Praxis.

6.4 Ausblick

Die Entwicklungspotentiale im Kontext des strategischen GRC-Managements beziehen sich auf unterschiedliche Aspekte. Im Folgenden sollen die Entwicklungspotentiale hinsichtlich der Entwicklung

eines strategischen GRC-Management-Ansatzes, bzgl. der eigenen Forschungsergebnisse in den Bereichen Anforderungen, Forschungsagenda und datenseitiges Modell für ein strategisches GRC-Management sowie im Allgemeinen Entwicklungspotentiale von GRC in Forschung und Praxis diskutiert werden.

Hinsichtlich der Entwicklung eines strategischen GRC-Management-Ansatzes zeigt die entwickelte Forschungsagenda detailliert auf, welcher Forschungsbedarf existiert und strukturiert diesen insbesondere im Hinblick auf die Bearbeitungsreihenfolge und Bedeutung. Entwicklungspotentiale hinsichtlich der eigenen Forschungsergebnisse in den Bereichen Anforderungen, Forschungsagenda, Delphi-Studie zu Anforderungen und Forschungsbedarfen und datenseitiges Modell wurden in den einzelnen Kapiteln betrachtet. An dieser Stelle soll nochmal auf die Notwendigkeit der Weiterentwicklung der bisherigen Forschungsergebnisse hingewiesen werden. Es ist davon auszugehen, dass die Forschungsergebnisse zwar eine solide Grundlage zur Verfügung stellen, diese jedoch kontinuierlich weiterentwickelt werden sollten. So könnten zukünftig auch neue Anforderungen relevant werden, die zu ergänzen wären.

Allgemein zeigt die vorliegende Arbeit, dass im Kontext des Themenkomplexes GRC eine Vielzahl von interessanten Fragestellungen existieren, wobei bereits erste integrierte GRC-Ansätze vorliegen. Hervorzuheben sind die Publikation von Racz et al. (2011b; 2010a; 2011a; 2011c; 2010b; 2010c; 2010d) sowie die hierauf basierende Dissertation von Racz (2011). Obwohl mehrere Forscher die strategische Bedeutung von GRC betonen, zeichnet sich die vorliegende Forschungsarbeit insbesondere durch die Betonung von Integration und strategischer Ausrichtung von GRC aus. Strategisches GRC-Management ist ein vielversprechender Ansatz um Nutzenpotentiale aus GRC zu verwirkli-

chen. Entwicklungspotentiale ergeben sich jedoch nicht nur hinsichtlich der Integration und strategischen Ausrichtung. Vielmehr zeigen die Anforderungen detailliert die vielfältigen relevanten Aspekte des Themenkomplexes GRC auf. Die GRC-Forschung steht, obwohl sie auf einer längeren Forschungstradition in den GRC-Teilbereichen aufbauen kann, noch am Anfang. Die Entwicklung eines Management-Ansatzes von GRC wird Anstrengungen von mehreren Forschern erfordern. Auch erscheint die Entwicklung von Software, die das strategische GRC-Management unterstützt, Entwicklungspotential zu haben. Bislang ist das Themengebiet auch informationstechnisch von Insellösungen geprägt. Es bleibt abzuwarten, ob zukünftig Informationssysteme entwickelt werden, die ähnlich wie ERP-Systeme für die Kernprozesse des Unternehmens, integrierte Prozesse und Informationen für GRC zur Verfügung stellen. Die vorliegende Forschungsarbeit versucht die Grundlegung eines allgemeinen Verständnisses für das strategische GRC-Management. Dies soll eine Einordnung von Forschungsarbeiten zu Detailfragen, die auch weiterhin notwendig sein werden, ermöglichen. Ziel ist es, die vielfältigen erforderlichen Methoden und Werkzeuge in einem Management-Rahmenwerk für GRC zu integrieren, ähnlich wie auch das GPM vielfältige Methoden und Werkzeuge in einem Management-Rahmenwerk zu integrieren versucht.

Für die Praxis ist weitere Forschung zum strategischen GRC-Management unerlässlich. Zum einen wird die Komplexität hinsichtlich der GRC-Vorgaben und Risiken, insbesondere in großen international agierenden Unternehmen mit vielen Landesgesellschaften, weiter zunehmen. Zum anderen entstehen schon heute hohe Kosten für die Erfüllung von GRC-Vorgaben. Für Unternehmen ist es daher unerlässlich ihre GRC-Management-Systeme kontinuierlich weiterzuentwickeln

um Komplexität und Kosten zu beherrschen und mögliche Nutzenpotentiale aus GRC auszuschöpfen.

Anhang

A Anhang zu Kapitel 3 Anforderungen und Forschungsagenda für das strategische GRC-Management

Tab. 58: Auswertung der in der GRC-Literatur angewendeten Forschungsmethoden

Methodische Vorgehensweise
Um die in der GRC-Literatur angewandten Methoden systematisch auszuwerten, ist ein einheitliches Verständnis der für Betriebswirtschaft, Wirtschaftsinformatik und Information Systems relevanten Forschungsmethoden notwendig. Hier soll auf die Strukturierung von Forschungsmethoden der Wirtschaftsinformatik nach Wilde und Hess (2007) zurückgegriffen werden. In Betriebswirtschaft und Information Systems dominieren empirisch-quantitative Forschungsmethoden (Schwaiger und Meyer 2009; Wilde und Hess 2007), die auch von der oben genannten Strukturierung erfasst werden. Es ist daher auch von einer Anwendbarkeit dieser Strukturierung für Forschungsarbeiten aus Betriebswirtschaft und Information Systems auszugehen. Ergänzt wird diese lediglich durch das Literaturreview sowie den Forschungsansatz „Mixed-Method", der eine Kombination qualitativer und quantitativer Forschungsmethoden beinhaltet (Tashakkori und Teddlie 2003), um der steigenden Bedeutung dieser Methoden gerecht zu werden. Zur Datenanalyse soll ebenso wie von Wilde und Hess (2007) auf eine klassifizierende Frequenzanalyse als Form der quantitativen Inhaltsanalyse (Schnell et al. 2005, S. 407-408) zurückgegriffen werden. Zu beachten ist, dass in gestaltungsorientierten Arbeiten oftmals unterschiedliche Methoden für Entwurf und Evaluierung der Artefakte angewendet werden. Bei Beiträgen, denen mehrere Methoden eindeutig zugeordnet werden können, wird diejenige Methode für die Analyse aufgenommen, mit welcher die Kernergebnisse erzielt wurden. Zur Identifikation der verwendeten Forschungsmethode wurde zuerst Titel, Abstract und Einleitung gelesen. Konnte hieraus die verwendete Forschungsmethode nicht entnommen werden, wurden weitere Kapitel herangezogen. Es wurde hierbei grundsätzlich nicht die stringente Anwendung der jeweiligen Forschungsmethode überprüft. Dies sollte durch den Review-Prozess sichergestellt sein.

Forschungsmethode	Häufigkeit	Prozent
Formal/konzeptionell/argumentativ-deduktive Analyse	134	55,60%
Simulation	0	0,00%
Referenzmodellierung	6	2,49%
Aktionsforschung	3	1,24%
Prototyping	0	0,00%
Ethnographie	0	0,00%
Fallstudie	21	8,71%
Grounded Theory	4	1,66%
Qualitative Querschnittsanalyse	14	5,81%
Quantitative Querschnittsanalyse	33	13,69%
Labor-/Feldexperiment	4	1,66%
Multi-Method	8	3,32%
Literatur-Review	14	5,81%

Tab. 59: Überblick über Literaturreviews aus Teilbereichen von GRC (1 von 5)

Zitation	Abdullah et al. 2009
Forschungsziel(e)	Der Beitrag verfolgt als Ziel die Aufarbeitung des gegenwärtigen Forschungsstandes zum Compliance-Management mit Bezug zu Informationssystemen. Dieser soll zusammen mit Experteninterviews zu gegenwärtigen Herausforderungen im Compliance-Management die Entwicklung einer Forschungsagenda ermöglichen.
Berücksichtigte Publikationen und Publikationsorgane	Insgesamt wurden 46 Beiträge aus den Jahren 2001-2008 berücksichtigt, wobei die folgenden Zeitschriften ausgewertet wurden. Business Process Management Journal, Communication of the Association for Information Systems, Communication of the Association for Computing Machinery, European Journal of Information Systems, Journal of Information and Management, Journal of Information Systems Research, Journal of the Association for Information Systems, MIS Quarterly, Journal of Information Systems - Sarasota, Information Systems Frontier, Information Systems Journal - Blackwell, Information Systems – Elsevier und Journal of Management Information Systems.
Forschungsergebnis	Compliance-Management ist ein wachsender Forschungszweig in der Information Systems-Forschung. Die Beiträge fokussieren derzeit auf gesetzliche Anforderungen (bspw. HIPAA, SOX) in den Bereichen Auditing, Healthcare und Finance. Regional liegt der Schwerpunkt der Beiträge auf Nordamerika, wobei die Forschungsansätze noch überwiegend explorativ sind. Gestaltungsorientierte Arbeiten umfassen sowohl präventive als auch detektive Ansätze.
Zitation	Abraham 2011
Forschungsziel(e)	Das Forschungspapier analysiert die Literatur zum Informationssicherheitsverhalten hinsichtlich der Faktoren, die das Informationssicherheitsverhalten in organisatorischen Kontexten beeinflussen.
Berücksichtigte Publikationen und Publikationsorgane	Es wurde den Empfehlungen von Webster und Watson (2002) folgend eine Datenbanksuche mit relevanten Schlagwörtern zum Informationssicherheitsverhalten sowie eine Vorwärts- und Rückwärtssuche durchgeführt. Insgesamt wurden hierdurch 84 relevante Veröffentlichungen identifiziert, zu welchen Zeitschriftenbeiträge sowie Konferenzpublikationen und Bücher gehören. Der Review wurde außerdem anhand der folgenden Themen strukturiert: Forschungsdisziplinen und Theorien, Faktoren, welche das Informationssicherheitsverhalten beeinflussen und Sicherheitstechnologie, die für das Verhalten relevant ist.
Forschungsergebnis	Die Autoren identifizieren die folgenden insgesamt 18 Themen, die für das Informationssicherheitsverhalten relevant sind (Oberkategorien jeweils für die vorgenannten Themen in Klammern): Security Policies, Communication Practices, Content of Awareness Efforts (The Body of Knowledge), Management Influences, Peer Influences, Deterrence Efforts, Rewards, Employee Participation (What they see in Practice in the Organization), User's Knowledge, Self-Efficacy (User's Security Common Sense and Decision Making Skills), Attitudes, Beliefs (The User's Personal Values and standard of conduct), Psychological ownership, Organizational commitment, Trust, Procedural justice (The user's psychological contract with employer), Ease of use, Effectiveness of security technology (Effort required for compliance and temptation not to comply).

Tab. 60: Überblick über Literaturreviews aus Teilbereichen von GRC (2 von 5)

Zitation	Aurigemma und Panko 2012
Forschungsziel(e)	Entwicklung eines vereinheitlichten Rahmenwerks für das Compliance-Verhalten bzgl. Informationssicherheitsanforderungen
Berücksichtigte Publikationen und Publikationsorgane	Es werden nur empirische Arbeiten berücksichtigt, die in führenden und begutachteten Journalen oder Konferenz-Proceedings veröffentlicht wurden. Hierzu gehören MIS Quarterly, Information Systems Research, Decision Support Systems, European Journal of Information Systems.
Forschungsergebnis	Es wird ein Rahmenwerk für das Compliance-Verhalten in Bezug auf Informationssicherheit entwickelt. Dieses basiert auf der Theorie des geplanten Verhaltens und beinhaltet die folgenden Hauptkomponenten: Sanction Effects, Threat Assessment, Cost-Benefit-Analysis, Subjective Norm, Attitude, Perceived Behavioral Control, Organization Security Commitment, Behavioral Intent, Actual Behavior.
Zitation	El Kharbili et al. 2008a
Forschungsziel(e)	Der gegenwärtige Status sowie zukünftige Trends von Compliance im Kontext des GPM sollen untersucht werden.
Berücksichtigte Publikationen und Publikationsorgane	Die Suchstrategie ist nicht dokumentiert.
Forschungsergebnis	Das Forschungspapier zeigt, dass zwischen drei Arten der Compliance-Sicherung unterschieden werden kann. Diese sind Design-Time Compliance Checking, Run-Time Compliance Checking und Backward Compliance Checking. Es wird geschlussfolgert, dass Methoden zur Compliance-Sicherung folgende vier Aspekte beinhalten sollten: (1) Integrierter Ansatz, der alle Phasen des Geschäftsprozesslebenszykluses umfasst, (2) Unterstützung der Compliance-Sicherung über den Kontrollfluss hinaus, (3) intuitive graphische Notation und (4) Anwendung von semantischen Technologien bei der Definition, Entwicklung und Ausführung der Compliance-Kontrollen.

Tab. 61: Überblick über Literaturreviews aus Teilbereichen von GRC (3 von 5)

Zitation	Haghjoo 2012
Forschungsziel(e)	Das Forschungspapier untersucht ob und wie IT zur Generierung von „business value“ beigetragen hat.
Berücksichtigte Publikationen und Publikationsorgane	Zum einen wurde vielzitierte Literatur (mehr als 29 Zitationen insgesamt bzw. 5 pro Jahr) durch eine Schlagwortsuche in GoogleScholar identifiziert. Außerdem wurde auf der Grundlage des Senior Scholars' Basket of Journals on IS (MIS Journal Ranking) führende Journale durchsucht. Zum anderen wurde eine Internetrecherche durchgeführt. Insgesamt berücksichtigt der Review 47 Publikationen.
Forschungsergebnis	Neben einer nach den Fragen „What?“, „Who?“ und „How?“ strukturierten Definition für IT-Governance liefert das Forschungspapier mögliche Nutzeneffekte einer effektiven IT-Governance sowie ein Modell der Mechanismen, die zur Erzielung dieser Nutzeneffekte führen sollen. Zu den in der Literatur am weitesten verbreiteten Nutzeneffekte gehören „Strategic alignment between IT and enterprise objectives“, „Protecting the enterprise's investment in IT“, „Taking advantages of current business opportunities“; „Avoiding potential business threats”. Gemäß dem entwickelten „IT governance and business value”-Modell müssen die folgenden moderierenden Variablen verfügbar sein, damit eine effektive IT-Governance zur Erzielung von „Business Value” führt: „Applicability of mechanisms“, „Clarity of accountability and responsibility in mid/operational levels”, „Desirable behavior in the use of IT”.
Zitation	Lebek et al. 2013
Forschungsziel(e)	Das Forschungspapier präsentiert einen theoriebasierten Literaturreview zur Forschung im Bereich „information security awareness and behavior“. Der Beitrag konzentriert sich konkret auf die Frage, welche Theorien in der letzten Zeit in der Information Systems-Forschung zur Erklärung von „information security awareness and behavior“ verwendet wurden.
Berücksichtigte Publikationen und Publikationsorgane	Die Autoren folgen ebenfalls den Empfehlungen von Webster und Watson (2002) zur Strukturierung der Literatursuche. Es wurde eine Suche mit vielfältigen Schlagwörtern für das spezifische Themengebiet in mehreren akademischen Datenbanken durchgeführt. Es wurden nur Publikationen ab dem Jahr 2000 berücksichtigt. 95 Veröffentlichungen wurden durch diese Suche identifiziert. Eine Vorwärts- und Rückwärtssuche mit Hilfe der Datenbank Web of Science führt dazu, dass im Rahmen des Reviews insgesamt 113 Artikel berücksichtigt wurden.
Forschungsergebnis	Der Beitrag gibt zuerst einen Überblick über die in der Literatur zu diesem Themengebiet verwendeten Theorien und Forschungsmethoden. Hierauf aufbauend wird basierend auf den am meisten verwendeten Theorien ein Metamodell zum Informationssicherheitsverhalten erstellt sowie die zugrundeliegenden Konstrukte mit relevanten Beziehungen und deren Signifikanz diskutiert. Hierdurch können Empfehlungen für weitere Forschung abgeleitet werden. Zu den am meisten verwendeten Theorien gehören die Theorie des geplanten Verhaltens bzw. die Theorie des überlegten Handelns, die General Deterrence Theorie sowie die Theorie der Schutzmotivation.

Tab. 62: Überblick über Literaturreviews aus Teilbereichen von GRC (4 von 5)

Zitation	Milicevic und Goeken 2012 Milicevic und Goeken 2013a Milicevic und Goeken 2013b
Forschungsziel(e)	Ziel der vorgenannten drei Forschungspapiere von Milicevic und Goeken ist die Aufarbeitung empirischer Evidenz in der Forschung zur „IS Security Policy Compliance“ mit Hilfe eines systematischen (Meta-)Reviews.
Berücksichtigte Publikationen und Publikationsorgane	Es erfolgte eine Schlagewortsuche (deutsch und englisch) in akademischen Datenbanken (z.B. ABI/INFORM, EBSCO, Emerald, ScienceDirect, Springerlink). Hierbei wurden gemäß dem Forschungsziel relevante Schlagwörter des Themengebiets mit Schlagwörtern zu empirischen Forschungsmethoden kombiniert. Insgesamt wurden 354 Forschungsarbeiten erfasst.
Forschungsergebnis	Von den 354 relevanten Publikationen beschäftigten sich lediglich 9 mit ähnlichen Konstrukten zur Untersuchung von „Compliance“ bzgl. von Informationssicherheits-Policies. Die Autoren präsentieren basierend auf diesen Arbeiten eine Übersicht der Studienergebnisse unter anderem hinsichtlich der Signifikanz der untersuchten Variablen, eine „Factor Map“ sowie eine Meta-Analyse, wobei die „gepoolten“ Effekte der Variablen untersucht wurden.
Zitation	Rinderle-Ma et al. 2008
Forschungsziel(e)	Es wird ein Überblick zum gegenwärtigen Stand und den zukünftigen Entwicklungen von „Business Process Compliance“ aus Sicht der IT gegeben.
Berücksichtigte Publikationen und Publikationsorgane	Die Suchstrategie ist nicht dokumentiert.
Forschungsergebnis	Der Stand der Technik wird in den Bereichen Annotation von Regularien in Prozessmodellen, Zusicherung von Compliance zur Modellierzeit, Zusicherung von Compliance zur Laufzeit und Compliance bei Prozessänderungen diskutiert. Zukünftig sollten Integrationsaspekte dieser Methoden im Vordergrund stehen, die einerseits auf eine durchgängige Unterstützung von Business- zu IT-Anforderungen und andererseits auf den gesamten Prozesslebenszyklus abzielen sollten.

Tab. 63: Überblick über Literaturreviews aus Teilbereichen von GRC (5 von 5)

Zitation	Simonsson und Johnson 2006
Forschungsziel(e)	Es wird eine Konsolidierung von IT-Governance-Definition angestrebt.
Berücksichtigte Publikationen und Publikationsorgane	Folgende Datenbanken wurden im Februar 2005 mit für IT-Governance relevanten Suchbegriffen durchsucht: ACM Digital Library, ACM The Guide, IEEE Xplore, Science direct/Elsevier, Article Sciences, Compendex, Google Scholar, Springer/Kluwer, Emerald, and Wiley Intersciences. Insgesamt wurden 102 Veröffentlichungen berücksichtigt, die unter anderem aus den folgenden Publikationsorganen stammen: MIS Quarterly, Information Systems Control Journal, Information Systems Research, International Journal of Information Management, International Journal of Accounting.
Forschungsergebnis	Das durch den Literaturreview hergeleitete synthetisierte Verständnis von IT-Governance basiert auf den drei Dimensionen „Domain“, „Decision-making process“ und „Scope“, die jeweils weiter in Sub-Domänen untergliedert werden.

Tab. 64: Literaturbelege zur Kodierung mit Zuordnung zu den Anforderungskategorien und Unterkategorien (1 von 5)

Kategorie	Unterkategorie	Literaturverweise zu den kodierten Textstellen
Strategische Ausrichtung	GRC als Teil des strategischen Managements	Ali et al. 2009, S. 3; Baumöl 2012, S. 11; COSO 2004, S. 2; Damiandes 2005, S. 80; Dahlberg und Kivijärvi 2006, S. 2; Haghjoo 2012, S. 1; De Haes und Van Grembergen 2006, S. 2; De Haes und Van Grembergen 2009, S. 123; De Haes und Van Grembergen 2008a, S. 444; De Haes und Van Grembergen 2008b, S. 1; Deutscher und Felden 2010, S. 2; Grant et al. 2007, S. 5; ISO 2008, S. 3; Jacobson 2009, S. 2; Johannsen und Goeken 2006, S. 13; Karanja und Zaveri 2012, S. 1; Leih 2007, S. 3; Liang et al. 2011, S. 1; Musson und Jordan 2006; OECD 2004, S. 27; Raghupathi 2007, S. 96; Simonsson und Johnson 2006; Teubner und Feller 2008, S. 405; ITGI 2007, S. 5; Urbach et al. 2013, S. 3; Webb et al. 2006, S. 7; Willson und Pollard 2009, S. 99
	GRC als strategische Chance	Abrams et al. 2007, S. 220; Abdullah et al. 2010a, S. 262; Abdullah et al. 2010b, S. 550; Baumöl 2012, S. 7; Böhm 2008, S. 21; Damianides 2004, S. 37; Damiandes 2005, S. 77; Smith und McKeen 2006, S. 719; Krell und Matook 2008, S. 1; Krell und Matook 2009, S. 42; Lu et al. 2007, S. 1; Lu et al. 2009, S. 245; Menzies et al. 2008, S. 137; OCEG 2009, Intro S. 16; PwC 2004, S. 16; PwC 2007, S. 11; Racz et al. 2010b, S. 6; Racz et al. 2010a, S. 4; Schöler und Zink 2008, S. 21-22; Tarantino 2007, S. 31; Dittmar und Wagner 2006, S. 1; Haghjoo 2012, S. 1; Vicente und da Silva 2011a, S. 1
	„trade-off" zwischen Geschäfts- und Compliance-Zielen	Böhm et al. 2009, S. 12; Hoffmann et al. 2012; Krcmar et al. 2011, S. 9
	Nutzenpotentiale	Böhm 2008, S. 26-27; Baumöl 2012, S. 12; Damianides 2004, S. 39; Gill und Purushottam 2008, S. 45; Klotz 2009, S. 17-19; Kranawetter 2009, S. 25; Lazic et al. 2011, S. 6; Oh et al. 2007, S. 425; OCEG 2009, Intro S. 18; SAP 2009, S. 4; Volonio et al. 2004, S. 222; Walser et al. 2007, S. 56-57; Fill 2012; Haghjoo 2012, S. 3; Hardy und Leonard 2011, S. 8; Hoyt und Liebenberg 2011, S. 795-796; Isensee 2008, S. 162; Krcmar et al. 2011, S. 8; Li et al. 2012, S. 180; Puspasari et al. 2011, S. 312; Racz et al. 2011c, S. 7; Spanaki und Papazafeiropoulou 2013, S. 2; Tüllner 2012; Urbach et al. 2013, S. 8-9; van der Veen et al. 2011; Weidlich et al. 2011, S. 1009; Wiesche et al. 2011b, S. 8; Lohre 2009, S. 182-183
	Orientierung an Stakeholderanforderungen	Baumöl 2012, S. 10; Menzies 2006, S. 2; OCEG 2009, Intro S. 6; OECD 2004, S. 24

Tab. 65: Literaturbelege zur Kodierung mit Zuordnung zu den Anforderungskategorien und Unterkategorien (2 von 5)

Kategorie	Unterkategorie	Literaturverweise zu den kodierten Textstellen
Integration	Integration der GRC-Disziplinen	Abrams et al. 2007, S. 219; Baumöl 2012, S. 11; Bhimani 2009, S. 3; Böhm 2008, S. 22; Deloitte 2008, S. 10; Gericke et al. 2009a, S. 1; Gericke et al. 2009b, S. 1; Gill und Purushottam 2008, S. 38; Götz et al. 2008, S. 89; Grant et al. 2007, S. 5; Hauschka 2007, S. 3; Klotz und Dorn 2008, S. 7; Klotz 2009, S. 9; Kranawetter 2009, S. 24-25; Lohre 2009, S. 179; Lu et al. 2009, S. 245; Mossanen 2010, S. 228; OCEG 2009, Intro S. VIII; PwC 2007, S. 10; Racz et al. 2010b, S. 6; Racz et al. 2010c, S. 12; Sackmann 2009, S. 148; SAP 2009, S. 4; Schöler und Zink 2008, S. 21; Silveira et al. 2009; Tarantino 2007, S. 30-31; Withus 2010, S. 100; Krey 2010, S. 8; Krey 2012, S. 1607; Racz et al. 2011c, S. 1; Racz et al. 2011b, S. 325; Spanaki und Papazafeiropoulou 2013, S. 2; Tüllner 2012, S. 118-119; van der Veen et al. 2011, S. 265; Vicente und da Silva 2011a, S. 199; Vicente und da Silva 2011b, S. 1; Willson und Pollard 2009, S. 99; Webb et al. 2006, S. 7; Zoet et al. 2011, S. 454; Menzies 2006, S. 63-64; Racz et al. 2010a, S. 1
	Integriertes Management über GRC-Vorgaben oder Risikobereiche	Menzies 2006, S. 63-64; Racz et al. 2010a, S. 1; Abdullah et al. 2010b, S. 550; Alter und Goeken 2009; Böhm 2008, S. 23; Mossanen et al. 2010, S. 180-181; Barateiro et al. 2012, S. 1-2; Oh et al. 2007, S. 420; OCEG 2009, S. 15; Hoyt und Liebenberg 2011, S. 795; Zoet et al. 2011, S. 456
	Integration von IT-bezogenen und unternehmensweiten Ansätzen	Racz et al. 2010d, S. 6; Wolf und Goeken 2010, S. 239
	Integration in die operativen Geschäftsprozesse	MacLean und Behnam 2010, S. 1499; Menzies 2006, S. 332-333; OCEG 2009, Intro S. 15; Pupke 2008, S. 132
	Methodische und informationstechnische Integration	Deloitte 2008, S. 10; Delbaere und Ferreira 2007, S. 319; Faisst und Buhl 2005, S. 404; Fill et al. 2007, S. 419 und S. 429; PwC 2007, S. 8; Racz et al. 2010a, S. 5; Panitz et al. 2011, S. 3; Vicente und da Silva 2011b, S. 206

Tab. 66: Literaturbelege zur Kodierung mit Zuordnung zu den Anforderungskategorien und Unterkategorien (3 von 5)

Kategorie	Unterkategorie	Literaturverweise zu den kodierten Textstellen
Geschäfts-prozess-orientierung	Bedeutung von Geschäftspro-zessen für GRC	Bai et al. 2007, S. 1; Cannon und Byers 2006, S. 32; El Kharbili und Pulvermüller 2009, S. 61; Marinos et al. 2009, S. 367; zur Muehlen und Rosemann 2005, S. 1; Namiri und Stojanovic 2007a, S. 62; Namiri und Stojanovic 2007b, S. 61; Sackmann 2008a, S. 1137; Sackmann 2008b, S. 2; Sackmann 2009, S. 149; Sienou et al. 2008, S. 16; Weidlich et al. 2010, S. 1; Bai et al. 2012, S. 1; Bräuer et al. 2013, S. 1245; Cabanillas et al. 2012, S. 337; Caron et al. 2013, S. 1; Kittel 2013, S. 967; Lohmann 2011, S. 1; Lohmann 2013, S. 606; Ly et al. 2012, S. 2; Ramezani et al. 2012, S. 1; Schultz 2013, S. 120; Schultz et al. 2012, S. 1; Turetken et al. 2011, S. 1; Zoet et al. 2011, S. 454
	Integration von GPM und GRC-Management	Awad et al. 2008, S. 1; Awad et al. 2009, S. 1; DIN 2008a, S. 6; DIN 2008b, S. 5; El Kharbili et al. 2008a, S. 107; El Kharbili et al. 2008b, S. 3; Karagiannis 2008; S. 1160-1162; Lu et al. 2007, S. 2; Menzies 2006, S. 333; PwC 2004, S. 16; Rieke und Winkelmann 2008, S. 347; Sackmann 2008c, S. 42-43; Sadiq et al. 2007, S. 3; Schumm et al. 2010, S. 1; Sienou et al. 2008, S. 17; Ly et al. 2012, S. 7; Weiss und Winkelmann 2011, S. 1
	Bedeutung der gesamten Enter-prise Architec-ture	Barateiro et al. 2012, S. 1
	Bedeutung eines geschäftspro-zessorientierten Ansatzes für die Automatisierung der Compliance-Sicherung	Caron et al. 2013, S. 5; Elgammal et al. 2010b, S. 3; El Kharbili et al. 2008c, S. 181; Krcmar et al. 2011, S. 6; Liu et al. 2007, S. 335
Manage-ment-Systeme	---	Bhimani 2009, S. 2; Braganza und Franken 2007, S. 98; Isensee 2008, S. 161; Klotz 2009, S. 13-16; Lohre 2009, S. 183; Maheshwari et al. 2009, S. 12; von Werder und Grundei 2006, S. 19-20; Caron et al. 2013, S. 7; Chang et al. 2013, S. 2; Grünninger und Jantz 2013, S. 135; Leon et al. 2012, S. 453; van der Veen et al. 2011, S. 270

Tab. 67: Literaturbelege zur Kodierung mit Zuordnung zu den Anforderungskategorien und Unterkategorien (4 von 5)

Kategorie	Unterkategorie	Literaturverweise zu den kodierten Textstellen
Automatisierung	Unterscheidung der Bedeutungsvarianten von IT	Klotz und Dorn 2008, S. 9-10; Klotz 2009, S. 6-8; Teubner und Feller 2008, S. 401; Rath und Sponholz 2009, S. 119; Sackmann et al. 2008, S. 79
	IT-Unterstützung des GRC-Managements	Abdullah et al. 2010a, S. 262; Abdullah et al. 2010b, S. 550; Krcmar et al. 2011, S. 6; Oh et al. 2007, S. 420; PwC 2004, S. 17; Puspasari et al. 2011, S. 311; Racz et al. 2011b, S. 325; Walser et al. 2007, S. 57
	Automatisierung der Compliance-Sicherung	Agrawal et al. 2006, S. 1; Awad et al. 2008, S. 1; Awad et al. 2009, S. 1; Butler und McGovern 2008, S. 11; Beiler und Böhm 2009, S. 380; Cannon und Byers 2006, S. 33-34; El Kharbili und Pulvermüller 2009, S. 61; Kranawetter 2009, Prologue; Lotz et al. 2008, S. 1157; Masli et al. 2010 , S. 4 und S. 14; Menzies et al. 2008, S. 141; Pohlman 2008, S. 41; Sackmann 2008c, S. 39; Sackmann et al. 2008, S. 79; Sackmann und Kähmer 2008, S. 366; Tarantino 2007, S. 34; Asprion und Knolmayer 2013, S. 4; Schultz 2013, S. 123; Turetken et al. 2012, S. 29; Werner et al. 2012, S. 5350; Werner et al. 2013, S. 375-376; Wiesche et al. 2012, S. 2; Christiaanse und Hulstijn 2012, S. 322; Karanja und Zaveri 2012, S. 630
Flexibilität	Relevanz von Flexibilität	Lu et al. 2007, S. 2; Müller 2007, S. 109; Sackmann 2008c, S. 40; Sackmann 2008b, S. 1138; Sackmann 2008c, S. 2; Sackmann et al. 2008, S. 84; Sackmann 2009, S. 150; Sandner et al. 2010, S. 2; Weigand et al. 2011, S. 791; Kittel 2013, S. 968; Kittel et al. 2013, S. 1; Ly et al. 2012, S. 6; Sackmann et al. 2013, S. 31; Schultz 2013, S. 12; Turetken et al. 2011; Turetken et al. 2012, S. 28
	Trade-off zwischen Flexibilität und strategischer Zielerreichung	Grundei 2006, S. 45
	Flexibilität durch serviceorientierte Architekturen	Elgammal et al. 2010a, S. 2; Elgammal et al. 2010b, S. 3 und S. 13; Loosli 2008, S. 7; Lotz et al. 2008, S. 384; Lowis 2008, S. 1157
	Flexibilität durch Cloud-Computing	Accorsi et al. 2011, S. 1; Martens und Teuteberg 2011, S. 1

Tab. 68: Literaturbelege zur Kodierung mit Zuordnung zu den Anforderungskategorien und Unterkategorien (5 von 5)

Kategorie	Unterkategorie	Literaturverweise zu den kodierten Textstellen
Menschliche Faktoren	Compliance-Verhalten	Baumöl 2012, S. 10; Bulgurcu et al. 2009, S. 5; Bulgurcu et al. 2010, S. 523; Boss et al. 2009, S. 160; Cannoy und Salam 2010, S. 129; D' Arcy et al. 2009, S. 93; DIN 2008b, S. 17; De Haes und Van Grembergen 2006, S. 2; Grundei und Talaulicar 2009, S. 74; Hengmith 2008, S. 19; Herath und Rao 2009, S. 118; Hu et al. 2007, S. 154; Johnston et al. 2010, S. 1; Johnston und Warkentin 2010, S. 550; Lange 2008, S. 712; Myyry et al. 2009, S. 135; Puhakainen und Siponen 2010, S. 757; Pahnila et al. 2007, S. 9-10; Spears und Barki 2010, S. 503; Siponen und Vance 2010, S. 487; Siponen et al. 2006, S. 653; Smith und McKeen 2006, S. 723-724; Al-Omari et al. 2012a, S. 1; Al-Omari et al. 2013, S. 1; Aurigemma und Panko 2012, S. 1; Goo et al. 2012, S. 2959; Hu et al. 2011, S. 54; Lebek et al. 2013, S. 2976; Lowry und Moody 2013, S. 2998; Panitz et al. 2011, S. 1; Simonsson und Johnson 2006; Son 2011, S. 296; Vance et al. 2012, S. 190; Abraham 2011, S. 4050; Al-Omari et al. 2012b, S. 1633
	Compliance-Kultur	Ali et al. 2009, S. 4; Abdullah et al. 2010a, S. 262; Abdullah et al. 2010b, S. 550; Lange 2008, S. 712; OCEG 2009, Intro S. 25; Panitz et al. 2011, S. 3; PwC 2004, S. 15; Wecker und van Laak 2008, S. 41
	„tone at the top"	Baumöl 2012, S. 10; Eichler 2010, S. 58; IDW 2010, S. 5; Menzies 2006, S. 334; OCEG 2009, S. 10; PwC 2007, S. 13-14; SAP 2009, S. 12; Withus 2010, S. 101; Hu et al. 2012, S. 615; Kwon und Johnson 2013, S. 3974; Oh et al. 2007, S. 425; Panitz et al. 2011, S. 3; van der Veen et al. 2011, S. 268; Willson und Pollard 2009, S. 100; Becker et al. 2011b, S. 1976; Zafar et al. 2011, S. 315

Tab. 69: Einteilung von gestaltungsorientierten Arbeiten nach Management-Methoden, Methoden zur Modellierung von GRC-Informationen und Automatisierungsmethoden

Art der Methode	Kurzbeschreibung	Quellen
Management-Methoden	Management-Methoden zielen auf die Lösung von Management-Problemen ab, wobei als Adressat vorwiegend die Führungsebene angesprochen ist. Im Bereich der Management-Methoden werden unter anderem Methoden zur wirtschaftlichen Auswahl von risikosteuernden Maßnahmen, die Verknüpfung von GPM und Risikomanagement, Kennzahlensysteme unter Berücksichtigung unterschiedlicher GRC-Aspekte sowie die Auswahl von Services unter Einbeziehung von GRC-Aspekten behandelt.	Accorsi et al. 2008; Bai et al. 2007; Baumöl 2012; Barateiro et al. 2012; Chang et al. 2013; Damianides 2004; Delbaere und Ferreira 2007; Deutscher und Felden 2010; Faisst und Buhl 2005; Fill et al. 2007; Gehrke und Thams 2010; Gericke et al. 2009a; Gericke et al. 2009b; Goeken und Knackstedt 2009; Goeken und Knackstedt 2008; Guan und Levitan 2012; Isensee 2008; Kronschnabl 2010; Lohre 2009; Loosli 2008; Lu et al. 2009; Marinos et al. 2009; Md Khan 2007; Paine et al. 2005; Panitz et al. 2010; Pauli et al. 2010; Puhakainen und Siponen 2010; Sackmann 2008a; Sackmann 2008b; Sackmann et al. 2013; Sackmann et al. 2009; Schaad et al. 2009; Setiono et al. 2006; Sienou et al. 2008; Silveira et al. 2009; van der Veen et al. 2011; von Werder und Grundei 2006; Zoet et al. 2011
Methoden zur Modellierung von GRC-Informationen	Methoden zur Modellierung von GRC-Informationen zielen auf die bedarfsgerechte Bereitstellung von Informationen des GRC-Managements ab. Zur Modellierung von GRC-Informationen werden bspw. Methoden zur Geschäftsprozessmodellierung um GRC-Informationen ergänzt oder Ontologien zur semantischen Beschreibung von GRC-Informationen konstruiert.	Awad et al. 2008; Awad et al. 2009; Bai et al. 2007; Bai et al. 2012; Bräuer et al. 2013; Elgammal et al. 2010b; Fill 2012; Guan und Levitan 2012; Hengmith 2008; El Kharbili et al. 2008b; El Kharbili et al. 2008c; El Kharbili und Pulvermüller 2009; Liu et al. 2007; Lu et al. 2007; Lohmann 2013; Lohmann 2011; Ly et al. 2012; zur Muehlen und Rosemann 2005; Namiri und Stojanovic 2007a; Namiri und Stojanovic 2007b; Namiri und Stojanovic 2008; Sadiq et al. 2007; Schumm et al. 2010; Schultz 2013; Sienou et al. 2008; Strecker et al. 2011; Turetken et al. 2011; Turetken et al. 2012; Rieke und Winkelmann 2008; Weiss und Winkelmann 2011; Weidlich et al. 2010

Art der Methode	Kurzbeschreibung	Quellen
Automatisierungsmethoden	Methoden zur Automatisierung der Compliance-Sicherung und Risikosteuerung versuchen abweichendes Verhalten ex-ante zu verhindern („compliance by design“) oder wollen solches Verhalten nachträglich aufdecken („compliance by detection“).	Abrams et al. 2007; Accorsi et al. 2011; Agrawal et al. 2006; Awad et al. 2008; Awad et al. 2009; Birukou et al. 2010; Bräuer et al. 2013; Cabanillas et al. 2012; Cannon und Byers 2006; Caron et al. 2013; El Kharbili und Pulvermüller 2009; El Kharbili et al. 2008b; El Kharbili et al. 2008c; Elgammal et al. 2010b; Ghose und Koliadis 2007; Goedertier und Vanthienen 2006a; Goedertier und Vanthienen 2006b; Götz et al. 2008; Governatori et al. 2006; Hoffmann et al. 2012; Johnson und Grandison 2007; Kittel 2013; Kittel et al. 2013; Kudo et al. 2007; Küster et al. 2007; Liu et al. 2007; Lohmann 2013; Lohmann 2011; Lotz et al. 2008; Lowis 2008; Lu et al. 2007; Lu et al. 2009; Ly et al. 2012; Namiri und Stojanovic 2007a; Namiri und Stojanovic 2007b; Namiri und Stojanovic 2008; Pohlman 2008; Puspasari et al. 2011; PwC 2004; PwC 2007; Ramanathan et al. 2007; Ramezani et al. 2012; RedMonk 2008; Rozinat und van der Aalst 2008; Sackmann 2008c; Sackmann und Kähmer 2008; Sackmann et al. 2008; Sadiq et al. 2007; Sadiq et al. 2005; Sandner et al. 2010; SAP 2009; Schöler und Zink 2008; Schultz 2013; Schumm et al. 2010; Teuteberg und Freundlieb 2009; Turetken et al. 2011; Turetken et al. 2012; van der Werf et al. 2012; Weidlich et al. 2010; Weidlich et al. 2011; Weigand et al. 2011; Werner et al. 2012; Werner et al. 2013; Wolf und Gehrke 2009

Tab. 70: Zuordnung der Veröffentlichungen zur Automatisierung der Compliance-Sicherung und Risikosteuerung zu den verschiedenen Automatisierungsansätzen

Automatisierungsansatz	Literaturverweise
Compliance by design	Accorsi et al. 2011; Awad et al. 2008; Awad et al. 2009; Bräuer et al. 2013; Cabanillas et al. 2012; Elgammal et al. 2010b; Ghose und Koliadis 2007; Goedertier und Vanthienen 2006a; Goedertier und Vanthienen 2006b; Governatori et al. 2006; Hoffmann et al. 2012; Küster et al. 2007; Liu et al. 2007; Lohmann 2013; Lohmann 2011; Lu et al. 2007; Lu et al. 2009; Namiri und Stojanovic 2008; Sadiq et al. 2007; Schumm et al. 2010
Compliance by generation	Goedertier und Vanthienen 2006a; Goedertier und Vanthienen 2006b; Küster et al. 2007; Lohmann 2013; Lohmann 2011
Compliance by validation	Accorsi et al. 2011; Awad et al. 2008; Awad et al. 2009; Bräuer et al. 2013; Cabanillas et al. 2012; Elgammal et al. 2010b; Ghose und Koliadis 2007; Governatori et al. 2006; Hoffmann et al. 2012; Liu et al. 2007; Lu et al. 2009; Sadiq et al. 2007
Compliance by detection	Agrawal et al. 2006; Birukou et al. 2010; Caron et al. 2013; Namiri und Stojanovic 2007a; Namiri und Stojanovic 2007b; Ramezani et al. 2012; Rozinat und van der Aalst 2008; Sandner et al. 2010; Schultz 2013; van der Werf et al. 2012; Weidlich et al. 2010; Weidlich et al. 2011; Werner et al. 2012; Werner et al. 2013; Wolf und Gehrke 2009

B Anhang zu Kapitel 4 Delphi-Studie zu Anforderungen und Forschungsbedarfen eines strategischen GRC-Managements

Tab. 71: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (vollständige Liste; 1 von 5)

#	Forschungsbedarf (Kategorie / Forschungsziel)	Runde 2		Runde 3		
		M	SD	M	SD	SD_{Diff}
1	Are there "basic controls" being relevant for every compliance system? Are there differences between the industries? (Integration / DandE) [§1]	4,92	1,19	5,36	0,61	-0,58
1	Evaluation method for the consequences of compliance violations including effects on operational business processes (cost-benefit analysis of controls) (Human factors / Design) [§2]	5,50	0,65	5,36	0,72	0,07
3	Understand how organizations adopt existing tools and methods in the context of GRC (Automation / DandE) [§3]	5,00	0,95	5,29	0,70	-0,25
4	Which control types can be automated? (Automation / DandE) [§4]	5,40	0,80	5,21	0,67	-0,13
5	Theoretical and empirical examination of the potential benefits of GRC (Strategic Orientation / DandE) [§5]	5,08	0,76	5,14	0,64	-0,12
5	Development of general and industry specific control models (reference models for control processes) for the integrated fulfillment of GRC requirements (Integration / Design) [§6]	5,17	0,80	5,14	0,64	-0,16
5	Method to derive company specific controls from regulatory requirements (e.g. laws) (Integration / Design) [§7]	5,00	1,00	5,14	0,64	-0,36
5	Examinations of the conditions for the automation approaches (respectively control model used, compliance by design vs. compliance by detection) (Automation / DandE) [§8]	5,00	1,00	5,14	0,64	-0,36
5	Development of techniques and methods to improve the compliance behaviour and the compliance culture (Human factors / Design) [§9]	5,08	0,95	5,14	0,64	-0,31

Tab. 72: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (vollständige Liste; 2 von 5)

#	Forschungsbedarf (Kategorie / Forschungsziel)	Runde 2		Runde 3		SD_{Diff}
		M	SD	M	SD	
10	Empirical studies on the advantages of alternative coordination approaches for GRC (coordination with a central organizational unit, integration of GRC into the core business processes or a combined approach) (Integration / DandE) [§10]	4,83	0,90	5,07	0,46	-0,44
10	Extension and consolidation of existing empirical examinations of compliance behavior (Human factors / DandE) [§11]	5,17	0,99	5,07	0,59	-0,39
12	Application and evaluation of the automation methods for controls under real life conditions (Automation / Design) [§12]	5,00	1,00	5,00	0,76	-0,24
13	Examinations of overlapping / synergy effects and inconsistencies between the GRC disciplines (Governance, Risk Management, Compliance Management) (Integration / DandE) [§13]	4,82	1,19	4,93	0,70	-0,49
13	Examination of the influence of the company culture on GRC (Human factors / DandE) [§14]	5,00	1,01	4,93	0,70	-0,31
15	Comparison of Standards and Best Practices to the sub domains of GRC with view to overlapping and synergy effects (Integration / DandE) [§15]	4,67	0,85	4,92	0,73	-0,12
16	Development of methods that enable fast reactions on compliance requirement and risk changes (Flexibility / Design) [§16]	4,83	0,90	4,86	0,52	-0,38
17	Examination of the Integration of IT specific and enterprise wide approaches for GRC (Integration / DandE) [§17]	4,83	0,90	4,79	0,77	-0,12
17	Reference model for integrated control or reporting systems of GRC (e.g. on the basis of the Balanced Scorecard) (Integration / Design) [§18]	4,91	1,00	4,79	0,77	-0,22
17	Development of software/IS development practices that take GRC requirements into account. (Integration / Design) [§19]	5,00	0,85	4,79	0,67	-0,18
17	Further development of existing automation approaches for controls covering the complete process life cycle (Automation / Design) [§20]	4,83	0,80	4,79	0,56	-0,24

Tab. 73: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (vollständige Liste; 3 von 5)

#	Forschungsbedarf (Kategorie / Forschungsziel)	Runde 2		Runde 3		SD_{Diff}
		M	SD	M	SD	
17	Development of methods for the selection and combination of controls (Human factors / Design) [§21]	4,83	0,80	4,79	0,67	-0,13
22	Interplay of GRC and "normal" management (Strategic Orientation / DandE) [§22]	4,67	0,62	4,77	0,58	-0,05
22	Examination of the education required to implement, use and sustain the GRC environment (i.e. knowledge of internal vs. knowledge of external resources) (Human factors / DandE) [§23]	4,83	0,80	4,77	0,70	-0,10
24	Adaption of the stakeholder analysis for GRC-Management (Strategic Orientation / Design) [§24]	4,75	1,01	4,75	0,60	-0,42
25	Examinations of overlapping / synergy effects and inconsistencies of different GRC requirements (Integration / DandE) [§25]	4,75	0,92	4,71	0,59	-0,34
25	Examination of the integration of business process management and GRC management (Business Process Orientation / DandE) [§26]	4,60	1,20	4,71	0,80	-0,40
25	Examination of the connection between the determinants of compliance behaviour and the control types (Human factors / DandE) [§27]	4,75	0,83	4,71	0,59	-0,24
28	Adaption and evaluation of strategic planning methods for GRC-Management (Strategic Orientation / Design) [§28]	5,00	1,08	4,67	0,47	-0,61
29	Development of IT support for the GRC-Management (Integration / Design) [§29]	4,92	0,95	4,64	0,61	-0,34
29	Development of information system to support management aspects of GRC (Automation / Design) [§30]	4,83	0,90	4,64	0,61	-0,29
29	Examination of the isolated and combined deployment of different control types (Human factors / DandE) [§31]	4,75	1,01	4,64	0,48	-0,53
32	Examination of the interplay between GRC and operational business processes / IT service management processes (Integration / DandE) [§32]	4,75	1,09	4,62	0,62	-0,46
33	Development of risk based approaches to prioritize the fulfillment of compliance requirements (Integration / Design) [§33]	4,75	0,72	4,57	0,73	0,01

Tab. 74: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (vollständige Liste; 4 von 5)

#	Forschungsbedarf (Kategorie / Forschungsziel)	Runde 2		Runde 3		SD_{Diff}
		M	SD	M	SD	
33	Efficiency of the automation of GRC controls: cost-benefit-considerations (transaction costs theory) (Automation / DandE) [§34]	4,45	1,16	4,57	0,73	-0,43
33	Longitudinal analysis of behavioural and cultural aspects in the context of GRC (moving from 'low-effective GRC' to 'more-effective GRC') (Human factors / DandE) [§35]	4,92	0,86	4,57	0,62	-0,24
36	Examination of the strategic contribution of GRC in dependence of different implementation approaches for strategic GRC management (Big Bang and Top Down Approach, Implementation of GRC in cycles (continuous improvement), GRC as a lip service) (Strategic Orientation / DandE) [§36]	4,08	1,44	4,50	0,63	-0,81
36	Extension and evaluation of artefacts of GPM (procedure models, methods, tools) in the context of GRC (Business Process Orientation / Design) [§37]	4,45	0,89	4,50	0,82	-0,07
38	Examination of benefit potentials and weak points of software making an integrated management of GRC possible (Integration / DandE) [§38]	4,17	1,52	4,43	0,73	-0,79
38	Further development of existing approaches describing the management processes for an integrated management of GRC (Integration / Design) [§39]	4,36	1,07	4,43	0,49	-0,57
38	Development of a reference model for GRC software (Integration / Design) [§40]	4,75	1,16	4,43	0,82	-0,34
41	Consideration of the conflict of objectives between GRC requirements and strategic goals in existing methods for strategic planning (Strategic Orientation / Design) [§41]	4,50	1,12	4,42	0,64	-0,48
42	Examination of the strategic contribution of GRC in dependence of the strategy chosen (focus, cost leadership, diversification) (Strategic Orientation / DandE) [§42]	4,25	1,16	4,36	0,81	-0,35

Tab. 75: Befragungsergebnisse zu den Forschungsbedarfen für ein strategisches GRC-Management (vollständige Liste; 5 von 5)

#	Forschungsbedarf (Kategorie / Forschungsziel)	Runde 2		Runde 3		
		M	SD	M	SD	SD_{Diff}
42	Integration of GRC into enterprise modeling frameworks (e.g. ARIS, MEMO) (Integration / Design) [§43]	4,75	0,92	4,36	0,97	0,05
42	Development of a methodical support to balance out trade-off between GRC and strategic achievement of objectives (Flexibility / Design) [§44]	4,83	0,90	4,36	0,61	-0,29
45	Development of procedures, methods and tools for the coordination of the management systems (Management systems / Design) [§45]	4,45	0,89	4,31	0,72	-0,17
45	Examinations of conflicts between GRC requirements and strategic achievement of objectives (Flexibility / DandE) [§46]	4,67	1,31	4,31	0,61	-0,71
47	Examination of the advantages of a business process oriented approach for strategic GRC management (Business Process Orientation / DandE) [§47]	3,91	1,00	4,21	1,01	0,02
48	Development of conceptual data models for strategic GRC management (Integration / Design) [§48]	4,33	1,31	4,15	0,77	-0,54
49	Examination of the strategic contribution of GRC by means of the resource-based view (Strategic Orientation / DandE) [§49]	4,25	0,83	4,14	0,83	0,00
49	Examination of the limits of the integrated fulfillment of GRC requirements (Integration / DandE) [§50]	4,17	1,14	4,14	0,64	-0,50
51	Examinations of the influence of situation related aspects towards trade-off between GRC requirements and strategic achievement of objectives (Flexibility / DandE) [§51]	4,42	0,95	4,08	0,73	-0,22
52	Examination of context factors which support the advantages of a business process oriented approach (Business Process Orientation / DandE) [§52]	4,00	0,95	4,07	0,80	-0,15
53	Examination of the distribution of GRC-related tasks over GRC-related management systems (e.g. internal auditing, quality management) in practice (Management systems / DandE) [§53]	4,33	0,75	4,00	0,78	0,04
54	Development of a structural organization for a strategic GRC-Management (Integration / Design) [§54]	4,00	0,82	3,93	0,46	-0,36

#	Forschungsbedarf (Kategorie / For-	Runde 2		Runde 3		SD_{Diff}
54	Extension of business process modeling languages by all aspects of GRC (Integration / Design) [§55]	4,67	0,85	3,93	1,03	0,18

Tab. 76: Bedeutung der Anforderungen und Forschungsbedarfe nach Anforderungskategorien

Anforderungen			Forschungsbedarfe		
Rang	Anforderungskategorie	Durchschnittliche Bedeutung	Rang	Anforderungskategorie	Durchschnittliche Bedeutung
1	Automation	5,37	1	Automation	4,95
2	Human factors	5,33	2	Human factors	4,89
3	Management systems	5,21	3	Integration	4,63
4	Integration	5,13	4	Strategic orientation	4,59
5	Strategic orientation	5,07	5	Flexibility	4,40
6	Business process orientation	5,00	6	Business process orientation	4,38
7	Flexibility	4,50	7	Management systems	4,15

Tab. 77: Bedeutung der Forschungsbedarfe nach dem Forschungsansatz

Forschungsansatz	Durchschnittliche Bedeutung
Describing and Explaining	4,52
Designing	4,46

Tab. 78: Weitere Auswertungen zu den Anforderungen (1 von 2) [ID=Identifier; M_{Diff} = Differenz der Mittelwerte; R = Runde, $Rang_{Diff}$ = Differenz der Ränge; CV = Variationskoeffizient, CV_{Diff} = Differenz der Variationskeoffizienten]

Rang	ID	M_{Diff}	Rang (R2)	$Rang_{Diff}$	CV (R2)	CV (R3)	CV_{Diff}
1	#1	0,12	1	0	0,11	0,10	-0,01
2	#2	0,18	2	0	0,11	0,08	-0,03
2	#3	0,38	3	-1	0,18	0,08	-0,10
4	#4	0,23	4	0	0,20	0,11	-0,09
4	#5	0,37	9	-5	0,19	0,13	-0,05
4	#6	0,23	4	0	0,18	0,11	-0,06
7	#7	0,10	9	-2	0,20	0,11	-0,09
8	#8	0,01	7	1	0,21	0,13	-0,08
8	#9	0,21	12	-4	0,23	0,11	-0,12
8	#10	-0,06	4	4	0,15	0,15	0,00
11	#11	-0,06	7	4	0,22	0,14	-0,08
12	#12	-0,06	9	3	0,17	0,16	-0,01
13	#13	0,27	16	-3	0,28	0,17	-0,11
13	#14	0,00	12	1	0,16	0,15	-0,01
13	#15	0,13	14	-1	0,17	0,16	-0,01
16	#16	0,24	18	-2	0,24	0,19	-0,06
16	#17	0,14	17	-1	0,29	0,23	-0,06
18	#18	-0,30	15	3	0,22	0,16	-0,06
19	#19	0,08	19	0	0,29	0,29	-0,01

Tab. 79: Weitere Auswertungen zu den Anforderungen (2 von 2) [$Q_{0,25}$ = 0,25-Quantil (unteres Quartil); $Q_{0,75}$ = 0,75-Quantil (oberes Quartil); IQR = Interquartilsabstand; IQR_{Diff} = Differenz der Interquartilsabstände]

		Runde 2			Runde 3			
Rang	ID	$Q_{0,25}$	$Q_{0,75}$	IQR	$Q_{0,25}$	$Q_{0,75}$	IQR	IQR_{Diff}
1	#1	5	6	1	6	6	0	-1
2	#2	5	6	1	5	6	1	0
2	#3	5	6	1	5	6	1	0
4	#4	5	6	1	5	6	1	0
4	#5	5	6	1	5	6	1	0
4	#6	5	6	1	5	6	1	0
7	#7	5	6	1	5	6	1	0
8	#8	5	6	1	5	6	1	0
8	#9	4	6	2	5	6	1	-1
8	#10	5	6	1	5	6	1	0
11	#11	4	6	2	4,75	6	1,25	-0,75
12	#12	5	6	1	4	6	2	1
13	#13	4	6	2	4	6	2	0
13	#14	4	6	2	4	6	2	0
13	#15	4	6	2	4	6	2	0
16	#16	4	5	1	4	5,25	1,25	0,25
16	#17	4	6	2	4	6	2	0
18	#18	4	6	2	4	5	1	-1
19	#19	3	5	2	3,75	5	1,25	-0,75

Tab. 80: Weitere Auswertungen zu den Forschungsbedarfen (1 von 2) [ID = Identifier; M_{Diff} = Differenz der Mittelwerte; R = Runde, $Rang_{Diff}$ = Differenz der Ränge; CV = Variantionskoeffizient, CV_{Diff} = Differenz der Variantionskeoffizienten]

Rang	ID	M_{Diff}	Rang (R2)	$Rang_{Diff}$	CV (R2)	CV (R3)	CV_{Diff}
1	§1	0,44	14	-13,00	0,24	0,11	-0,13
1	§2	-0,14	1	0,00	0,12	0,13	0,02
3	§3	0,29	7	-4,00	0,19	0,13	-0,06
4	§4	-0,19	2	2,00	0,15	0,13	-0,02
5	§5	0,06	5	0,00	0,15	0,12	-0,03
5	§6	-0,03	3	2,00	0,15	0,12	-0,03
5	§7	0,14	7	-2,00	0,20	0,12	-0,08
5	§8	0,14	7	-2,00	0,20	0,12	-0,08
5	§9	0,06	5	0,00	0,19	0,12	-0,06
10	§10	0,24	18	-8,00	0,19	0,09	-0,10
10	§11	-0,10	3	7,00	0,19	0,12	-0,07
12	§12	0,00	7	5,00	0,20	0,15	-0,05
13	§13	0,11	26	-13,00	0,25	0,14	-0,10
13	§14	-0,07	7	6,00	0,20	0,14	-0,06
15	§15	0,25	35	-20,00	0,18	0,15	-0,03
16	§16	0,03	18	-2,00	0,19	0,11	-0,08
17	§17	-0,04	18	-1,00	0,19	0,16	-0,02
17	§18	-0,12	17	0,00	0,20	0,16	-0,04
17	§19	-0,21	7	10,00	0,17	0,14	-0,03
17	§20	-0,04	18	-1,00	0,17	0,12	-0,05
17	§21	-0,04	18	-1,00	0,17	0,14	-0,02
22	§22	0,10	35	-13,00	0,13	0,12	-0,01
22	§23	-0,06	18	4,00	0,17	0,15	-0,02
24	§24	0,00	27	-3,00	0,21	0,13	-0,09
25	§25	-0,04	27	-2,00	0,19	0,12	-0,07
25	§26	0,11	39	-14,00	0,26	0,17	-0,09
25	§27	-0,04	27	-2,00	0,17	0,12	-0,05
28	§28	-0,33	7	21,00	0,22	0,10	-0,12
29	§29	-0,28	14	15,00	0,19	0,13	-0,06
29	§30	-0,19	18	11,00	0,19	0,13	-0,05

Rang	ID	M_{Diff}	Rang (R2)	$Rang_{Diff}$	CV (R2)	CV (R3)	CV_{Diff}
29	§31	-0,11	27	2,00	0,21	0,10	-0,11
32	§32	-0,13	27	5,00	0,23	0,14	-0,09
33	§33	-0,18	27	6,00	0,15	0,16	0,01
33	§34	0,12	41	-8,00	0,26	0,16	-0,10
33	§35	-0,35	14	19,00	0,18	0,14	-0,04
36	§36	0,42	52	-16,00	0,35	0,14	-0,21
36	§37	0,05	41	-5,00	0,20	0,18	-0,02
38	§38	0,26	50	-12,00	0,36	0,16	-0,20
38	§39	0,07	45	-7,00	0,24	0,11	-0,13
38	§40	-0,32	27	11,00	0,24	0,19	-0,06
41	§41	-0,08	40	1,00	0,25	0,14	-0,10
42	§42	0,11	48	-6,00	0,27	0,19	-0,09
42	§43	-0,39	27	15,00	0,19	0,22	0,03
42	§44	-0,47	18	24,00	0,19	0,14	-0,05
45	§45	-0,14	41	4,00	0,20	0,17	-0,03
45	§46	-0,36	35	10,00	0,28	0,14	-0,14
47	§47	0,30	55	-8,00	0,25	0,24	-0,01
48	§48	-0,18	46	2,00	0,30	0,19	-0,12
49	§49	-0,11	48	1,00	0,20	0,20	0,01
49	§50	-0,03	50	-1,00	0,27	0,15	-0,12
51	§51	-0,34	44	7,00	0,22	0,18	-0,04
52	§52	0,07	53	-1,00	0,24	0,20	-0,04
53	§53	-0,33	46	7,00	0,17	0,20	0,02
54	§54	-0,07	53	1,00	0,20	0,12	-0,09
54	§55	-0,74	35	19,00	0,18	0,26	0,08

Tab. 81: Weitere Auswertungen zu den Forschungsbedarfen (2 von 2) [$Q_{0,25}$ = 0,25-Quantil (unteres Quartil); $Q_{0,75}$ = 0,75-Quantil (oberes Quartil); IQR = Interquartilsabstand; IQR_{Diff} = Differenz der Interquartilsabstände]

		Runde 2			Runde 3			
Rang	ID	$Q_{0,25}$	$Q_{0,75}$	IQR	$Q_{0,25}$	$Q_{0,75}$	IQR	IQR_{Diff}
1	§1	4	6	2	5	6	1	-1
1	§2	5	6	1	5	6	1	0
3	§3	4	6	2	5	6	1	-1
4	§4	4,75	6	1,25	5	6	1	-0,25
5	§5	4,25	6	1,75	5	6	1	-0,75
5	§6	4,25	6	1,75	5	6	1	-0,75
5	§7	4	6	2	5	6	1	-1
5	§8	4	6	2	5	6	1	-1
5	§9	4,25	6	1,75	5	6	1	-0,75
10	§10	4	6	2	5	5	0	-2
10	§11	4,25	6	1,75	5	5,25	0,25	-1,5
12	§12	4	6	2	5	5,25	0,25	-1,75
13	§13	5	6	1	4	5,25	1,25	0,25
13	§14	4	6	2	4	5,25	1,25	-0,75
15	§15	4	5	1	4	5,5	1,5	0,5
16	§16	4	6	2	4,75	5	0,25	-1,75
17	§17	4	5,75	1,75	4	5	1	-0,75
17	§18	4	6	2	4	5	1	-1
17	§19	5	6	1	4	5	1	0
17	§20	4,25	5	0,75	4	5	1	0,25
17	§21	4	5,75	1,75	4	5	1	-0,75
22	§22	4	5	1	4	5	1	0
22	§23	4	5,75	1,75	4,5	5	0,5	-1,25
24	§24	4	6	2	4	5	1	-1
25	§25	4	5,75	1,75	4	5	1	-0,75
25	§26	3	6	3	4	5,25	1,25	-1,75
25	§27	4	5,75	1,75	4	5	1	-0,75
28	§28	5	6	1	4	5	1	0
29	§29	4	6	2	4	5	1	-1
29	§30	4	5,75	1,75	4	5	1	-0,75
29	§31	4	6	2	4	5	1	-1
32	§32	4	6	2	4	5	1	-1
33	§33	4	5	1	4	5	1	0
33	§34	4	6	2	4	5	1	-1
33	§35	4,25	5,75	1,5	4	5	1	-0,5
36	§36	3,25	5	1,75	4	5	1	-0,75
36	§37	4	5	1	4	5	1	0
38	§38	2,25	5,75	3,5	4	5	1	-2,5

Rang	ID	Runde 2			Runde 3			IQR_{Diff}
		$Q_{0,25}$	$Q_{0,75}$	IQR	$Q_{0,25}$	$Q_{0,75}$	IQR	
38	§39	3	5	2	4	5	1	-1
38	§40	4	6	2	4	5	1	-1
41	§41	4	5	1	4	5	1	0
42	§42	3,25	5	1,75	4	5	1	-0,75
42	§43	4,25	5	0,75	4	5	1	0,25
42	§44	4	5,75	1,75	4	5	1	-0,75
45	§45	4	5	1	4	5	1	0
45	§46	4	6	2	4	5	1	-1
47	§47	3	5	2	3	5	2	0
48	§48	4	5	1	4	5	1	0
49	§49	3,25	5	1,75	4	5	1	-0,75
49	§50	3,25	5	1,75	4	5	1	-0,75
51	§51	3,25	5	1,75	3,5	5	1,5	-0,25
52	§52	3	5	2	3,75	4,25	0,5	-1,5
53	§53	4	5	1	3,5	4	0,5	-0,5
54	§54	3	5	2	4	4	0	-2
54	§55	4	5	1	4	4	0	-1

C Anhang zu Kapitel 5 Datenseitiges Modell für das strategische GRC-Management

Tab. 82: Zuordnung von weiteren Entitäten aus den bestehenden konzeptionellen Modellen zu den Informationsobjekten des Modells

IO	Sonstige zugeordnete Begriffe
Kontrolle	Input Event (7), OutputEvent (7), OutputData (7), Input Data (7), Configuration (7), Decision (7), executable constraint (11), RecoveryAction (13), ControlPattern (ActivityOccurrence, Absence, Universality, Existence, BoundedExistence, ActivityOrder, Precedence, ChainPrecedence, Response, ChainResponse) (14), ControlTrigger (Frequency, DateTrigger, Activity) (14), Beschreibung (18), Region/Land (18), Gesellschaft (legal entity) (18), Priorität (18), Compliance erreicht (18), Konsequenz bei Nichterfüllung (18), MeasureImpact (28), MeasureRelationship (28)
Rolle	Organizational Level (27), Organizational Element (32), Job Position Type in Organizational Unit (32), Job Position Type (32)
Geschäftsprozess	Property (2), State (3), SignificantAccount (12), Input (34), Output (34), Result (34)
Risiko	RiskFactor (3), Risk Tolerance (3), RiskAppetite (3), RiskSituation (3), Risk Factor (23), Risk Appetite (24), Risk Register (24), Assumption (27), Probability (27), Impact (27), Quantitative / Qualitative Description (27), Assignment (28), Uncertainty (28), ChanceRiskRelationship (28), Risk Appetite (31), Risikoneigung (33), Risikoart (33), Risikotoleranz (33)
Kontrollziel	---
GRC-Vorgabe	---
Ressource	---
Ziel	---
Assessment	Audit Scoping (24), Findings (24), Findings (31), Recommendations (31), Action Plans (31)
Kennzahl	ETL-Prozessmodell (ETL-Prozess, Subprozess, Prozessart, Prozessende, Datenquellen, Transformationsschritte, Datenziele, Parallelität) (16)
Richtlinie	Constraint (6), Policy Life-Cycle (31)
Dokumentation	ActivityType (8), DocumentType (8), DerivationRule (8), IntegrityConstraint (8), DomainPredicate (8), DeonticAssignment (Permission, Obligation, ConditionalCommitment) (8), ActivityType (9), Obligation (9), ActivityType (10), ConditionalCommitment (10)
IT-Komponente	---
Anwendungsbereich	---

IO	Sonstige zugeordnete Begriffe
Ausführung	---
Implementierungslogik	Formalism (7), Subject (7), Function (7), Event-Condition-Action (ECA) (7), Action (7), ComplexAction (7), Condition (7), Custom (7)
Rahmenwerk	---
Strategie	---
Stakeholder	Interest (3)
Reifegrad	---
Verletzung	---

Tab. 83: Definition der Informationsobjekte des Modells

Informationsobjekt	Definition
Kontrolle	Kontrollen stellen angemessene Maßnahmen dar, welche die Erreichung der Kontrollziele unterstützen. Sie können entweder präventiv oder reaktiv ausgestaltet sein und unterschiedliche Ebenen adressieren (unternehmensweite Kontrollen bis hinzu Kontrollen für bestimmte Anwendungssysteme). Die Begriffe Kontrolle und Regel werden teilweise synonym verwendet oder unter Regeln werden lediglich Kontrollen verstanden, die automatisierbar sind.
Rolle	Unter Rollen werden Personen oder Organisationseinheiten verstanden, die für eine bestimmte Aktivität innerhalb eines Prozesses verantwortlich sind.
Geschäftsprozess	Ein Geschäftsprozess wird definiert als eine logische Abfolge von Aktivitäten, die einen Input hinsichtlich der Erreichung eines geschäftlichen Ziels umwandeln. An der Ausführung von Geschäftsprozessen sind üblicherweise mehrere Funktionen oder Abteilungen beteiligt.
Risiko	Risiken werden als negative Abweichung eines tatsächlichen von einem erwarteten Ereignis definiert. Sie gefährden hiermit die Erreichung von Zielen. Teilweise werden auch positive Abweichungen (Chance) unter dem Risikobegriff subsumiert.
Kontrollziel	Kontrollziele definieren die erwarteten Resultate einer durchzuführenden Kontrolle. Sie übersetzen hiermit GRC-Vorgaben in konkrete Anforderungen für ein bestimmtes Unternehmen, die bei der Ausführung der Geschäftsprozesse zu berücksichtigen sind.
GRC-Vorgabe	GRC-Vorgaben sind die Quellen zur Definition der Kontrollziele und Kontrollen eines Unternehmens. Sie können externem oder internem Ursprungs sowie freiwilliger oder verpflichtender Natur sein. Beispiele sind Gesetze oder sonstige Regularien, Standards und Best Practices, die befolgt werden sollen sowie interne Vorgaben, wie ein Code of Conduct.

Informations-objekt	Definition
Ressource	Als Ressourcen werden jegliche Artefakte verstanden, die neben oder als Teil von Geschäftsprozessen Gegenstand von GRC sein können. Zu Ressourcen gehören neben Geschäftsprozessen auch Daten, Produkte oder Projekte.
Ziel	Ein Ziel wird als ein angestrebter Zustand eines Unternehmens verstanden.
Assessment	Assessments werden als jede Art der Prüfung, Bewertung oder Analyse von Geschäftsprozessen oder Risiken verstanden.
Kennzahl	Kennzahlen werden als Messgröße zur Ermittlung der Zielerreichung von Geschäftsprozessen verstanden.
Richtlinie	Richtlinien werden als Dokumente innerhalb eines Unternehmens verstanden, die Kontrollziele innerhalb eines Anwendungsbereichs für die Mitarbeiter zusammenführen und darstellen.
Dokumentation	Ein wichtiger Bestandteil von GRC ist die Erbringung eines Nachweises für normkonforme Geschäftsprozesse. Hierbei ist die Dokumentation von herausragender Bedeutung.
IT-Komponente	Hierunter werden jegliche IT-Systeme einschließlich der Infrastrukturkomponenten verstanden.
Anwendungsbereich	Richtlinien beziehen sich zur Strukturierung üblicherweise auf einen bestimmten Anwendungsbereich. Die Strukturierung der Anwendungsbereiche ist unternehmensspezifisch. Mögliche Anwendungsbereiche sind nach GRC-Vorgaben strukturiert Informationssicherheit, Datenschutz oder Finanzberichterstattung.
Rahmenwerk	Unter Rahmenwerken werden Standards bzw. Best Practices wie im IT-Bereich ITIL oder COBIT verstanden, die bei der Umsetzung von GRC-Vorgaben unterstützend herangezogenen werden können.
Strategie	Im Rahmen des Modells wird die Strategie als den Zielen übergeordnete Instanz betrachtet. Sie soll die langfristigen Maßnahmen zur Erreichung der Unternehmensziele beinhalten.
Stakeholder	Unter Stakeholdern werden die Anspruchsgruppen des Unternehmens verstanden. Hierzu gehören Kunden, Kapitalgeber und Mitarbeiter.
Reifegrad	Die Bewertung des Reifegrads mittels Reifegradmodellen wird als eine mögliche Form des Assessments verstanden.
Verletzung	Eine Verletzung liegt vor, wenn eine bestimmte Instanz eines Geschäftsprozesses nicht konform zu den Vorgaben des Geschäftsprozesses durchgeführt wird. Dies bedeutet, dass nicht alle Kontrollen korrekt ausgeführt wurden.
Entscheidung	Entscheidungen betreffen im Rahmen des Modells insbesondere die Auswahl von Strategien und Zielen. Zum Treffen von Entscheidungen werden adäquate Informationen benötigt, die durch Kennzahlen und Assessments gewonnen werden.
Schwachstelle	Schwachstelle oder Schwäche wird im Kontext des Modells im Hinblick auf Kontrollen im Sinne von Kontrollschwächen verwendet. Schwachstellen beinhalten das Risiko von Compliance-Verletzungen. Sie sollten daher im Rahmen von Assessments aufgedeckt und beseitigt werden.

Literaturverzeichnis

Abdullah, S.N.; Indulska, M.; Sadiq, S. (2009): A Study of Compliance Management in Information Systems Research. In: Proceedings of the 17th European Conference on Information System (ECIS 2009). Verona, Paper 5. (#)

Abdullah, S.N.; Indulska, M.; Sadiq, S. (2010a): Emerging challenges in information systems research for regulatory compliance management. In: Pernici, B. (Hrsg.): Proceedings of the 22nd International Conference on Advanced Information Systems Engineering (CAISE 2010). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 251-265. (#)

Abdullah, S.N.; Sadiq, S.; Indulska, M. (2010b): Information Systems Research: Aligning to Industry Challenges in Management of Regulatory Compliance. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Taipei. (#)

Abraham, S. (2011): Information Security Behavior: Factors and research directions. In: Proceedings of the 17th Americas Conference on Information Systems (AMCIS 2011). Detroit, Paper 462. (#)

Abrams, C.; von Känel, S.; Müller, S.; Pfitzmann, B.; Ruschka-Taylor, S. (2007): Optimized enterprise risk management. In: IBM Systems Journal (46, 2), S. 219-234. (#)

Accorsi, R.; Lowis, L.; Sato, Y. (2011): Automatisierte Compliance-Zertifizierung Cloud-basierter Geschäftsprozesse. In: Wirtschaftsinformatik (53, 3), S. 139-149. (#)

Accorsi, R.; Sato, Y.; Kai; S. (2008): Compliance Monitor for Early Warning Risk Determination. In: Wirtschaftsinformatik (50, 5), S. 375-382. (#)

Agrawal, R.; Johnson, C.; Kiernan, J.; Leymann, F. (2006): Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology. In: Proceedings of the 22nd International Conference on Data Engineering (ICDE 2006). IEEE. (#)

Ajzen, I. (1985): From Intensions to Actions: A Theory of Planned Behavior. In: Kuhl, J.; Beckmann, J. (Hrsg.): Action Control. Springer, Berlin et al., S. 11-39.

Ajzen, I.; Madden, T.J. (1986): Prediction of goal-directed behavior: attitudes, intentions, and perceived behavioral control. In: Journal of Experimental Social Psychology (22, 5), S. 453-474.

Albach, H. (2001): Shareholder Value und Unternehmenswert - Theoretische Anmerkungen zu einem aktuellen Thema. Zeitschrift für Betriebswirtschaft (71, 6), S. 643-674.

Ali, S.; Green, P.; Parent, M. (2009): The role of a Culture of Compliance in Information Technology Governance. In: Sadiq, S.; Indulska, M.; zur Muehlen, M.; Dubois, E.; Johannesson, P. (Hrsg.): Proceedings of the 2nd International Workshop on Governance, Risk and Compliance − Applications in Information Systems (GRCIS 2009). CEUR, Amsterdam. (#)

Alter, S.; Goeken, M. (2009): Konzeptionelle Metamodelle von IT-Governance-Referenzmodellen als Basis der Kombination und Iintegration in einer Multi-Modell-Umgebung. In: Hansen, H.R.; Karagiannis, D.; Fill, H.-G. (Hrsg.): Business Services: Konzepte, Technologien, Anwendungen. 9. Internationale Tagung Wirtschaftsinformatik. Österreichische Computer Gesellschaft, Wien, Band 1, S. 705-716. (#)

Allweyer, T. (2005): Geschäftsprozessmanagement. Strategie, Entwurf, Implementierung, Controlling. W3L, Bochum.

Al-Omari, A.; Deokar, A.; El-Gayar, O.; Walters, J.; Aleassa, H. (2013): Information Security Policy Compliance: An Empirical Study of Ethical Ideology. In: Proceedings of the 46th Annual Hawaii International Conference on System Sciences (HICSS 2013). IEEE, S. 3018-3027. (#)

Al-Omari, A.; El-Gayar, O.; Deokar, A. (2012a): Information Security Policy Compliance: The Role of Information Security Awareness. In: Proceedings of the 18th Americas Conference on Information Systems (AMCIS 2012). Seattle, Paper 16. (#)

Al-Omari, A.; El-Gayar, O.; Deokar, A. (2012b): Security Policy Compliance: User Acceptance Perspective. In: Proceedings of the 45th Annual Hawaii International Conference on System Sciences (HICSS 2012). IEEE, S. 3317-3326. (#)

Armstrong, J.S. (1982): The value of formal planning for strategic decisions: A review of empirical research. In: Strategic Management Journal (3, July-September), S. 197-211.

Arrow, K. (1985): The Economics of Agency. In: Pratt, J.W.; Zeckhauser, R.J. (Hrsg.): Principals and Agents: The Structure of Business. Harvard Business School Press, Bosten, S. 37-51.

Arsanjani, A.; Booch, G.; Boubez, T.; Brown, P.C.; Chappell, D.; deVadoss, J.; Erl, T.; Josuttis, N.; Krafzig, D.; Little, M.; Loesgen, B.; Manes, A.T.; McKendrick, J.; Ross-Talbot, S.; Tilkov, S.; Utschig-Utschig, C.; Wilhelmsen, H. (ohne Jahr): SOA-Manifest. http://www.soa-manifesto.org/default_german.html, Abruf am 2015-04-20.

Asprion, P.M.; Knolmayer, G.F. (2013): Assimilation of Compliance Software in Highly Regulated Industries: An Empirical Multitheoretical Investigation. In: Proceedings of the 46th Annual Hawaii International Conference on System Sciences (HICSS 2013). IEEE, S. 4405-4414. (#)

Atteslander, P. (2010): Methoden der empirischen Sozialforschung. 12. Auflage, Erich Schmidt Verlag, Berlin.

Aurigemma, S.; Panko, R. (2012): A Composite Framework for Behavioral Compliance with Information Security Policies. In: Proceedings of the 45th Annual Hawaii International Conference on System Sciences (HICSS 2012). IEEE, S. 3248-3257. (#)

Awad, A.; Decker, G.; Weske, M. (2008): Efficient Compliance Checking using BPMN-Q and Temporal Logic. In: Dumas, M.; Reichert, M.; Shan, M.-C. (Hrsg.): Business Process Management: Proceedings of the 6th International Conference on Business Process Management (BPM 2008). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 326-341. (#)

Awad, A.; Weidlich, M.; Weske, M. (2009): Secification, Verification and Explanation of Violation for Data Aware Compliance Rules. In: Baresi, L.; Chi, C.-H.; Suzuki, J. (Hrsg.): Proceedings of the 7th International Joint Conference on Service Oriented Computing (ICSOC 2009). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 500-515. (#)

Bai, X.; Padman, R.; Krishnan, R. (2007): A Risk Management Approach to Business Process Design. In: Proceedings of the 28th International Conference on Information Systems (ICIS 2007). Montreal, Paper 28. (#)

Bai, X.; Krishnan, R.; Padman, R.; Wang, H.J. (2012): On Risk Management with Information Flows in Business Processes. In: Information System Research, published online before print November 8. (#)

Baker, M.J. (2000): Writing a Literature Review. In: Marketing Review (1, 2), S. 219-247.

Ball, L.; Harris, R. (1982): SMIS Members: A Membership Analysis. In: MIS Quarterly (6, 1), S. 19-38.

Bamberg, A.; Kaven, A. (2006): Deutsche Telekom: Von einem konzernweiten S-OX404-Projekt zur Compliance-Organisation. In: Menzies, C. (Hrsg.): Sarbanes-Oxley und Corporate Compliance: Nachhaltigkeit, Optimierung, Integration. Schäffer-Poeschel, Stuttgart, S. 432-441.

Barateiro, J.; Antunes, G.; Borbinha, J. (2012): Manage Risks through the Enterprise Architecture. In: Proceedings of the 45th Annual Hawaii International Conference on System Sciences (HICSS 2012). IEEE, S. 3297-3306. (#)

Barney, J. (1991): Firm Resources and Sustained Competitive Advantage. In: Journal of Management (17, 1), S. 99-120.

Bartsch, S.; Schlagwein, D. (2010): Ein konzeptionelles Framework zum Verständnis des multidimensionalen Gegenstandes des Wertbeitrags der IT. In: Schumann, M.; Kolbe, L.M.; Breitner, M.H.; Frerichs, A. (Hrsg.): Tagungsband der Multikonferenz Wirtschaftsinformatik 2010 (MKWI 2010). Universitätsverlag Göttingen, Göttingen, S. 233-245.

Baskerville, R.; Pries-Heje, J. (2010): Erklärende Designtheorie. In: Wirtschaftsinformatik (52, 5), S. 259-271.

Bate, P. (2007): Editorial to the special issue "bringing the design sciences to organization development and change management". In: Journal of Applied Behavioral Science (43, 1), S. 8-11.

Baumöl, U. (2012): IT-Governance als Basis für ein wertorientiertes Informatikmanagement. In: HMD - Praxis der Wirtschaftsinformatik (49, 284), S. 6-14. (#)

Bayerl, B.; Alber, K.; Wohlgemuth, W.A.; Freitag, M.H.; Nagel, E. (2009): Evidenzbasierte Medizin und gesundheitsbezogene Lebensqualität als potentielle Priorisierungskriterien medizinischer Leistungen am Beispiel der peripheren arteriellen Verschlusskrankheit - Identifikation relevanter Stakeholder und Interviewleitfadenentwicklung. In: Wohlgemuth, W.A.; Freitag, M.H. (Hrsg.): Priorisierung in der Medizin – Interdisziplinäre Forschungsansätze. Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin, S 119-157.

Bea, F.X.; Göbel, E. (2006): Organisation. 3. Auflage, Lucius & Lucius, Stuttgart.

Bea, F.X.; Haas, J. (2005): Strategisches Management. 4. Auflage, Lucius & Lucius, Stuttgart.

Becker, G. (1968): Crime and punishment: An economic approach. In: Journal of Political Economy (76, 2), S. 169-217.

Becker, J.; Bergner, P.; Delfmann, P.; Eggert, M.; Weiss, B. (2011a): Supporting Business Process Compliance in Financial Institutions − A Model-Driven Approach. In: Bernstein, A.; Schwabe, G. (Hrsg.): Proceedings of the 10th International Conference on Wirtschaftsinformatik (WI 2011), Zürich, Band 1, S. 355-364. (#)

Becker, J.; Delfmann, P.; Knackstedt, K.; Kuropka, K. (2002): Konfigurative Referenzmodellierung. In: Becker, J.; Knackstedt, R. (Hrsg.): Wissensmanagement mit Referenzmodellen. Konzepte für die Anwendungssystem- und Organisationsgestaltung. Heidelberg, S. 25-144.

Becker, J.; Eggert, M.; Heddier, M.; Knackstedt, R. (2012): Merging Conceptual Modeling and Law for Legally Compliant Information Systems Design – A Framework-Based Research Agenda. In: Proceedings of the 45th Annual Hawaii International Conference on System Sciences (HICSS 2012). IEEE, S. 5241-5250. (#)

Becker, J.; Eggert, M.; Winkelmann, A.; Knackstedt, R. (2011b): Towards a Contingency Theory based Model of the Influence of Regulation on MIS. In: Proceedings of the 17th Americas Conference on Information Systems (AMCIS 2011). Detroit, Paper 220. (#)

Becker, J.; Kugler, M.; Rosemann, M. (2005): Prozessmanagement - Ein Leitfaden zur prozessorientierten Organisationsgestaltung. 5. Auflage, Springer, Berlin et al.

Becker, J.; Mathas, C.; Winkelmann, A. (2009): Geschäftsprozessmanagement. Springer, Berlin et al.

Becker, W.; Holzmann, R.; Ulrich, P. (2011c): Non-Compliance in Organisationen. Wie lässt sich wirtschaftskriminelles Handeln vermeiden? In: Zeitschrift für Corporate Governance (6, 1/2), S. 5-12. (#)

Becker, J.; Schütte, R. (2004): Handelsinformationssysteme. 2. Auflage, Redline, Landsberg/Lech.

Beiler, T.; Böhm, M. (2009): Internal Controls Scripting Language (ICSL): Grundzüge einer Instruktionssprache für Interne Kontrollen. In: Hansen, H.R.; Karagiannis, D.; Fill, H.-G. (Hrsg.): Business Services: Konzepte, Technologien, Anwendungen. 9. Internationale Tagung Wirtschaftsinformatik. Österreichische Computer Gesellschaft, Wien, Band 1, S. 377-388. (#)

Bellamy, R.K.E.; Erickson, T.; Fuller, B.; Kellogg, W.A.; Rosenbaum, R.; Thomas, J.C.; Vetting-Wolf, T. (2007): Seeing is believing: Designing visualizations for managing risk and compliance. In: IBM Systems Journal (46, 2), S. 205-218. (#)

Benbasat, I.; Zmud, R.W. (2003): The Identity Crisis within the IS Discipline: Defining and Communicating the Discipline's Core Properties. In: MIS Quarterly (27, 2), S. 183-194.

Bhimani, A. (2009): Risk Management, corporate governance and management accounting. Emerging interdependencies. In: Management Accounting Research (20, 1), S. 2-5. (#)

Bird, F. (2001): Good governance: A Philosophical discussion of the responsibilities and practices of organizational governors. In: Canadian Journal of Administrative Studies (18, 4), S. 298-312.

Birukou, A.; D' Andrea, V.; Leymann, F.; Serafinski, J.; Silveira, P.; Strauch, S.; Thuczek, M. (2010): An Integrated Solution for Runtime Compliance Governance in SOA. In: Maglio, P.P.; Weske, M.; Yang, J.; Fantinato, M. (Hrsg.): Proceedings of the 8th International Conference on Service Oriented Computing (ICSOC 2010). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 122-136. (#)

Böhm, M. (2008): IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT. In: HMD – Praxis der Wirtschaftsinformatik (45, 263), S. 15-29. (#)

Böhm, M.; Goeken, M.; Johannsen, W. (2009): Compliance und Alignment: Vorgabenkonformität und Strategieabgleich als Erfolgsfaktoren für eine wettbewerbsfähige IT. In: HMD – Praxis der Wirtschaftsinformatik (46, 269), S. 7-17. (#)

Bohnsack, R.; Marotzki, W.; Meuser, M. (2006): Hauptbegriffe qualitativer Sozialforschung. 2. Auflage, Budirch, Opladen.

Börner, R.; Goeken, M. (2009): Identification of Business Services – Literature Review and Lessons Learned. In: Proceedings of the 15th Americas Conference on Information Systems (AMCIS 2009). San Francisco, Paper 106.

Boss, S.R.; Kirsch, L.J.; Angermeier, I.; Shingler, R.A.; Boss, R.W. (2009): If someone is watching, I'll do what I'm asked: mandatories, control, and information security. In: European Journal of Information Systems (18, 2), S. 151-164. (#)

Braganza, A.; Desouza, K.: Implementing Section 404 of the Sarbanes Oxley Act. Recommendations for the Information Systems Organization. In: Communications of the Association for Information Systems (18, Article 22), S. 464-487. (#)

Braganza, A.; Franken, A.: SOX, compliance, and power relationships. In: Communications of the ACM (50, 9), S. 97-102.

Brancheau, J.C.; Janz, B.; Wetherbe, J.C. (1996): Key issues in information systems management: 1994-95 SIM Delphi results. In: MIS Quarterly (20, 2), S. 225-242.

Bräuer, S.; Delfmann, P.; Dietrich, H.-A.; Steinhorst, M. (2013): Using a Generic Model Query Approach to Allow for Process Model Compliance Checking – An Algorithmic Perspective. In: Alt, R.; Franczyk, B. (Hrsg.): Proceedings of the 11th International Conference on Wirtschaftsinformatik (WI 2013). Leipzig, S. 1245-1259. (#)

Brown, C.V.; Magill, S.L. (1994): Aligning the IS Functions with the Enterprise: Toward a Model of Antecedents. In: MIS Quarterly, (18, 4), S. 371-403.

Bretz, J. (2007): Gesetzliche und bankenaufsichtliche Anforderungen an die IT-Sicherheit. In: Bretz, J. et al. (Hrsg.): IT-Sicherheitsmanagement in Banken und Sparkassen. Finanz Colloquium Heidelberg, Heidelberg.

Brühl, R.; Buch, S. (2006): Einheitliche Gütekriterien in der empirischen Forschung? – Objektivität, Reliabilität und Validität in der Diskussion. In: ESCP-EAP Working Paper No. 20, Dezember.

Brynjolfsson, E.; Hitt, L. (2003): Computer Productivity: Firm-Level Evidence. In: The Review of Economics and Statistics (85, 4), S. 793-808.

Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. (2009): Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance. In: Proceedings of the 15th Americas Conference on Information Systems (AMCIS 2009). San Francisco, Paper 419. (#)

Bulgurcu, B.; Lavusoglu, H.; Benbasat, I. (2010): Information Systems Security Policy Compliance: An Empirical-Study of Rationality-Based Beliefs and Information Security Awareness. In: MIS Quaterly (34, 3), S. 523-548. (#)

Burgelman, R. (1983): Corporate entrepreneurship and strategic management: Insights from a process study. In: Management Science (29, 12), S. 1349-1364.

Butler, T.; McGovern, D. (2008): Adopting IT to Manage Compliance and Risk: An Institutional Perspective. In: Proceedings of the 16th European Conference on Information System (ECIS 2008). Galway, Paper 241. (#)

Burmann, C. (2005): Strategische Flexibilität und der Marktwert von Unternehmen. In: Kaluza, B.; Behrens, S. (Hrsg.): Erfolgsfaktor Flexibilität. Strategien und Konzepte für wandlungsfähige Unternehmen. Schmidt Technological Economics, Berlin, S. 29-53.

Byrd, T.; Turner, D. (2000): Measuring the flexibility of information technology infrastructure: exploratory analysis of a construct. In: Journal of Management Information Systems (17, 1), S. 167-208.

Byrd, T.; Turner, D. (2001): An exploratory examination of the relationship between flexible IT infrastructure and competitive advantage. In: Information & Management (39, 1), S. 41-52.

Cabanillas, C.; Resinas, M.; Ruiz-Cortés, A. (2012): Introducing a Mashup-based Approach for Design-Time Compliance Checking in Business Processes. In: Bajec, M.; Eder, J. (Hrsg.): Advanced Information Systems Engineering Workshops (CAISE 2012 International Workshops). Springer, Lecture Notes in Business Information Processing (LNBIP), Berlin et al., S. 337-350. (#)

Cannon, J.C.; Byers, M. (2006): Compliance Deconstructed. In: ACM Queue September, S. 30-37. (#)

Cannoy, S.D.; Salam, A.F. (2010): A framework for health care information assurance policy and compliance. In: Communications of the ACM (53, 3), S. 126-131. (#)

Caron, F.; Vanthienen, J.; Baesens, B. (2013): Comprehensive rule-based compliance checking and risk management with process mining. In: Decision Support Systems (54, 3), S. 1357-1369. (#)

Carr, N.G. (2003): IT doesn't matter. In: Harvard Business Review (81, May), S. 41-49.

Carr, N.G. (2004): Does IT matter? Information technology and the corrosion of competitive advantage. Harvard Business School Press, Bosten.

Chang, I-C.; Chang, S.-I; Liu, C.-C. (2013): Assessment Mechanism of Internal Control for Information Technology Governance. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS). Jeju Island, Paper 117. (#)

Chen, P.P.-S. (1976): The entity-relationship model − toward a unified view of data. In: ACM Transactions on Database Systems (1, 1), S. 9-36.

Chow, R.; Golle P.; Jakobsson, M.; Shi, E.; Staddon, J.; Masuoka, R.; Molina, J. (2009): Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings ACM workshop on cloud computing security. ACM, New York, S 85-90.

Christ, M.H.; Emett, S.A.; Summers, S.L.; Wood, D.A. (2012): The Effects of Preventive and Detective Controls on Employee Performance and Motivation. In: Contemporary Accounting Research (29, 2), S. 432-452. (#)

Christiaanse, R.; Hulstijn, J. (2012): Control Automation to reduce Costs of Control. In: Bajec, M.; Eder, J. (Hrsg.): Advanced Information Systems Engineering Workshops (CAISE 2012 International Workshops). Springer, Lecture Notes in Business Information Processing (LNBIP), Berlin et al., S. 322-336. (#)

Committee of Sponsoring Organizations of the Treadway Commission (COSO, Hrsg., 1994): Internal Control – Integrated Framework. 2. Auflage, o.O. (#)

Committee of Sponsoring Organizations of the Treadway Commission (COSO, Hrsg., 2004): Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk. http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_German.pdf, Abruf am 2015-05-21. (#)

Committee of Sponsoring Organizations of the Treadway Commission (COSO, Hrsg., 2013): Internal Control – Integrated Framework. Executive Summary. http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf, Abruf am 2016-11-07.

Cook, T. D.; Campbell, D. (1979): Quasi-Experimentation: Design and Analysis Issues for Field Settings. Rand McNally College Publishing Company.

Cooper, H.M. (1988): Organizing knowledge syntheses: A taxonomy of literature reviews. In: Knowledge in Society (1, 1), S. 104-126.

Craig, R.T. (1981): Generalization of Scott's Index of Intercoder Agreement. In: Public Opinion Quarterly (45, 2), S. 260-264.

Crawford, D.; Crawford, J. (2013): GRC Assessment Tools. Lulu.com, o.O.

Currie, W. (2008): Institutionalization of IT Compliance: A Longitudinal Study. In: Proceedings of the 29th International Conference on Information Systems (ICIS 2008). Paris, Paper 182. (#)

Cushing, B.E. (1990): Frameworks, Paradigms, and Scientific Research in Management Information Systems. In: Journal of Information Systems (4, 2), S. 38-59.

Dahlberg, T.; Kivijärvi, H. (2006): An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument. In: Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS). IEEE. (#)

Dajani, J.S.; Sincoff, M.Z.; Talley, W.K. (1979): Stability and agreement criteria for the termination of Delphi studies. In: Technological Forecasting and Social Change (13, 1), S. 83-90.

Damianides, M. (2004): How does SOX change IT? In: Journal of Corporate Accounting and Finance (15, 6), S. 35-41. (#)

Damiandes, M. (2005): Sarbanes-Oxley and IT-Governance: New Guidance on IT Control and Compliance. In: Informations Systems Journal (22, 1), S. 77-85. (#)

Danielson, M.G.; Heck, J.L., Shaffer, D.R. (2008): Shareholder Theory − How Opponents and Proponents Both Get It Wrong. In: Journal of Applied Finance (18, 2), S. 62-66.

D' Arcy, J.; Hovav, A.; Galletta, D. (2009): User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. In: Information Systems Research (20, 1), S. 79-98. (#)

Davis, F.D. (1986): A technology acceptance model for empirically testing new end-user information systems: Theory and results. Sloan School of Management, Massachusetts Institute of Technology.

Davis, F.D. (1989): Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. In: MIS Quarterly (13, 3), S. 319-340.

Davis F.D.; Bagozzi, R.P.; Warshaw, P.R. (1989): User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. In: Management Science (35, 8), S. 982-1003.

Davis, J.H.; Schoorman, F.D.; Donaldson, L. (1997): Toward a Stewardship Theory of Management. In: The Academy of Management Review (22, 1), S. 20-47.

De Haes, S.; Van Grembergen, W. (2006): Information Technology Governance Best Practices in Belgian Organisations. In: Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS 2006). IEEE. (#)

De Haes, S.; Van Grembergen, W. (2008a): An Exploratory Study into the Design of an IT Governance Minimum Baseline through Delphi Research. In: Communications of the Association for Information Systems (22, 1), Article 24, S. 444-458. (#)

De Haes, S.; Van Grembergen, W. (2008b): Analysing the Relationship between IT Governance and Business/IT Alignment Maturity. In: Proceedings of the 41th Annual Hawaii International Conference on System Sciences (HICSS 2008). IEEE. (#)

De Haes, S.; Van Grembergen, W. (2009): An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment. In: Information Systems Management (26, 2), S. 123-137. (#)

Delbaere, M.; Ferreira, R. (2007): Addressing the data aspects of compliance with industry models. In: IBM Systems Journal (46, 2), S. 319-334. (#)

Deloitte (Hrsg., 2008): Growing confidence (the smart way to manage governance, risk, and compliance). http://www.myexpospace.com/OracleDemogrounds2008/PDFDOCLIB/GRC-growingconfidence.pdf, Abruf am 2014-08-28. (#)

Delfmann, P. (2006): Adaptive Referenzmodellierung. Methodische Konzepte zur Konstruktion und Anwendung wiederverwendungsorientierter Informationsmodelle. Logos-Verlag, Berlin, zugelassene Dissertation Universität Münster.

Deutscher, J.-H.; Felden, C. (2010): Proposal of an Artifact that Supports the IT-Governance Control Process. In: Proceedings of the 18th European Conference on Information System (ECIS 2010). Pretoria, Paper 127. (#)

De Vet, E.; Brug, J.; De Nooijer, J.; Dijkstra, A.; De Vries, N.K. (2005): Determinants of forward stage transitions: a Delphi study. In: Health Education Research (20, 2), S. 195-205.

Delbecq, A.L.; Van de Ven, A.H.; Gustafson, D.H. (1975): Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes. Scott, Foresman and Company, Glenview, Illinois.

Deutsche Bundesbank (Hrsg., 2010): Die neue Basler Eigenkapitalvereinbarung (Basel II). Deutsche Bundesbank Monatsbericht April 2001. http://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Monatsberichtsaufsaetze/2001/2001_04_basel.pdf?__blob=publicationFile, Abruf am 2015-05-13. (#)

Deutsches Institut für Interne Revision (Hrsg., 2011): Internationale Standards für die berufliche Praxis der Internen Revision 2011. Frankfurt am Main.

Deutsches Institut für Normung e.V. (DIN, Hrsg., 2000): DIN EN ISO 9000. Qualitätsmanagementsysteme, Grundlagen und Begriffe. Beuth, Berlin. (#)

Deutsches Institut für Normung e.V. (DIN, Hrsg., 2004): Umweltmanagementsysteme − Anforderungen mit Anleitung zur Anwendung (ISO14001:2004). Beuth, o.O.

Deutsches Institut für Normung e.V. (DIN, Hrsg., 2008a): Informationstechnik − IT-Sicherheitsverfahren − Informationssicherheits-Managementsysteme − Anforderungen (ISO/IEC 27001:2005). o.O. (#)

Deutsches Institut für Normung e.V. (DIN, Hrsg., 2008b): Qualitätsmanagementsysteme − Anforderungen (ISO 9001:2008). Beuth, o.O.

Dibbern, J.; Goles, T.; Hirschheim, R.; Jayatilaka, B. (2004): Information Systems Outsourcing: A Survey and Analysis of the Literature. In: The DATA BASE for Advances in Information Systems (35, 4), S. 6-102.

Dickson, G.W.; Leitheiser; R.L., Wetherbe, J.C.; Nechis, M. (1984): Key Information Systems Issues for the 1980's. In: MIS Quarterly (8, 3), S. 135-159.

DiMaggio, P.J.; Powell, W.W. (1983): The Iron Cage Revisited − Institutional Isomorphism and Collective Rationality in Organizational Fields. In: American Sociological Review (48, 2), S. 147-160.

DiMaggio, P.J.; Powell, W.W. (1991): Introduction. In: Powell, W.W.; DiMaggio, P.J. (Hrsg.): The Institutionalism in Organizational Analysis. University of Chicago Press, Chicago, S. 1-38.

Dittmar, L.; Wagner, S. (2006): The Unexpected Benefits of Sarbanes-Oxley. In: Harvard Business Review (84, 4), S. 133-140. (#)

Domschke, W.; Drexl, A. (2011): Einführung in Operations Research. 8. Auflage, Springer, Berlin et al.

Donaldson, L. (1990): The ethereal hand: Organizational economics and management theory. In: Academy of Management Review (15, 3), S. 369-381.

Donaldson, L. (2001): The contingency theory of organizations. Sage, Thousand Oaks et al.

Donaldson, L.; Davis, J.H. (1991): Stewardship Theory or Agency Theory: CEO governance and share-holder returns. In: Australian Journal of Management (16, 1), S. 49-65.

Dostal, W. (2008): Service-orientierte Architekturen mit Web Services. Konzepte – Standards – Praxis. Elsevier, Heidelberg et al.

Ebers, M.; Gotsch, W. (2006): Institutionenökonomische Theorien der Organisation. In: Kieser, A.; Ebers, M. (Hrsg.): Organisationstheorien. 6. Auflage, Kohlhammer, Stuttgart.

Eckert, S.; Lamparter, G.; Möller, K. (2004): Konzept und Umsetzung eines Risikomanagementsystems bei der DÜRR AG. In: Zeitschrift für Controlling & Management (48, Special Issue 3), S. 26-36.

Eichler, H. (2010): Nachhaltige Unternehmenskultur als Grundlage wirksamer Corporate Governance. In: Zeitschrift für Corporate Governance (5, 2), S. 57-64. (#)

Ein-Dor, P.; Segev, E. (1982): Organizational Context and MIS Structure: Some Empirical Evidence. In: MIS Quarterly (6, 3), S. 55-68.

Elgammal, A.; Turetken, O.; van den Heuvel, W.-J.; Papazoglou, M. (2010a): On the Formal Specification of Regulatory Compliance: A Comparative Analysis. In: Maximilien, E.M.; Rossi, G.; Yuan, S.-T.; Ludwig, H.; Fantinato, M. (Hrsg.): Proceedings of the International Workshops on Service Orientied Computing (ICSOC Workshops). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 27-38. (#)

Elgammal, A.; Turetken, O.; van den Heuvel, W.-J.; Papazoglou, M. (2010b): Root-Cause Analysis of Design-Time Violations on the Basis of Property Patterns. In: Maglio, P.P.; Weske, M.; Yang, J.; Fantinato, M. (Hrsg.): Proceedings of the 8th International Conference on Service Oriented Computing (ICSOC 2010), Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 17-31. (#)

El Kharbili, M.; de Medeiros, A.; Stein, S.; van der Aalst, W.M.P. (2008a): Business Process Compliance Checking: Current State and Future Challenges. In: Loos, P.; Nüttgens, M.; Turowski, K.; Werth, D. (Hrsg.): Modellierung betrieblicher Informationssysteme − Modellierung zwischen SOA und Compliance Management (MobIS 2008). Lecture Notes in Informatics (LNI), Saarbrücken, S. 107-113. (#)

El Kharbili, M.; Stein, S.; Markovic, I.; Pulvermüller, E. (2008b): Towards a Framework for Semantic Business Process Compliance Management. In: Sadiq, S.; Indulska, M.; zur Muehlen, M.; Franch, X.; Hunt, E.; Coletta, R. (Hrsg.): Proceedings of the 1st International Workshop on Governance, Risk and Compliance − Applications in Information Systems (GRCIS 2008). CEUR, Montpellier, S. 1-15. (#)

El Kharbili, M.; Stein, S.; Pulvermüller, E. (2008c): Policy-Based Semantic Compliance Checking for Business Process Management. In: Loos, P.; Nüttgens, M.; Turowski, K.; Werth, D. (Hrsg.): Proceedings of the Workshops colocated with the MobIS2008 conference: including EPK2008, KobAS2008 and ModKollGP2008. CEUR, Saarbrücken, S. 178-192. (#)

El Kharbili, M.; Pulvermüller, E. (2009): A Semantic Framework for Compliance Management in Business Process Management. In: Abramowicz, W.; Maciaszek, L.A.; Kowalczyk, R.; Speck, A. (Hrsg.): Business Process, Services Computing and Intelligent Service Management (BIS 2009). Lecture Notes in Informatics (LNI), S. 60-80. (#)

European Commission Health and Consumers Directorate (Hrsg., 2010): EudraLex. The Rules Governing Medicinal Products in the European Union. Volume 4 Good Manufacturing Practice Medicinal Products for Human and Veterinary Use. Annex 11: Computerised Systems. http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf, Abruf am 2015-03-19.

Faisst, U.; Buhl, H.-U. (2005): Integrated Enterprise Balancing mit integrierten Ertrags- und Risikodatenbanken. In: Wirtschaftsinformatik (47, 6), S. 403-412. (#)

Fayol, H. (1949): General and Industrial Management. Sir Isaac Pitman & Sons, London.

Feeny, D.F.; Willcocks, L.P. (1998): Core IS capabilities for exploiting information technology. In: MIT Sloan Management Review (39, 3), S. 9-21.

Ferstl, O.K.; Sinz, E.J. (1990): Objektmodellierung betrieblicher Informationssysteme im Semantischen Objektmodell. In: Wirtschaftsinformatik (32, 6), S. 566-581.

Ferstl, O.K.; Sinz, E.J. (1991): Ein Vorgehensmodell zur Objektmodellierung betrieblicher Informationssysteme im Semantischen Objektmodell (SOM). In: Wirtschaftsinformatik (33, 6), S. 477-491.

Ferstl, O.K.; Sinz, E.J. (1995): Der Ansatz des Semantischen Objektmodells (SOM) zur Modellierung von Geschäftsprozessen. In: Wirtschaftsinformatik (37, 3), S. 209-220.

Fettke, P. (2006a): State-of-the-Art des State-of-the-Art – Eine Untersuchung der Forschungsmethode "Review" innerhalb der Wirtschaftsinformatik. In: Wirtschaftsinformatik (46, 4), S. 257-266.

Fettke, P. (2006b): Referenzmodellevaluation – Konzeption der strukturalistischen Referenzmodellierung und Entfaltung ontologischer Gütekriterien. Logos-Verlag, Berlin, zugelassene Dissertation Johannes Gutenberg Universität.

Fettke, P. (2014): Eine Methode zur induktiven Entwicklung von Referenzmodellen. In: Suhl, L.; Kundisch, D. (Hrsg.): Tagungsband der Multikonferenz Wirtschaftsinformatik (MKWI 2014), Paderborn, S. 1034-1047.

Fettke, P.; Loos, P. (2002): Der Referenzmodellkatalog als Instrument des Wissensmanagements – Methodik und Anwendung. In: Becker, J.; Knackstedt, R. (Hrsg.): Wissensmanagement mit Referenzmodellen. Konzepte für die Anwendungssystem- und Organisationsgestaltung. Springer, Berlin et al., S. 3-23.

Fettke, P.; Loos, P. (2004a): Entwicklung eines Bezugsrahmens zur Evaluierung von Referenzmodellen – Langfassung eines Beitrages. In: Loos, P. (Hrsg.): Working Papers of the Research Group Information Systems & Management. Mainz.

Fettke, P.; Loos, P. (2004b): Referenzmodellierungsforschung. In: Working Papers of the Research Group Information Systems & Management, Universität Mainz, Mainz.

Fill, H.-G. (2012): An Approach for Analyzing the Effects of Risks on Business Processes Using Semantic Annotations. In: Proceedings of the 20th European Conference on Information System, (ECIS 2012). Barcelona, Paper 111. (#)

Fill, H.-G.; Gericke, A.; Karagiannis, D.; Winter, R. (2007): Modellierung für Integrated Enterprise Balancing. In: Wirtschaftsinformatik (49, 6), S. 419-429. (#)

Fishbein, M.; Ajzen, I. (1975): Belief, Attitude, Intention and Behavior − An Introduction to Theory and Research. Addison-Wesley, Massachusetts.

Fischer, C.; Winter, R.; Wortmann, F. (2010): Gestaltungstheorie. In: Wirtschaftsinformatik (52, 6), S. 382-386.

Flick, U. (2000): Qualitative Forschung. Theorie, Methoden, Anwendung in Psychologie und Sozialwissenschaften. 5. Auflage, Rowohlt, Reinbeck.

Flick, U.; von Kardorff, E.; Steinke, I. (2008): Qualitative Forschung: Ein Handbuch. 6. Auflage, Rowohlt, Reinbek.

Forrester, J.W. (1972): Grundzüge einer Systemtheorie. Gabler, Wiesbaden.

Frank, U. (1994): Multiperspektivische Unternehmensmodellierung: Theoretischer Hintergrund und Entwurf einer objektorientierten Entwicklungsumgebung. Oldenbourg, München.

Frank, U. (2002): Multi-perspective enterprise modeling (MEMO): Conceptual framework and modeling languages. In: Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS 2002). IEEE, S. 72-82.

Freeman, R.E. (1984): Strategic Management. A Stakeholder Approach. Pitman, Boston.

Frey, D.; Stahlberg, D.; Gollwitzer, P.M. (2001): Einstellung und Verhalten: Die Theorie des überlegten Handelns und die Theorie des geplanten Verhaltens. In Frey, D.; Irle, M. (Hrsg.): Theorien der Sozialpsychologie. Band I: Kognitive Theorien. 2. Auflage, Hans Huber, Bern et al., S. 361-398.

Fröhlich, M.; Glasner, K. (2007a): Aufbau einer zentralen Betriebsorganisation. In: Fröhlich, M.; Glasner, K. (Hrsg.): IT Governance. Leitfaden für eine praxisgerechte Implementierung. Gabler, Wiesbaden, S. 273-280.

Fröhlich, M.; Glasner, K. (2007b): IT Governance @ PwC. In: Fröhlich, M.; Glasner, K. (Hrsg.): IT Governance. Leitfaden für eine praxisgerechte Implementierung. Gabler, Wiesbaden, S. 273-280.

Fröhlich, M.; Glasner, K. (2007c): IT Governance bei einem IT-Service-Provider im Konzernverbund. In: Fröhlich, M.; Glasner, K. (Hrsg.): IT Governance. Leitfaden für eine praxisgerechte Implementierung. Gabler, Wiesbaden, S. 261-272.

Gartner (Hrsg., 2008): Survey Analysis: How Executives Use Business Metrics. Research Report, Gartner Corporation.

Gehrke, N., Thams, R. (2010): VAT Compliance. In: Schumann, M.; Kolbe, L.M.; Breitner, M.H.; Frerichs, A. (Hrsg.): Tagungsband der Multikonferenz Wirtschaftsinformatik 2010 (MKWI 2010), Universitätsverlag Göttingen, Göttingen, S. 569-581. (#)

Gericke, A.; Fill, H.-G.; Karagiannis, D.; Winter, R. (2009a): Situational Method Engineering for Governance, Risk and Compliance Information Systems. In: Proceedings of the International Conference on Design Science Research in Information Systems and Technology (DESRIST), Philadelphia, Article No. 24. (#)

Gericke, A.; Fill, H.-G.; Karagiannis, D.; Winter, R. (2009b): Method Engineering for Integrated Enterprise Balancing. In: Sadiq, S.; Indulska, M.; zur Muehlen, M.; Dubois, E.; Johannesson, P. (Hrsg.): Proceedings of the 2nd International Workshop on Governance, Risk and Compliance − Applications in Information Systems (GRCIS 2009), CEUR, Amsterdam. (#)

Gehlert, A.; Schermann, M.; Pohl, K.; Krcmar, H. (2009): Towards A Research Method For Theory-Driven Design Research. In: Hansen, H.R.; Karagiannis, D.; Fill, H.-G. (Hrsg.): Business Services: Konzepte, Technologien, Anwendungen. 9. Internationale Tagung Wirtschaftsinformatik. Österreichische Computer Gesellschaft, Wien, Band 1, S. 441-450.

Ghose, H.; Koliadis, G. (2007): Auditing business process compliance. In: Krämer, B.J.; Lin, K.J.; Narasimhan, P. (Hrsg.): Proceedings of the 5th International Conference on Service-Oriented Computing (ICSOC 2007). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al, S. 169-180. (#)

Gigerl, T.; Unger, C.; Baumgartner, C. (2007): Umsetzung eines integrierten IT-Compliance-Frameworks − am Beispiel ALTANA Pharma. In: Information Management & Consulting (22, 4), S. 70-77.

Gill, S.; Purushottam, U. (2008): Integrated GRC – Is your Organization Ready to Move? In: SETLabs Briefings (6, 3), S. 37-46. (#)

Gleißner, W. (2011): Grundlagen des Risikomanagements in Unternehmen. Controlling, Unternehmensstrategie und wertorientiertes Management. 2. Auflage, Vahlen, München.

Goedertier, S.; Vanthienen, J. (2006a): Business Rules for Compliant Business Process Models. In: Abramowicz, W.; Mayr, H.C. (Hrsg.): Proceedings of the 9th International Conference on Business Information Systems (BIS 2006). Lecture Notes in Informatics (LNI), Klagenfurt, S. 558-572. (#)

Goedertier, S.; Vanthienen, S. (2006b): Designing compliant business processes with obligations and permissions. In: Eder, J.; Dustdar, S. (Hrsg.): Business Process Management Workshops (BPM 2006 International Workshops). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 5-14. (#)

Goeken, M.; Knackstedt, R. (2008): Referenzmodellgestütztes Compliance Reporting am Beispiel der EU-Finanzmarktrichtlinie MiFID. In: HMD – Praxis der Wirtschaftsinformatik (45, 263), S. 47-57. (#)

Goeken, M.; Knackstedt, R. (2009): Multidimensionale Referenzmodelle zur Unterstützung des Compliancemanagements. Grundlagen – Sprache – Anwendung. In: Hansen, H.R.; Karagiannis, D.; Fill, H.-G. (Hrsg.): Business Services: Konzepte, Technologien, Anwendungen. 9. Internationale Tagung Wirtschaftsinformatik. Österreichische Computer Gesellschaft, Wien, Band 2, S. 359-368. (#)

Goeken, M.; Patas, J. (2010): Evidenzbasierte Strukturierung und Bewertung empirischer Forschung im Requirements Engineering. Grundlagen, Ordnungsrahmen, Forschungslandkarte. In: Wirtschaftsinformatik (52, 3), S. 173-184.

Goeken, M.; Patas, J. (2009): Wertbeitrag der IT als Gegenstand der IT-Governance und des IT-Controllings. In: Controlling (21, 12), S. 650-655.

Governatori, G; Milosevic, Z.; Sadiq, S. (2006): Compliance Checking between business processes and business contracts. In: Proceedings IEEE International Enterprise Distributed Object Computing Conference (EDOC 2006). IEEE, S. 221-232. (#)

Goo, J.; Yim, M.-S., Kim, D.J. (2012): A Path Way to Successful Management of Individual Intention to Security Compliance: A Role of Organizational Security Climate. In: Proceedings of the 45th Annual Hawaii International Conference on System Sciences (HICSS 2012). IEEE, S. 2959-2968. (#)

Goulding, C. (2002): Grounded Theory: A Practical Guide for Management, Business and Market Researchers. SAGE, London.

Götz, B.; Köhntopp, F.; Mayer, B.; Wagner, G. (2008): Einsatz einer ganzheitlichen GRC-Softwarelösung. In: HMD – Praxis der Wirtschaftsinformatik (45, 263), S. 89-98. (#)

Grant, G.; Brown, A.; Uruthirapathy, A.; McKnight, S. (2007): An Extended Model of IT Governance: A Conceptual Proposal. In: Proceedings of the 13th Americas Conference on Information Systems (AMCIS 2007). Keystone, Paper 215. (#)

Gregor, S. (2006): The nature of theory in information systems. In: MIS Quaterly (30, 3), S. 611-642.

Gregor, S.; Jones, D. (2007): The anatomy of a design. In: Journal of the Association for Information Systems (8, 5), S. 312-335.

Gresov, C.; Drazin, R. (1997): Equifinality: Functional equivalence in organization design. In: Academy of Management Review (22, 2), S. 403-428.

Grundei, J. (2006): Examining the Relationship between Trust and Control in Organizational Design: (How) Can Divergent Requirements be Reconciled? In: Burton, R.M.; Eriksen, B.; Hakonsson, D.D.; Snow, C.C. (Hrsg.): Organization Design: The Evolving State-of-the-Art. Springer, New York, S. 43-65. (#)

Grundei, J. (2008): Are managers agents or stewards of their principals? Logic, critique, and reconciliation of two conflicting theories of corporate governance. In: Journal für Betriebswirtschaft (58, 3), S. 141-166.

Grundei, J.; Talaulicar, T. (2009): Corporate Compliance. In: Wirtschaftswissenschaftliches Studium (38, 2), S. 73-77. (#)

Grünninger, S.; Jantz, M. (2013): Möglichkeiten und Grenzen der Prüfung von Compliance-Management-Systemen. In: Zeitschrift Corporate Governance (8, 3), S. 131-136. (#)

Guan, J.; Levitan, A.S. (2012): A Model for Investigating Internal Control Weaknesses. In: Communications of the Association for Information Systems (31, July, Article 3), S. 61-84. (#)

Guo, K.H.; Yuan, Y. (2012): The effects of multilevel sanctions on information security violations: A mediating model. In: Information and Management (49, 6), S. 320-326. (#)

Haghjoo, P. (2012): Towards a Better Understanding of How Effective IT Governance Leads to Business Value: A Literature Review and Future Research Directions. In: Proceedings of the Australian Conference on Information Systems (ACIS). Geelong. (#)

Hall, S.; Liedtka, S. (2007): The Sarbanes-Oxley Act: Implications for Large Scale IT-Outsourcing. In: Communications of the ACM (50, 3), S. 95-100. (#)

Harbrecht, W. (1993): Bedürfnis, Bedarf, Gut, Nutzen. In: Wittmann, W.; Kern, W.; Köhler, H.-U.M von Wysocki, K. (Hrsg.): Handwörterbuch der Betriebswirtschaft. 5. Auflage, Band 1, Schäffer-Poeschel, Stuttgart, S. 266-280.

Hardy, C.; Leonard, J. (2011): Governance, risk and compliance (GRC): Conceptual muddle and technological tangle. In: Proceedings of the Australian Conference on Information Systems (ACIS). Sydney, Paper 42. (#)

Hauschka, C. (2007): Handbuch der Haftungsvermeidung im Unternehmen. Beck, München. (#)

Haworth, D.; Pietron, I. (2006): Sarbanes-Oxley: Achieving Compliance by Starting with ISO 1799. In: Information Systems Management (23, 1), S. 73-87. (#)

Häder, M. (2000): Die Expertenauswahl bei Delphi-Befragungen. In: ZUMA How-to-Reihe, Nr. 5.

Häder, M. (2009): Delphi-Befragungen. Ein Arbeitsbuch. 2. Auflage, VS Verlag, Wiesbaden.

Heinrich, L.J.; Heinzl, A.; Rothmayr, F. (2007): Wirtschaftsinformatik. Einführung und Grundlegung. 3. Auflage, Oldenbourg, München et al.

Heinzl, A.; König, W.; Hack, J. (2001): Erkenntnisziele der Wirtschaftsinformatik in den nächsten drei und zehn Jahren. In: Wirtschaftsinformatik (43, 3), S. 223-233.

Henderson, J.C.; Sifonis, J.G. (1988): The value of strategic IS planning – understanding consistency, vaidity, and IS markets. In: MIS Quaterly (12, 2), S. 187-200.

Henderson, J.C.; Venkatraman, N. (1993): Strategic alignment: leveraging information technology for transforming organizations. In: IBM Systems Journal (32, 1), S. 4-16.

Hengmith, L. (2008): Management operationeller Risiken: eine Methode zur Modellierung und Simulation von Prozessen in Banken. Eul, Lohmar et al. (#)

Herath, T.; Rao, R. (2009): Protection motivation and deterrence: a framework for security policy compliance in organizations. In: European Journal of Information Systems (18, 2), S. 106-125. (#)

Herzwurm, G.; Stelzer, D. (2008): Wirtschaftsinformatik versus Information Systems – Eine Gegenüberstellung. In: Bankhofer, U.; Nissen, V.; Stelzer, D.; Straßburger, S. (Hrsg.): Ilmenauer Beiträge zur Wirtschaftsinformatik. Arbeitsbericht Nr. 2008-01, Januar 2008. Institut für Wirtschaftsinformatik, TU Ilmenau, Ilmenau.

Heumann, J.; Wiener, M. (2012): The Role of Formal Control in Facilitating Cultural Control. In: Proceedings of the 20th European Conference on Information System, (ECIS 2012). Barcelona, Paper 194. (#)

Hevner, A.R.; Chatterjee, S. (2010): Design Research in Information Systems: Theory and Practice. Springer, Berlin.

Hevner, A.R.; March, S.T.; Park, J.; Ram, S. (2004): Design science in information system research. In: MIS Quarterly (28, 1), S. 75-105.

Heydkamp, P.; Ostrowski, O. (2006): Compliance-Controlling bei IBM am Beispiel des Sarbanes-Oxley Act. In: von Werder, A.; Stöber, H.; Grundei, J. (Hrsg.): Organisations-Controlling – Konzepte und Praxisbeispiele. Gabler, Wiesbaden, S. 187-206.

Heym, M. (1993): Methoden-Engineering – Spezifikation und Integration von Entwicklungsmethoden für Informationssysteme. Dissertation, Universität St. Gallen.

Higgins, G.E.; Wilson, A.L.; Fell, B.D. (2005): An Application of Deterrence Theory to Software Piracy. In: Journal of Criminal Justice and Popular Culture (12, 3), S. 166-184.

Hoffmann, J.; Weber, I.; Governatori, G. (2012): On compliance checking for clausal constraints in annotated process models. In: Information Systems Frontiers (14, 2), S. 155-177. (#)

Horvath, P. (2011): Controlling. 12. Auflage, Vahlen, München.

Horvath, P. (2003): Das Controllingkonzept. Der Weg zu einem wirkungsvollen Controllingsystem. 5. Auflage, Verlag, München.

Houy, C.; Fettke, P.; Loos, P. (2009): Stilisierte Fakten der Ereignisgesteuerten Prozesskette – Anwendung einer Methode zur Theoriebildung in der Wirtschaftsinformatik. In: Nüttgens, M.; Rump, F.J.; Mendling, J.; Gehrke, N. (Hrsg.): Proceedings EPK 2009 Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten. CEUR, Berlin, S. 22-41.

Houy, C.; Fettke, P.; Loos, P. (2011): Stilisierte Fakten in der gestaltungsorientierten Wirtschaftsinformatik – Allgemeine Potentiale und erste Erfahrungen. In: Bernstein, A.; Schwabe, G. (Hrsg.): Proceedings of the 10th International Conference on Wirtschaftsinformatik (WI 2011), Zürich, Band 2, S. 1157-1166.

Houy, C.; Fettke, P.; Loos, P. (2014a): On the Theoretical Foundations of Research into the Understandability of Business Process Models. In: Proceedings of the 22nd European Conference on Information Systems (ECIS 2014). Tel Aviv.

Houy, C.; Frank, J.; Niesen, T.; Fettke, P.; Loos, P. (2014b): Zur Verwendung von Theorien in der Wirtschaftsinformatik – Eine quantitative Literaturanalyse. In: Loos, P. (Hrsg.): Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 198, Saarbrücken.

Houy, C.; Vella, A.-L.; Thaler, T.; Fettke, P.; Loos, P. (2013): Analyse des Qualitätsdiskurses zur Modellverständlichkeit in experimentellen Studien. In: Alt, R.; Franczyk, B. (Hrsg.): Proceedings of the 11th International Conference on Wirtschaftsinformatik (WI 2013). Leipzig, S. 1213-1227.

Hoyt, R.E.; Liebenberg, A.P. (2011): The Value of Enterprise Risk Management. In: Journal of Risk and Insurance (78, 4), S. 795-822. (#)

Hsu, C.W. (2009): Frame misalignment: interpreting the implementation of information systems security certification in an organization. In: European Journal of Information Systems (18, 2), S. 140-150. (#)

Hu, Q.; Dinev, T.; Hart, P. (2012): Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. In: Decision Sciences (43, 4), S. 615-660. (#)

Hu, Q.; Xu, Z.; Dinev, T.; Ling, H. (2011): Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? In: Communications of the ACM (54, 6), S. 54-60. (#)

Hu, Q.; Hart, P.; Looke, D. (2007): The role of external and internal influences on information security − a neo-institutional perspective. In: The Journal of Strategic Information Systems (16, 2), S. 153-172. (#)

Huff, A.; Tranfield, D.; Van Aken, J.E. (2006): Management as a design science mindful of art and surprise: A conversation between Anne Huff, David Tranfield, and Joan Ernst van Aken. In: Journal of Management Inquiry (15, 4), S. 413-424.

Hügens, T.; Zelewski, S. (2006): Eine Stakeholder-Analyse zur Ermittlung potentieller Perspektiven für das Beziehungsmanagement mithilfe der Balanced Scorecard. In: Wirtschaftswissenschaftliches Studium (35, 7), S. 368-373.

Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW, Hrsg., 2010): Entwurf IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW EPS 980) Stand: 11.03.2010. Düsseldorf. (#)

Institute of Electrical and Electronics Engineers (IEEE, Hrsg., 2000): IEEE 1471-2000 IEEE Recommended Practice for Architectural Description of Software-Intensive Systems – Description.

International Organization for Standardization (ISO, Hrsg., 2007) ISO/IEC 42010:2007 Systems and software engineering – Recommended practice for architectural description of software-intensive systems.

International Organization for Standardization, International Electrotechnical Commission (ISO, IEC, Hrsg., 2008): Corporate Governance of information technology. (#)

International Society for Pharmaceutical Engineering (ISPE, Hrsg., 2008): GAMP 5. A risk-based approach to compliant GxP computerized systems. 2008.

ISACA (Hrsg., 2009): The Risk IT Framework. ISACA, Rolling Meadows.

Isensee, J. (2008): Compliance-Controlling. In: Controlling (20, 3), S. 161-162. (#)

Jacobson, D.D. (2009): Revisiting IT Governance in the Light of Institutional Theory. In: Proceedings of the 42nd Annual Hawaii International Conference on System Sciences (HICSS 2009). IEEE, S. 1-9. (#)

Janisch, M. (1992): Das strategische Anspruchsgruppenmanagement. Von Shareholder Value zum Stakeholder Value. St. Gallen.

Jensen, M.C.; Meckling, W.H. (1976): Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. In: Journal of Financial Economics (3, 4), S. 305-360.

Joachim, B. (2006): Umsetzung der Anforderungen hinsichtlich »rechnungsrelevanter Aussagen« bei E.ON. In: Menzies, C. (Hrsg.): Sarbanes-Oxley und Corporate Compliance: Nachhaltigkeit, Optimierung, Integration. Schäffer-Poeschel, Stuttgart, S. 442-449.

Johannsen, W.; Goeken, M. (2006): IT-Governance − neue Aufgaben des IT-Managements. In: HMD – Praxis der Wirtschaftsinformatik (43, 250), S. 7-20. (#)

Johnson, C.M.; Grandison, T.W.A. (2007): Compliance with data protection laws using Hippocratic Database active enforcement and auditing. In: IBM Systems Journal (46, 2), S. 255-264. (#)

Johnston, A.C.; Warkentin, M. (2010): Fear Appeals and Information Security Behaviors: An Empirical Study. In: MIS Quarterly (34, 3), S. 548-566. (#)

Johnston, A.C.; Welch, B.; Jack, E.; Beavers, M. (2010): Reigning in the Remote Employee: Applying Social Learning Theory to Explain Information Security Policy Compliance. In: Proceedings of the 16th Americas Conference on Information Systems (AMCIS 2010). Lima, Paper 493. (#)

Jörges-Süß, K.; Süß, S. (2004): Neo-Institutionalistische Ansätze in der Organisationstheorie. In: WISU – Das Wirtschaftsstudium (33, 3), S. 316-318.

Jost, P.J. (2001): Der Transaktionskostenansatz in der Betriebswirtschaftslehre. Schaeffer-Poeschel, Stuttgart.

Julisch, K. (2008): Security Compliance: the next frontier in security research. In: Proceedings of the 2008 workshop on new security paradigms. ACM, New York, S. 71-74. (#)

Just, D.; Tami, F. (2007): Praxisbeispiel: Bewertung von Applikationsportfolios und IT-Prozessen. In: Johannsen, W.; Goeken, M. (Hrsg.): Referenzmodelle für IT-Governance. Strategische Effektivität und Effizienz mit COBIT, ITIL & Co. Dpunkt.verlag, Heidelberg, S. 225-242.

Kajüter, P. (2001): Der Entwurf DRS 5 zur Risikoberichterstattung. In: Die Wirtschaftsprüfung (54, 4), S. 205-209.

Karagiannis, D. (2008): A business process-based modelling extension for regulatory compliance. In: Bichler, M.; Hess, T.; Krcmar, H.; Lechner, U.; Matthes, F.; Picot, A.; Speitkamp, B.; Wolf, P. (Hrsg.): Tagungsband der Multikonferenz Wirtschaftsinformatik (MKWI 2008). GITO-Verlag, Berlin, S. 1159-1173. (#)

Karanja, E.; Zaveri, J. (2012): Effect of the SOX Act on IT Governance. In: Proceedings of the 18th Americas Conference on Information Systems (AMCIS 2012). Seattle, Paper 3. (#)

Kasi, V.; Keil, M.; Mathiassen, L.; Pedersen, K. (2008): The post mortem paradox: a Delphi study of IT specialist perceptions. In: European Journal of Information Systems (17), S. 62-78.

Kasiri, N.; Sharda, R.; Hardgrave, B. (2012): A balanced scorecard for item level RFID in the retail sector: a Delphi study. In: European Journal of Information Systems (21), S. 255-267.

Keill, M.; Tiwana, A.; Bush, A. (2002): Reconciling User and Project Manager Perceptions of IT Project Risk: A Delphi Study. In: Information Systems Journal (12, 2), S. 103-119.

Keller, G.; Nüttgens, M.; Scheer, A-W. (1992): Semantische Prozeßmodellierung auf der Grundlage "Ereignisgesteuerter Prozeßketten (EPK)". In: Scheer, A.-W. (Hrsg.): Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 89, Saarbrücken.

Kim, H.M.; Fox, M.S.; Sengupta, A. (2007): How to Build Enterprise Data Models to Achieve Compliance to Standards or Regulatory Requirements (and share data). In: Journal of the Association for Information Systems (8, 2), S. 105-128. (#)

Kitchenham B.A., Brereton O.P., Budgen D., Turner, M., Bailey J., Linkman S. (2009): Systematic literature reviews in software engineering – a systematic literature review. In: Information and Software Technology (51, 1), S. 7-15.

Kittel, K. (2013): Agilität von Geschäftsprozessen trotz Compliance. In: Alt, R.; Franczyk, B. (Hrsg.): Proceedings of the 11th International Conference on Wirtschaftsinformatik (WI 2013). Leipzig, S. 967-981. (#)

Kittel, K.; Sackmann, S.; Betke, H.; Hofmann, M. (2013): Achieving Flexible and Compliant Processes in Disaster Management. In: Proceedings of the 46th Annual Hawaii International Conference on System Sciences (HICSS 2013). IEEE, S. 4687-4696. (#)

Kley, W.-D. (2011): Risiko- und Chancenmanagement der MAN SE. In: Zeitschrift für Controlling & Management (55, 2), S. 105-110.

Kloos, O. (2014): Generierung von Simulationsmodellen auf der Grundlage von Prozessmodellen. Dissertation. ilmedia, Ilmenau.

Klotz, M. (2007): IT-Compliance – auf den Kern reduziert. In: IT-Governance (1, 1), S. 14-18.

Klotz, M. (2009): IT-Compliance. Ein Überblick. Dpunkt, Heidelberg. (#)

Klotz, M.; Dorn, D.-W. (2008): IT-Compliance – Begriff, Umfang und relevante Regelwerke. In: HMD – Praxis der Wirtschaftsinformatik (45, 263), S. 5-14. (#)

Kluckhohn, C. (1962): Values and value-orientation in the theory of action. In: Parson, T.; Shils E. (Hrsg): Toward a General Theory of action. Harvard University Press, Cambridge.

Knolmayer, G. (2007): Compliance-Nachweise bei Outsourcing von IT-Aufgaben. In: Wirtschaftsinformatik (49, Sonderheft), S. 98-106. (#)

Kosiol, E. (1976): Organisation der Unternehmung. 2. Auflage, Gabler, Wiesbaden.

König, W.; Heinzl, A.; von Poblotzki, A. (1995): Die zentralen Forschungsgegenstände der Wirtschaftsinformatik in den nächsten zehn Jahren. In: Wirtschaftsinformatik (37, 6), S. 558-569.

Kranawetter, M. (2009): Nutzenpotentiale regulatorischer Anforderungen zur Geschäftsoptimierung. IT-Infrastruktur Compliance Reifegradmodell für Geschäftsführung, Compliance und IT-Verantwortliche. Microsoft.
http://download.microsoft.com/download/D/5/8/D58EEC38-FBAC-42BC-9C3C-C88C042103DE/IT_Infrastruktur_Compliance_Reifegradmodell_Microsoft_Kranawetter.pdf, Abruf am 2015-05-15. (#)

Krcmar, H.; Wiesche, M.; Schermann, M.; Grau, A.; Lauth, A. (2011): Governance, Risikomanagement und Compliance: Erfolg durch transparente Unternehmensführung. In: Information Management and Consulting (26, 3), S. 6-11. (#)

Krell, K.; Matook, S. (2008): On the Impact of Strategic Planning on Mandatory IS Investments. In: Proceedings of the 14th Americas Conference on Information Systems (AMCIS 2008). Toronto, Paper 289. (#)

Krell, K.; Matook, S. (2009): Competitive advantage from mandatory investments: An empirical study of Australian firms. In: The Journal of Strategic Information Systems (18, 1), S. 31-45. (#)

Krell, K.; Matook, S.; Rohde, F. (2009): The effects of regulatory pressure on information system adoption success: An institutional theory perspective. In: Proceedings of the 17th European Conference on Information System, (ECIS 2009). Verona, Paper 402. (#)

Kremer, M.; Haase, M. (2011): ITK-Governance bei der Deutschen Bahn AG. In: IT-Governance (5, 9), S. 14-20.

Krey, M. (2010): Information Technology Governance, Risk and Compliance in Health Care − A Management Approach. In: Proceedings Developments in E-systems Engineering (DESE), S. 7-11. (#)

Krey, M. (2012): Entwicklung einer Methode zur Umsetzung von IT Governance, Risk Management und Compliance im Krankenhaus. In: Goltz, U.; Magnor, M.; Appelrath, H.-J.; Mathies, H.; Balke, W.-T.; Wolf, L. (Hrsg.): INFORMATIK 2012: Was bewegt uns in die Zukunft. Lecture Notes in Informatics (LNI), Braunschweig, S. 1602-1618. (#)

Krey, M.; Furnell, S.; Harriehausen, B.; Knoll, M. (2012): Approach to the Evaluation of a Method for the Adoption of Information Technology Governance, Risk Management and Compliance in the Swiss Hospital Environment. In: Proceedings of the 45th Annual Hawaii International Conference on System Sciences (HICSS 2012). IEEE, S. 2810-2819. (#)

Krey, M.; Harriehausen, B.; Knoll, M. (2011): Approach to the Classification of Information Technology Governance, Risk and Compliance Frameworks. In: Proceedings of the International Conference on Modelling and Simulation (UKSim). S. 350-354. (#)

Krippendorff, K. (2004): Content analysis: an introduction to its methodology. SAGE, Beverly Hills et al.

Krippendorff, K.; Bock, M.A. (2009): The Content Analysis Reader. SAGE, Los Angeles et al.

Kronschnabl, S.A. (2010): Konzeption eines Modells zur Bestimmung des optimalen Investitionsbeitrags in IT-Sicherheits- bzw. IT-Notfallmaßnahmen unter Berücksichtigung Compliance-bedingter Anforderungen. In: Schumann, M.; Kolbe, L.M.; Breitner, M.H.; Frerichs, A. (Hrsg.): Tagungsband der Multikonferenz Wirtschaftsinformatik 2010 (MKWI 2010). Universitätsverlag Göttingen, Göttingen, S. 2181-2192. (#)

Kruskal, W.H.; Wallis, W.A. (1952): Use of ranks in one-criterion variance analysis. In: Journal of the American Statistical Association (47, 260), S. 583-621.

Kudo, M.; Arako, Y.; Nomiyama, H.; Saito, S.; Sohda, Y. (2007): Best practices and tools for personal information compliance management. In: IBM Systems Journal (46, 2), S.235-253. (#)

Kuhlin, B; Thielmann, H. (Hrsg., 2005): Real-Time Enterprise in der Praxis: Fakten und Ausblick. Springer, Berlin et al.

Kurz, E.; Woltering, A. (2008): ITK-Governance bei der Deutschen Bahn – nachhaltige ITK Steuerung im Vorstandsressort Personenverkehr. In: IT-Governance (2, 3), S. 3-8.

Küster, J.; Ryndina, K.; Gall, H. (2007): Generation of business process models for object life cycle compliance. In: Alonso, G.; Dadam, P.; Rosemann, M. (Hrsg.): Business Process Management: Proceedings of the 5th International Conference on Business Process Management (BPM 2007). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al, S. 165-181. (#)

Kwon, J.; Johnson, M.E. (2013): Healthcare Security Strategies for Regulatory Compliance and Data Security. In: Proceedings of the 46th Annual Hawaii International Conference on System Sciences (HICSS 2013). IEEE, S. 3972-3981. (#)

Lange, C. (2005): Ein Bezugsrahmen zur Beschreibung von Forschungsgegenständen und -methoden in Wirtschaftsinformatik und Information Systems. ICB-Research Report No. 1, Universität Duisburg-Essen.

Lange, D. (2008): A Multidimensional Conceptualization of Organizational Corruption Control. In: Academy of Management Review (33, 3), S. 710-729. (#)

Lankhorst, M. (2005): Enterprise Architecture at Work: Modelling, Communication and Analysis. Springer, Berlin et al.

Latour, B. (2005): Reassembling the Social: An Introduction to Actor-Network-Theory. USA, Oxford University Press, New York.

Lazic, M.; Groth, M.; Schillinger, C.; Heinzl, A. (2011): The Impact of IT Governance on Business Performance. In: Proceedings of the 17th Americas Conference on Information Systems (AMCIS 2011). Detroit, Paper 189. (#)

Lebek, B.; Uffen, J.; Breitner, M.H.; Neumann, M.; Hohler, B. (2013): Employees' Information Security Awareness and Behavior: A Literature Review. In: Proceedings of the 46th Annual Hawaii International Conference on System Sciences (HICSS 2013). IEEE, S. 2978-2987. (#)

Lederer, A.L.; Salmela, H. (1996): Toward a theory of strategic information systems planning. In: The Journal of Strategic Information Systems (5, 3), S. 237-253.

Lederer, A.L.; Sethi, V. (1988): The implementation of strategic information-systems planning methodologies. In: MIS Quarterly (12, 3), S. 445-461.

Lehner, F.; Hildebrand, K.; Maier, R. (1995): Wirtschaftsinformatik: Theoretische Grundlagen. Hanser, Wien.

Leih, M. (2006a): The Impact of the Sarbanes-Oxley Act on IT Project Management. In: Journal of Information Technology Theory and Application (8, 3), 13-30. (#)

Leih, M. (2006b): IT Governance and the Sarbanes-Oxley Act. In: Proceedings of the 12th Americas Conference on Information Systems (AMCIS 2006). Acapulco. (#)

Leih, M. (2007): Regulatory Impact on IT Governance: A Multiple Case Study on the Sarbanes-Oxley Act. In: Proceedings of the 13th Americas Conference on Information Systems (AMCIS 2007). Keystone, Paper 399. (#)

Leon, L.; Kalbers, L.; Coster, N.; Abraham, D. (2012): A spreadsheet life cycle analysis and the impact of Sarbanes-Oxley. In: Decision Support Systems (54, 1), S. 452-460. (#)

Leontiadis, M.; Tezel, A. (1980): Planning Perceptions and Planning Results. In: Strategic Management Journal (1, 1), S. 65-79.

Levy, M., Ellis, T.J. (2006): A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. In: Informing Science Journal (9, January), S. 181-212.

Li, C.; Peters, G.F.; Richardson, V.J.; Watson, M.W. (2012): The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Control Reports. In: MIS Quarterly 36 (2012) 1, S. 179-203. (#)

Li, C.; Richardson, V.J.; Peters, G.F.; Watson, M. (2010): The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Reports. In: Proceedings of the 16th Americas Conference on Information Systems (AMCIS 2010). Lima, Paper 8. (#)

Liang, T.-P.; Chiu, Y.-C.; Wu, S.P.J.; Straub, D. (2011): The Impact of IT Governance on Organizational Performance. In: Proceedings of the 17th Americas Conference on Information Systems (AMCIS 2011). Detroit, Paper 268. (#)

Liang, H.; Xue, Y.; Wu, L. (2013): Ensuring Employees' IT Compliance: Carrot or Stick? In: Information Systems Research (24, 2), S. 279-294. (#)

Liang, T.P.; You, J.J. (2009): Resource-based View in Information Systems Research: A Meta-Analysis. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Hyderabad.

Lim, S.; Saldanha, T.; Malladi, S.; Melville, N.P. (2009): Theories Used in Information Systems Research: Identifying Theory Networks in Leading IS Journals. In: Proceedings of the 30th International Conference on Information Systems (ICIS 2009). Phoenix, Paper 91.

Lim, S.; Saldanha, T.J.V.; Malladi, S.; Melville, N.P. (2013): Theories Used in Information Systems Research: Insights from Complex Network Analysis. In: Journal of Information Technology Theory and Application (14, 2), S. 5-46.

Lincoln, Y.S.; Guba, E.G. (1985): Naturalistic inquiry. SAGE, Beverly Hills.

Linstone, H.A.; Turoff, M. (1975): The Delphi method: techniques and applications. Reading, MA: Addison-Wesley.

Liu, Y.; Müller, S.; Xu, K. (2007): A static compliance-checking framework for business process models. In: IBM Systems Journal (46, 2), S. 335-362. (#)

Loh, L.; Venkatraman, N. (1992): Determinants of Information Technology Outsourcing: A Cross-Sectional Analysis. In: Journal of Management Information Systems (9, 1), S. 7-24.

Lohmann, N. (2011): Compliance by design for artifact-centric business processes. In: Rinderle-Ma, S.; Toumani, F.; Wolf, K. (Hrsg.): Business Process Management: Proceedings of the 9th International Conference on Business Process Management (BPM 2011). Lecture Notes in Computer Science (LNCS), Spriner, Berlin et al, S. 99-115. (#)

Lohmann, N. (2013): Compliance by design for artifact-centric business processes. In: Information Systems (38, 4), S. 606-618. (#)

Lohre, T. (2009): Beitrag der Internen Revision zur IT-Compliance. In: Zeitschrift für Interne Revision (44, 4), S. 179-189. (#)

Loosli, G. (2008): Compliance-Prüfung bei der Anwendung dynamischer Bindung in service-orientierten Architekturen. In: Loos, P.; Nüttgens, M.; Turowski, K.; Werth, D. (Hrsg.): Modellierung betrieblicher Informationssysteme – Modellierung zwischen SOA und Compliance Management (MobIS 2008). Lecture Notes in Informatics (LNI), Saarbrücken, S. 7-21. (#)

Lorange, P. (1980): Corporate Planning. Prentice-Hall, Englewood Cliffs.

Lotz, V.; Pigout, E.; Fischer, P.; Kossmann, D.; Massacci, F.; Pretschner, A. (2008): Towards Systematic Achievement of Compliance in Service-Oriented Architectures: The Master Approach. In: Wirtschaftsinformatik (50, 5), S. 383-391. (#)

Lowis, L. (2008): Towards Automated Risk Identification in Service-Oriented Architectures. In: Bichler, M.; Hess, T.; Krcmar, H.; Lechner, U.; Matthes, F.; Picot, A.; Speitkamp, B.; Wolf, P. (Hrsg.): Tagungsband der Multikonferenz Wirtschaftsinformatik (MKWI 2008). GITO-Verlag, Berlin. (#)

Lowry, P.B.; Moody, G.D. (2013): Explaining Opposing Compliance Motivations towards Organizational Information Security Policies. In: Proceedings of the 46th Annual Hawaii International Conference on System Sciences (HICSS 2013). IEEE, S. 2998-3007. (#)

Lu, R.; Sadiq, S.; Governatori, G. (2007): Compliance Aware Business Process Design. In: Hofstede, A.; Benatallah, B.; Paik, H.-Y. (Hrsg.): Business Process Management Workshops (BPM 2007 International Workshops). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 211-220. (#)

Lu, R.; Sadiq, S.; Governatori, G. (2009): Measurement of Compliance Distance in Business Processes. In: Information Systems Management (25, 4), S. 344-355. (#)

Ly, L.T.; Rinderle-Ma, S.; Göser, K.; Dadam, P. (2012): On enabling integrated process compliance with semantic constraints in process management systems. In: Information Systems Frontiers (14, 2), S. 195-219. (#)

MacLean, T.; Behnam, M. (2010): The Dangers of Decoupling: The Relationship between Compliance Programs, Legitimacy Perceptions, and Institutionalized Misconduct. In: The Academy of Management Journal (53, 6), S. 1499-1520. (#)

MacNeil, I.R. (1974): The many futures of contracts. In: Southern California Law Review (47, 3), S. 691-816.

MacNeil, I.R. (1978): Contracts: Adjustments of long-term economic relations under classical, neoclassical and relational contract law. In: Northwestern University Law Review (72, 1), S. 854-905.

MacNeil, I.R. (1987): Relational contract theory as sociology: A reply to Professors Lindenberg and de Vos. In: Journal of Institutional and Theoretical Economics (143), S. 272-290.

Maheshwari, B.; Pollanen, R.; Kumar, V. (2009): Contrasting Information Systems and Financial Executive Perspective on Implementing Regulatory Controls. In: Proceedings of the 15th Americas Conference on Information Systems (AMCIS 2009). San Francisco, Paper 401. (#)

Malik, F. (2009): Systemisches Management, Evolution, Selbstorganisation. Grundprobleme, Funktionsmechanismen und Lösungsansätze für komplexe Systeme. 5. Auflage, Haupt, Bern et al.

Mallin, C.A. (2007): Corporate Governance. 2. Auflage, Oxford University, Oxford.

Mann, F. (2009): Die Diffusionstheorie. In: Schwaiger, M.; Meyer, A. (Hrsg.): Theorien und Methoden der Betriebswirtschaft. Vahlen, München, S. 97-114.

March, S.T.; Smith, G.F. (1995): Design and Natural Science Research on Information Technology. In: Decision Support Systems (15, 4), S. 251-266.

Marekfia, W.; Nissen, V. (2009): Strategisches GRC-Management – Grundzüge eines konzeptionellen Bezugsrahmens. In: Nissen, V. (Hrsg.): Reihe Forschungsberichte zur Unternehmensberatung, Forschungsbericht Nr. 2009-02.

Marekfia, W.; Nissen, V. (2012): Anforderungen an ein strategisches GRC-Management. In: Goltz, U.; Magnor, M.; Appelrath, H.-J.; Mathies, H.; Balke, W.-T.; Wolf, L. (Hrsg.): INFORMATIK 2012: Was bewegt uns in die Zukunft. Lecture Notes in Informatics (LNI), Braunschweig, S. 731-745.

Marekfia, W.; Nissen, V. (2013): Entwicklung eines fachkonzeptionellen Referenzmodells für ein strategisches GRC-Management. In: Horbach, M. (Hrsg.): INFORMATIK 2013 Informatik angepasst an Mensch, Organisation und Umwelt. Lecture Notes in Informatics (LNI), S. 1216-1230.

Marekfia, W.; Nissen, V. (2014): Strategisches GRC-Management – Anforderungen und datenseitiges Referenzmodell. In: HMD – Praxis der Wirtschaftsinformatik (51, 3), S. 228-239.

Marinos, L.; Kirchner, L.; Junginger, S. (2009): Integration of an IT-Risk Management / Risk Assessment Framework with Operational Processes. In: Hansen, H.R.; Karagiannis, D.; Fill, H.-G. (Hrsg.): Business Services: Konzepte, Technologien, Anwendungen. 9. Internationale Tagung Wirtschaftsinformatik. Österreichische Computer Gesellschaft, Wien, Band 1, S. 367-376. (#)

Martens, B.; Teuteberg, F. (2009): Why Risk Management Matters in IT Outsourcing – A Systematic Literature Review and Elements of a Research Agenda. In: Proceedings of the 17th European Conference on Information Systems (ECIS 2009). Verona, Paper 164.

Martens, B.; Teuteberg, F. (2011): Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model. In: Proceedings of the 17th Americas Conference on Information Systems (AMCIS 2011). Detroit, Paper 228. (#)

Masli, A.; Peters, G.F.; Richardson, V.J.; Sanchez, J.M. (2010): Examing the Potential Benefits of Internal Control Monitoring Technology. In: The Accounting Review (85, 3), S. 1001-1034. (#)

Mayring, P. (1993): Einführung in die qualitative Sozialforschung. 2. Auflage, Beltz, Weinheim.

Mayring, P. (2008): Qualitative Inhaltsanalyse. Grundlagen und Techniken. 10. Auflage, Beltz, Weinheim et al.

McCarthy, B. (2002): New Economics of Sociological Criminology. In: Annual Review of Sociology (28, 1), S. 417-442.

McFarlan, F.W.; McKenney, J.L.; Pyburn, P. (1983): The information archipelago – plotting a course. In: Harvard Business Review (61, 1), S. 145-156.

Md Khan, K. (2007): Selecting Web Services with Security Compliances: A Managerial Perspective. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS). Auckland. (#)

Mei, L.; Chan, W.K.; Tse, T.H. (2008): A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues. In: Proceedings of the IEEE Asia-Pacific Services Computing Conference. IEEE, Yilan, S. 464-469.

Meise, V. (2000): Ordnungsrahmen zur prozessorientierten Organisationsgestaltung: Modelle für das Management komplexer Reorganisationsprojekte. Kovac, Hamburg, zugelassene Dissertation Universität Münster.

Melarkode, A.; Fromm-Poulsen, M.; Warnakulasuriya, S. (2004): Delivering agility through IT. In: Business Strategy Review (15, 3), S. 45-50.

Melnyk, S.; Burns, L.; Lummus, R.; Vokurka, R.; Santor, J. (2009): Mapping the future of supply chain management: a Delphi study. In: International Journal of Production Research (47, 16), S. 4629-4653.

Melville, N., Kraemer, K.; Gurbaxani, V. (2004): Review: Information Technology and Organizational Performance: An Integrative Model of IT Business Value. In: MIS Quarterly (28, 2), S. 283-322.

Menzies, C. (Hrsg., 2006): Sarbanes-Oxley und Corporate Compliance – Nachhaltigkeit, Optimierung, Integration. Schäffer-Poeschel, Stuttgart. (#)

Menzies, C.; Tüllner, J.; Martin, A. (2008): Compliance Management: Nachhaltige Umsetzung in der Praxis. In: Zeitschrift für Führung und Organisation (77, 3), S. 136-142. (#)

Mertens, P. (1995): Wirtschaftsinformatik: Von den Moden zum Trend. In: König, W. (Hrsg.): Wirtschaftsinformatik '95. Wettbewerbsfähigkeit, Innovation, Wirtschaftlichkeit. Physica, Heidelberg, S. 25-64.

Mertens, P.; Bodendorf, F.; König, W.; Picot, A.; Schumann, M.; Hess, T. (2012): Grundzüge der Wirtschaftsinformatik. 11. Auflage, Springer, Berlin et al.

Meyer, J.W.; Rowan, B. (1977): Institutionalized organizations: Formal structure as myth and ceremony. In: American Journal of Sociology (83, 2), S. 340-363.

Meyer, J.; Teuteberg, F. (2012): Nachhaltiges Geschäftsprozessmanagement – Status Quo und Forschungsagenda. In: Mattfeld, D.C.; Robra-Bissantz, S. (Hrsg.): Tagungsband der Multikonferenz der Wirtschaftsinformatik (MKWI 2012). GITO-Verlag, Braunschweig, S. 1515-1529.

Morgenthaler Michels, T.; Krzeminska, A. (2006): Sarbanes-Oxley Act und Six Sigma als Instrumente des Prozess-Controllings bei der AXA Konzern AG. In: von Werder, A.; Stöber, H.; Grundei, J. (Hrsg.): Organisations-Controlling – Konzepte und Praxisbeispiele. Gabler, Wiesbaden, S. 135-151.

Milicevic, D.; Goeken, M. (2010): Konzepte der Informationssicherheit in Standards am Beispiel der ISO 27001. In: Fähnrich, K.-P.; Franczyk, B. (Hrsg): INFORMATIK 2010 Service Science – Neue Perspektiven für die Informatik Band 2. Lectures Notes in Informatics (LNI), Leipzig, S. 305-310. (#)

Milicevic, D.; Goeken, M. (2012): Strukturierung empirischer Evidenz im Informationssicherheitsmanagement. In: Goltz, U.; Magnor, M.; Appelrath, H.-J.; Mathies, H.; Balke, W.-T.; Wolf, L. (Hrsg.): INFORMATIK 2012: Was bewegt uns in die Zukunft. Lecture Notes in Informatics (LNI), Braunschweig, S. 774-788. (#)

Milicevic, D.; Goeken, M. (2013a): Social Factors in Policy Compliance – Evidence Found in Literature to Assist the Development of Policies in Information Security Management. In: Proceedings of the 46th Annual Hawaii International Conference on System Sciences (HICSS 2013), IEEE, S. 4476-4484. (#)

Milicevic, D.; Goeken, M. (2013b): Systematic Review and Meta-Analysis of IS Security Policy Compliance Research. First Steps towards Evidence-Based Structuring of the IS Security Domain. In: Alt, R.; Franczyk, B. (Hrsg.): Proceedings of the 11th International Conference on Wirtschaftsinformatik (WI 2013). Leipzig, S. 1067-1082. (#)

Miller, G. A. (1956): The Magical Number Seven, Plus Or Minus Two: Some Limits On Our Capacity For Processing Information. In: The Psychological Review (63, 2), S. 81-97.

Mingers, J. (2001): Combining IS Research Methods: Towards a Pluralist Methodology. In: Information Systems Research (12, 3), S. 240-259.

Mintzberg, H. (1978): Patterns in strategy formation. In: Management Science (24, 9), S. 934-948.

Mintzberg, H.; McHugh, A. (1985): Strategy formation in adhocracy. In: Administrative Science Quarterly (30, 2), S. 160-197.

Mishra, S.; Weistroffer, H.R. (2007): A Framework for Integrating Sarbanes-Oxley Compliance into the System Development Process. In: Communications of the Association for Information Systems (20, Article 44), S. 712-727. (#)

Mitroff, I. (1983): Stakeholders of the Organizational Mind. Jossey-Bass, San Francisco et al.

Morgenthaler, M. (2011): Datenschutzmanagementsystem im Active Global Support der SAP AG. In: IT-Governance (5, 10), S. 18-20.

Mossanen, K. (2010): Compliance im IT-Outsourcing. Ermittlung diskriminierender Einflussfaktoren und Entwicklung von Gestaltungsempfehlungen. Kovac, Hamburg. (#)

Mossanen, K.; Amberg, M. (2008): IT-Outsourcing & Compliance. In: HMD – Praxis der Wirtschaftsinformatik (45, 263), S. 58-68. (#)

Mossanen, K.; Panitz, J.C.; Amberg, M. (2010): Compliance im IT-Outsourcing. In: Schumann, M.; Kolbe, L.M.; Breitner, M.H.; Frerichs, A. (Hrsg.): Proceedings der Multikonferenz Wirtschaftsinformatik 2010 (MKWI 2010). Universitätsverlag Göttingen, Göttingen, S. 179-192. (#)

Mucic, L. (2006): Vom Projekt zum Prozess am Beispiel der SAP AG – Nachhaltigkeit und Mehrwert der unternehmensinternen SOX-Compliance Anstrengungen sichern. In: Menzies, C. (Hrsg.): Sarbanes-Oxley und Corporate Compliance: Nachhaltigkeit, Optimierung, Integration. Schäffer-Poeschel, Stuttgart, S. 450-460.

Musson, D.; Jordan, E. (2006): The benefits of IT governance. In: Proceedings of the 14th European Conference on Information System, (ECIS 2006). Helsinki, Paper 48. (#)

Müller, C. (1995): Agency-Theorie und Informationsgehalt. In: Betriebswirtschaft (55, 1), S. 61-76. (#)

Müller, G. (2007): Für Sie gelesen. In: Wirtschaftsinformatik (49, Sonderheft), S. 107-109.

Müller, R.M.; Linders, S.; Pires, L.F. (2010): Business Intelligence and Service-oriented Architecture: A Delphi Study. In: Information Systems Management (27, 2), S. 168-187.

Murphy, M.K.; Black, N.A.; Lamping, D.L.; McKee, C.M.; Sanderson, C.F.B, Askham, J.; Marteau, T. (1998): Consensus development methods, and their use in clinical guideline development. In: Health Technology Assessment (2, 3), S. 1-88.

Myyry, L.; Siponen, M.; Pahnila, S.; Vartiainen, T.; Vance, A. (2009): What levels of moral reasoning and values explain adherence to information security rules? An empirical study. In: European Journal of Information Systems (18, 2), S. 126-139. (#)

Nakatsu, R.T.; Iacovou, C.L. (2009): A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study. In: Information & Management (46, 1), S. 57-68.

Namiri, K.; Stojanovic, N. (2007a): A Semantic-based Approach for Compliance Management of Internal Controls in Business Process Management. In: Eder, J.; Tomassen, S.L.; Opdahl, A.; Sindre, G. (Hrsg.): Proceedings of the CAiSE'07 Forum at the 19th International Conference on Advanced Information Systems Engineering (CAISE 2007 Forum). CEUR, Trondheim, S. 61-64. (#)

Namiri, K.; Stojanovic, N. (2007b): Pattern-based design and validation of business process compliance. In: Meersmann, R.; Tari, Z. (Hrsg.): On the Move to Meaningful Internet Systems 2007: Confederated International Conferences (Part 1). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 59-76. (#)

Namiri, K.; Stojanovic, N. (2008): Towards A Formal Framework For Business Process Compliance. In: Bichler, M.; Hess, T.; Krcmar, H.; Lechner, U.; Matthes, F.; Picot, A.; Speitkamp, B.; Wolf, P. (Hrsg.): Tagungsband der Multikonferenz Wirtschaftsinformatik (MKWI 2008). GITO-Verlag, Berlin. (#)

Neff, A.A.; Hamel, F.; Herz, T.P.; Übernickel, F.; Brenner, W. (2013): IT Governance in Multi-business Organizations: Performance Impacts and Levers from Processes, Structures, and Relational Mechanisms. In: Proceedings of the 46th Annual Hawaii International Conference on System Sciences (HICSS 2013). IEEE, S. 4466-4475. (#)

Nevo, D.; Chan, Y.E. (2007): A Delphi study of knowledge management systems: scope and requirements. In: Information and Management (44, 6), S. 583-597.

Niederman, F.; Brancheau, J.C.; Wetherbe, J.C. (1991): Information Systems Management Issues in the 1990s. In: MIS Quarterly (15, 4), S. 474-499.

Nissen, V. (2008): Einige Grundlagen zum Management von IT-Agilität. In: Bankhofer, U.; Nissen, V.; Stelzer, D.; Straßburger, S. (Hrsg.): Ilmenauer Beiträge zur Wirtschaftsinformatik, Arbeitsbericht Nr. 2008-03.

Nissen, V. (2006): Integration von ITIL und Computervalidierung in der Pharmabranche am Beispiel Change Management. In: HMD – Praxis der Wirtschaftsinformatik (43, 250), S. 78-87.

Nissen, V.; Marekfia, W. (2013): Towards a research agenda for strategic governance, risk and compliance (GRC) management. In: Proceedings of the 15th IEEE Conference on Business Informatics (CBI 2013). IEEE computer society, S. 1-6.

Nissen, V.; Marekfia, W. (2014): The development of a data-centred conceptual reference model for strategic GRC-Management. In: Journal of Service Science and Management (7, 2), S. 63-76.

Nissen, V.; Mladin, A.: Messung und Management von IT-Agilität. In: HMD – Praxis der Wirtschaftsinformatik (46, 269), S. 42-51.

Nolan, R.; McFarlan, F.W. (2005): Information Technology and the Board of Directors. In: Harvard Business Review (83, 10), S. 96-106.

Nordsieck, F. (1934): Grundlagen der Organisationslehre. 2. Auflage, Poeschel, Stuttgart.

Novakowski, N.; Wellar, B. (2008): Using the Delphi Technique in Normative Planning Research: Methodological Design Considerations. In: Environment and Planning (40, 6), S. 1485-1500.

Office of the Government Commerce (OGC, Hrsg., 2007a): ITIL Service Strategy. TSO.

Office of the Government Commerce (OGC, Hrsg., 2007b): ITIL Service Transition. TSO.

Ogden, J.A.; Petersen, K.J.; Carter, J.R.; Monczkan, R.M. (2005): Supply management strategies for the future: a Delphi study. In: The Journal of Supply Chain Management (41, 3), S. 29-48.

Oh, L.-B.; Phua, T.-W.; Teo, H-H. (2007): A Conceptual Model for IT-Enabled Enterprise Risk Management in Financial Organisations. In: Proceedings of the 15th European Conference on Information System, (ECIS 2007). St. Gallen. (#)

Okoli, C.; Pawlowski, S.D. (2004): The Delphi method as a research tool: an example, design considerations and applications. In: Information & Management (42, December), S. 15-29.

Olbrich, S.; Pöppelbuß, J.; Niehaves, B. (2012): Critical Contextual Success Factors for Business Intelligence: A Delphi Study on Their Relevance, Variability, and Controllability. In: Proceedings of the 45th Annual Hawaii International Conference on System Sciences (HICSS 2012). IEEE, S. 4148-4157.

Olson, M.H., Chervany, N.L. (1980): The Relationship between Organizational Characteristics and the Structure of the Information Services Function. In: MIS Quarterly (4, 2), S. 57-68.

OMG (2010a): Unified Modeling Language: Infrastructure, Version 2.3, formal/2010-05-03. Needham.

OMG (2010b): Unified Modeling Language: Superstructure, Version 2.3, formal/2010-05-05. Needham.

Ono, R.; Wedemeyer, D.J. (1994): Assessing the Validity of the Delphi Technique. In: Futures (26, 3), S. 289-304.

O'Neill, S.; Murray, S.; Conboy, K. (2009): A Delphi study on collaborative learning in distance education. In: Proceedings of the 17th European Conference on Information System, (ECIS 2009). Verona, Paper 234.

Open Compliance and Ethics Group (OCEG, Hrsg., 2009): GRC Capability Model. Red Book 2.0. http://www.oceg.org, Abruf am 2010-06-12. (#)

Open Compliance & Ethics Group (OCEG, Hrsg., 2012): 2012 GRC Maturity Survey. http://www.oceg.org/event/the-2012-grc-maturity-survey-report/, Abruf am 2015-10-01.

Open Compliance & Ethics Group (OCEG, Hrsg., 2015): 2015 GRC Maturity Survey. http://www.oceg.org/resources/oceg-2015-grc-maturity-survey-report/, Abruf am 2015-12-05.

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD, Hrsg., 2004): OECD-Grundsätze der Corporate Governance – Neufassung 2004. (#)

Ortwerth, K.; Teuteberg, F. (2012): Green IT/IS Forschung – Ein systematischer Literaturreview und Elemente einer Forschungsagenda. In: Mattfeld, D.C.; Robra-Bissantz, S. (Hrsg.): Tagungsband der Multikonferenz der Wirtschaftsinformatik (MKWI 2012). GITO-Verlag, Braunschweig, S. 1501-1513.

o.V. (2003): Mitteilungen des GI-Fachbereichs Wirtschaftsinformatik. Rahmenempfehlung für die Universitätsausbildung. In: Wirtschaftsinformatik (45, 3), S. 381-384.

Österle, H. (1995): Business Engineering. Prozess- und Systementwicklung, Band 1, Entwurfstechniken. Springer, Berlin et al.

Österle, H.; Becker, J.; Frank, U.; Hess, T.; Karagiannis, D.; Krcmar, H.; Loos, P.; Mertens, P.; Oberweis, A; Sinz, E.J. (2010): Memorandum zur gestaltungsorientierten Wirtschaftsinformatik. In: Österle, H.; Winter, R.; Brenner, W. (Hrsg.): Gestaltungsorientierte Wirtschaftsinformatik: Ein Plädoyer für Rigor und Relevanz. Infowerk, St. Gallen, S. 1-6.

Ouchi, W.G. (1979): A Conceptual Framework for the Design of Organizational Control Mechanisms. In: Management Science (25, 9), S. 833-848.

Paetzmann, K. (2008): Corporate Governance. Strategische Marktrisiken, Controlling, Überwachung. Springer, Berlin et al.

Pahnila, S.; Siponen, M.; Mahmood, A. (2007): Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS). Auckland. (#)

Paine, L.; Deshpandé, R.; Margolis, J; Bettcher, K.E. (2005): Up to Code: Does Your Company's Conduct Met World-Class Standards? In: Harvard Business Review (83, 12), S. 122-133. (#)

Panitz, J. C.; Amberg, M.; Wiener, M. (2010): A Balanced Scorecard for Compliance – Requirements of a Comprehensive Compliance-Reporting. In: Proceedings of the 16th Americas Conference on Information Systems (AMCIS 2010). Lima, Paper 160. (#)

Panitz, J.C.; Wiener, M.; Amberg, M. (2011): Factors Facilitating Compliance Implementation – Case Study Results from Multinational Enterprises. In: Proceedings of the 19th European Conference on Information System, (ECIS 2011). Helsinki, Paper 3. (#)

Panko, R. (2006): Compliance-Appropriate Spreadsheet Testing. In: Proceedings of the 12th Americas Conference on Information Systems (AMCIS 2006). Acapulco, Paper 130. (#)

Pare, G.; Cameron, A.F.; Poba-Nzaou, P.; Templier, M. (2013): A Systematic Assessment of Rigor in Information Systems Ranking-Type Delphi Studies. In: Information & Management (50, 5), S. 207-217.

Park, I.; Jinkyu, L.; Rao, H.R.; Upadhyaya, S.J. (2006): Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management − Results of a Delphi Study. In: IEEE Transactions on Systems, Man & Cybernetics Part A: Systems and Humans (36, 3), S. 421-428.

Pauli, M.; Schermann, M.; Krcmar, H. (2010): The Risk Aware Enterprise Architecture: Towards a Transparent Inventory of IT Risk Management Artifacts. In: Fähnrich, K.-P.; Franczyk, B. (Hrsg): INFORMATIK 2010 Service Science – Neue Perspektiven für die Informatik Band 2. Lectures Notes in Informatics (LNI), Leipzig, S. 259-264. (#)

Pearce, J.A.; Freeman, E.B.; Robinson, R.B. (1987): The tenuous link between formal strategic planning and financial performance. In: Academy of Management Review (12, 4), S. 658-675.

Peek, T.; Rode, M. (2010): Compliance im Wandel. Integrated Compliance & Risk Management als Ansatz für die Zukunft. Deloitte. http://www.deloitte.com/assets/Dcom-Germany/Local%20Assets/Documents/09_Finanzdienstleister/2010/de_FS_R_Compliance_im_Wandel_150410.pdf, Abruf am 2015-01-09.

Peffers, K.; Tuunanen, T.; Gengler, C.E.; Rossi, M.; Hui, W.; Virtanen, V.; Bragge, J. (2006): The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. In: Proceedings of the International Conference on Design Science Research in Information Systems and Technology (DESRIST). Claremont, S. 83-106.

Peffers, K.; Tuunanen, T.; Rothenberger, M.; Chatterjee, S. (2007): A design science research methodology for information systems research. In: Journal of Management Information Systems (24, 3), S. 45-77.

Peterson, R. (2000): Emerging capabilities of Information Technology Governance: Exploring Stakeholder Perspectives in Financial Services. In: Proceedings of the 8th European Conference of Information Systems (ECIS 2000). Wien.

Peterson, R.; Parker, M.; Ribbers, P. (2002): Information Technology Governance Processes Under Environmental Dynamism: Investigating Competing Theories of Decision Making and Knowledge Sharing. In: Proceedings of the 23th International Conference on Information Systems (ICIS 2002), Barcelona.

Pfeffer, J. (1982): Organizations and Organization Theory. Pitman, Bosten et al.

Pfeiffer, D.; Niehaves, B. (2005): Evaluation of conceptual models – a structuralist approach. In: Proceedings of the 13th European Conference on Information System, (ECIS 2005). Regensburg, Paper 43.

Philip, T.; Wende, E.; Schwabe, G. (2010): Identifying Early Warning Signs of Failures in Offshore Software Development Projects - A Delphi survey. In: Proceedings of the 16th Americas Conference on Information Systems (AMCIS 2010). Lima, Paper 462.

Piccoli, G.; Ives, B. (2005): Review: IT-dependent strategic initiatives and sustained competitive advantage: a review and synthesis of the literature. In: MIS Quarterly (29, 4), S. 747-776.

Picot, A. (1982): Transaktionskostenansatz in der Organisationstheorie: Stand der Diskussion und Aussagewert. In: Betriebswirtschaft (42, 2), S. 267-284.

Picot, A.; Baumann, O. (2009): Die Bedeutung der Organisationstheorie für die Entwicklung der Wirtschaftsinformatik. In: Wirtschaftsinformatik (51, 1), S. 72-81.

Pischon, A. (1999): Integrierte Managementsysteme für Qualität, Umweltschutz und Arbeitssicherheit. Springer, Berlin et al.

Pohlman, M. (2008): Oracle identity management: governance, risk, and compliance architecture. 3. Auflage, CRC Press, Boca Raton et al. (#)

Poole, M.S.; Van de Ven, A.H. (1989): Using paradox to build management and organization theories. In: Academy of Management Review (14, 4), S. 562-578.

Porter, M. (1980): Competitive Strategy. Free Press, New York.

Porter, M. (1985): Competitive Advantage. Free Press, New York.

Porter, M.B. (1996): What is strategy? Harvard Business Review (74, 6), S. 61-78.

Powell, C. (2003): The Delphi technique: myths and realities. In: Journal of Advanced Nursing (41, 4), S. 376-382.

PricewaterhouseCoopers (PwC, Hrsg., 2004): Integrity-Driven Performance. A New Strategy for Success Through Integrated Governance, Risk and Compliance Management. A White Paper. http://www.grc-resource.com/resources/pwc_integritydrivenperformance.pdf, Abruf am 2015-11-01. (#)

PricewaterhouseCoopers (PwC, Hrsg., 2007): White Paper: Governance, Risikomanagement und Compliance: Nachhaltigkeit und Integration unterstützt durch Technologie. Frankfurt am Main. (#)

Project Management Institute (PMI, Hrsg., 2008): A Guide To Project Management Body of Knowledge. 4. Auflage, Upper Saddle River.

Prokein, O. (2008): IT-Risikomanagement. Identifikation, Quantifizierung und wirtschaftliche Steuerung. Gabler, Wiesbaden.

Puhakainen, P.; Siponen, M. (2010): Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. In: MIS Quarterly (34, 4), S. 757-778. (#)

Pupke, D. (2008): Compliance and corporate performance: the impact of compliance coordination on corporate performance. Books on Demand, Norderstedt. (#)

Puspasari, D.; Hammi, M.K.; Sattar, M.; Nusa, R. (2011): Designing a tool for IT Governance Risk Compliance: A case study. In: Proceedings of the International Conference on Advanced Computer Science and Information System (ICACSIS 2011), S. 311-316. (#)

Racz, N. (2011): Governance, Risk & Compliance (GRC) for Information Systems: Towards an Integrated Approach. Dissertation, Technische Universität Wien. http://catalogplus.tuwien.ac.at/primo_library/libweb/action/display.do;jsessionid=E9C8F22662E4749AF9BC21224270499D?tabs=detailsTab&ct=display&fn=search&doc=UTW_aleph_acc000522707&indx=2&recIds=UTW_aleph_acc000522707&recIdxs=1&elementId=1&renderMode=poppedOut&displayMode=full&frbrVersion=6&dscnt=0&frbr=&scp.scps=scope%3A%28UTW_O_SFX%29%2Cscope%3A%28UTW_aleph_acc%29%2Cprimo_central_multiple_fe&tab=default_tab&dstmp=1420789451359&srt=rank&mode=Basic&dum=true&vl(freeText0)=Racz&vid=UTW&y=0&x=0, Abruf am 2015-01-09.

Racz, N.; Panitz, J.C.; Amberg, M.; Weippl, E.; Seufert, A. (2010a): Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from a Survey among Large Enterprises. In: Proceedings of the Australian Conference on Information Systems (ACIS). Brisbane, Paper 21. (#)

Racz, N.; Weippl, E.; Bonazzi, R. (2011a): IT Governance, Risk & Compliance (GRC) Status Quo and Integration. An Explorative Industry Case Study. In: Proceedings of the 1st International Workshop on IT GRC (ITGRC 2011). IEEE, Washington. (#)

Racz, N.; Weippl, E.; Seufert, A. (2010b): A frame of reference for research of integrated GRC. In: De Decker, B.; Schaumüller-Bichl, I. (Hrsg.): Communications and Multimedia Security. Proceedings CMS, Springer, Berlin, S. 106-117. (#)

Racz, N.; Weippl, E.; Seufert, A. (2010c): A process model for integrated IT governance, risk & compliance management. In: Databases and Information Systems VI. Selected Papers from the 9th International Baltic Conference. (#)

Racz, N.; Weippl, E.; Seufert, A. (2010d): Questioning the need for separate IT risk management frameworks. In: Fähnrich, K.-P.; Franczyk, B. (Hrsg.): INFORMATIK 2010 Service Science – Neue Perspektiven für die Informatik Band 2. Lectures Notes in Informatics (LNI), Leipzig, S. 245-252. (#)

Racz, N., Weippl, E.; Seufert, A. (2011b): Integrating IT Governance, Risk, and Compliance Management Processes. In: Barzdins, J.; Kirikova, M (Hrsg.); Databases and Information Systems VI. Selected Papers from the Ninth International Baltic Conference, DB&IS 2010. IOS Press, Amsterdam, S. 325-338. (#)

Racz, N.; Weippl, E.; Seufert, A. (2011c): Governance, Risk & Compliance (GRC) Software – An Exploratory Study of Software Vendor and Market Research Perspectives. In: Proceedings of the 44th Annual Hawaii International Conference on System Sciences (HICSS 2011). IEEE, S. 1-10. (#)

Raghupathi, W. (2007): Corporate Governance of IT: A Framework for Development. In: Communications of the ACM (50, 8), S. 94-99. (#)

Ramanathan, J.; Cohen, R. J., Plassmann, E.; Ramamoorthy, K. (2007): Role of an auditing and reporting service in compliance management. In: IBM Systems Journal (46, 2), S. 305-318. (#)

Ramezani, E.; Fahland, D.; van der Aalst, W. (2012): Where Did I Misbehave? Diagnostic Information in Compliance Checking. In: Barros, A.; Gal, A.; Kindler, E. (Hrsg.): Business Process Management: Proceedings of the 10th International Conference on Business Process Management (BPM 2012). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 262-278. (#)

Rappaport, A. (1999): Shareholder Value. Wertsteigerung als Maßstab für die Unternehmensführung. 2. Auflage, Schäffer-Poeschel, Stuttgart.

Rath, M.; Sponholz, R. (2009): IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen. Schmidt, Berlin. (#)

RedMonk (Hrsg., 2008): SOA Meets Compliance: Compliance Oriented Architecture. http://redmonk.com/public/COA_Final.pdf, Abruf am 2015-05-15. (#)

Regierungskommission DCGK (Hrsg., 2010): Deutscher Corporate Governance Kodex. (#)

Reid, N.C. (1988): The Delphi technique, its contribution to the evaluation of professional practice. In: Ellis, R. (Hrsg.): Professional Competence and Quality Assurance in the Caring Professions. Croom-Helm, Beckenharn, Kent, S. 230-262.

Reiß, M; Corsten, H. (1995): Schnittstellenfokussierte Unternehmensführung. In: Corsten, H.; Reiß, M. (Hrsg.): Handbuch Unternehmensführung. Konzepte – Instrumente – Schnittstellen. Gabler, Wiesbaden, S. 5-18.

Riege, C.; Saat, J.; Bucher, T. (2009): Systematisierung von Evaluationsmethoden in der gestaltungsorientierten Wirtschaftsinformatik. In: Becker, J.; Krcmar, H.; Niehaves, B. (Hrsg.): Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik. Physica-Verlag, Heidelberg, S. 69-86.

Riegler, T. (2001): Wertorientierte Unternehmensführung – Umsetzungserfahrung im DaimlerChrysler Konzern. In: Zeitschrift für Controlling & Management (45, 2), S. 89-94.

Rieke, T.; Winkelmann, A. (2008): Modellierung und Management von Risiken – Ein prozessorientierter Risikomanagement-Ansatz zur Identifikation und Behandlung von Risiken in Geschäftsprozessen. In: Wirtschaftsinformatik (50, 5), S. 346-356. (#)

Rinderle-Ma, S.; Ly, L.T.; Dadam, P. (2008): Aktuelles Schlagwort: Business Process Compliance. In: Mitteilungen der GI-Fachgruppe Entwicklungsmethoden für Informationssysteme und deren Anwendung (EMISA) (28, 2), S. 24-29. (#)

Ritschel, A.; Hochstein, A.; Josi, M.; Brenner, W. (2006): SOX-IT-Compliance bei Novartis. In: HMD – Praxis der Wirtschaftsinformatik (43, 250), S. 68-77.

Ritzmann, E. (2006): Compliance bei Non-SEC-Unternehmen am Beispiel der Schweizerische Bundesbahnen SBB. In: (Menzies, C. Hrsg.): Sarbanes-Oxley und Corporate Compliance: Nachhaltigkeit, Optimierung, Integration. Schäffer-Poeschel, Stuttgart, S. 461-470.

Rogers, E.M. (2003): Diffusion of innovations. 5. Auflage, Free Press, New York.

Rogers, R.W. (1983): Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation In: Cacioppo, J.T.; Petty, R.E. (Hrsg.): Social Psychophysiology: A Sourcebook. Guilford Press, New York, S. 153-176.

Romeike, F.; Brühwiler, B. (2010): Praxisleitfaden Risikomanagement – ISO 31000 und ONR 49000 sicher anwenden. Erich Schmidt Verlag, Berlin.

Romme, A.G.L. (2003): Making a difference: Organization as design. In: Organization Science (14, 5), S. 558-573.

Rosemann, M. (1999): Gegenstand und Aufgaben des Integrationsmanagements. In: Scheer, A.-W.; Rosemann, M.; Schütte, R. (Hrsg.): Integrationsmanagement. Arbeitsberichte des Instituts für Wirtschaftsinformatik. Arbeitsbericht Nr. 65, Institut für Wirtschaftsinformatik der Westfälischen Wilhelms-Universität Münster, S. 5-18.

Rosemann, M.; de Bruin, T. (2005): Towards a Business Process Management Maturity Model. In: Proceedings of the 13th European Conference on Information System, (ECIS 2005). Regensburg.

Rowley, J.; Slack, F. (2004): Conducting a literature review. In: Management Research News (27, 6), S. 31-39.

Rozinat, A.; van der Aalst, W.M.P. (2008): Conformance Checking of Process Based on Monitoring Real Behavior. In: Information Systems (33, 1), S. 64-95. (#)

Saalfeld, C. (2006): Übergang von der SOX-Projektorganisation zur dauerhaften Linienverantwortung bei der Bayer AG. In: Menzies, C. (Hrsg.): Sarbanes-Oxley und Corporate Compliance: Nachhaltigkeit, Optimierung, Integration. Schäffer-Poeschel, Stuttgart, S. 425-431.

Sackmann, S. (2008a): A Reference Model for Process-oriented IT Risk Management. In: Proceedings of the 16th European Conference on Information System (ECIS 2008). Galway, Paper 246. (#)

Sackmann, S. (2008b): Assessing the Effects of IT Changes on IT Risk – A Business Process-Oriented View. In: Bichler, M.; Hess, T.; Krcmar, H.; Lechner, U.; Matthes, F.; Picot, A.; Speitkamp, B.; Wolf, P. (Hrsg.): Tagungsband der Multikonferenz Wirtschaftsinformatik (MKWI 2008). GITO-Verlag, Berlin. (#)

Sackmann, S. (2008c): Automatisierung von Compliance. In: HMD – Praxis der Wirtschaftsinformatik (45, 263), S.39-46. (#)

Sackmann, S. (2009): Integriertes Management von Risiko, Compliance und Geschäftsprozessen. In: Müller, G.; Neumann, G. (Hrsg.): Wirtschaftsinformatik – 35 Jahre zurück und 35 Jahre voraus. Österreichische Computer Gesellschaft, Wien, S. 147-52. (#)

Sackmann, S.; Hofmann, M.; Kühnel, S. (2013): Ein Ansatz zur wirtschaftlichen Spezifizierung von internen Kontrollsystemen. In: HMD – Praxis der Wirtschaftsinformatik (50, 289), S. 31-40. (#)

Sackmann, S.; Kähmer, M.; Gilliot, M.; Lowis, L. (2008): A Classification Model for Automating Compliance. In: Proceedings IEEE Conference on E-Commerce Technology. IEEE, Washington, S. 79-86. (#)

Sackmann, S.; Kähmer, M. (2008): ExPDT: A Layer-based Approach for Automating Compliance. In: Wirtschaftsinformatik (50, 5), S. 366-374. (#)

Sackmann, S.; Lowis, L.; Kittel, K. (2009): Selecting Services in Business Process Execution – A Risk-based Approach. In: Hansen, H.R.; Karagiannis, D.; Fill, H.-G. (Hrsg.): Business Services: Konzepte, Technologien, Anwendungen. 9. Internationale Tagung Wirtschaftsinformatik. Österreichische Computer Gesellschaft, Wien, Band 1, S. 357-366. (#)

Sadiq, S.; Governatori, G.; Naimiri, K. (2007): Modeling Control Objectives for Business Process Compliance. In: Alonso, G.; Dadam, P.; Rosemann, M. (Hrsg.): Business Process Management: Proceedings of the 5th International Conference on Business Process Management (BPM 2007). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 149-164. (#)

Sadiq, S.; Orlowska, M.; Sadiq, W. (2005): Specification and validation of process constraints for flexible workflows. In: Information Systems (30, 5), S. 349-378. (#)

Sambamurthy, V.; Bharadwaj, A.; Grover, V. (2003): Shaping Agility through digital options: reconceptualization of the role of information technology in contemporary firms. In: MIS Quarterly (27, 2), S. 237-263.

Sambamurthy, V.; Zmud, R.W. (1999): Arrangements for information technology governance: A theory of multiple contingencies. In: MIS Quarterly (23, 2), S. 261-290.

Sandner, T.; Kehlenbeck, M.; Breitner, M. (2010): An Implementation of a Process-Oriented Cross-System Compliance Monitoring Approach in SAP ERP and BI Environment. In: Proceedings of the 18th European Conference on Information System (ECIS 2010). Pretoria. (#)

SAP (Hrsg., 2009): An Integrated Approach to Managing Governance, Risk and Compliance. (#)

SAP (Hrsg., 2015): SAP-Lösungen für Governance, Risikomanagement und Compliance: mehr Sicherheit für Ihr Unternehmen. http://www.sap.com/germany/pc/analytics/governance-risk-compliance/software/overview/highlights.html, Abruf am 2015-01-11.

Saunders, C.S.; Jones, J.W. (1992): Measuring Performance of the Information Systems Function. In: Journal of Management Information Systems (8, 4), S. 63-82.

Schaad, A.; Flegel, U.; Wolter, C.; Miseldine, P. (2009): A Framework for Seamless and Compliant Service Consumption in Outsourcing Scenarios. In: Sadiq, S.; Indulska, M.; zur Muehlen, M.; Dubois, E.; Johannesson, P. (Hrsg.): Proceedings of the 2nd International Workshop on Governance, Risk and Compliance − Applications in Information Systems (GRCIS 2009), CEUR, Amsterdam. (#)

Scheer, A.-W. (2001): ARIS – Modellierungsmethoden, Metamodelle, Anwendungen. 4. Auflage, Springer, Berlin et al.

Scheer, A.-W. (2002): ARIS – Vom Geschäftsprozess zum Anwendungssystem. 4. Auflage, Springer, Berlin et al.

Scheer, A.-W. (Hrsg., 2003): Real-Time Enterprise: mit beschleunigten Prozessen Zeit und Kosten sparen. Springer, Berlin et al.

Scheer, A.-W. (1997): Wirtschaftsinformatik, Referenzmodelle für industrielle Geschäftsprozesse. 7. Auflage, Springer, Berlin et al.

Schewe, G. (2005): Unternehmensverfassung: Corporate Governance im Spannungsfeld von Leitung, Kontrolle und Interessenvertretung. Springer, Berlin et al.

Schierenbeck, H. (2003): Grundzüge der Betriebswirtschaftslehre. 16. Auflage, Oldenbourg, München.

Schmelzer, H.J.; Sesselmann, W. (2013): Geschäftsprozessmanagement in der Praxis. 8. Auflage, Hanser, München.

Schmidt, R. (1997): Managing Delphi surveys using nonparametric statistical techniques. In: Decision Sciences (28, 3), S. 763-774.

Schmiedel, T.; vom Brocke, J.; Recker, J. (2013): Which cultural values matter to business process management? Results from a global Delphi study. In: Business Process Management Journal (19, 2), S. 292-317.

Schneberger, S., Wade, M.; Allen, G., Vance, A., Eargle, D. (Hrsg., 2013): Theories Used in IS Research Wiki. http://istheory.byu.edu, Abruf am 2015-10-16.

Schnell, R.; Hill, P.B.; Esser, E. (2005): Methoden der empirischen Sozialforschung. 7. Auflage, Oldenbourg, München.

Schöler, S.; Zink, O. (2008): Governance, Risk und Compliance mit SAP. Galileo Press Verlag, Bonn. (#)

Schultz, M. (2013): Enriching Process Models for Business Process Compliance Checking in ERP Environments. In: vom Brocke, J.; Hekkala, R.; Ram, S.; Rossi, M. (Hrsg.): Proceedings of the International Conference on Design Science Research in Information Systems and Technology (DESRIST). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 120-135. (#)

Schultz, M.; Mueller-Wickop, N.; Nüttgens, M. (2012): Key Information Requirements for Process Audits – an Expert Perspective. In: Rinderle-Ma, S.; Weske, M. (Hrsg.): Der Mensch im Zentrum der Modellierung (EMISA 2012). Lecture Notes in Informatics (LNI), Wien, S. 137-150. (#)

Schumm, D.; Anstett, T.; Leymann, F.; Schleicher, D.; Strauch, S. (2010): Essential Aspects of Compliance Management with Focus on Business Process Automation. In: Fähnrich, K.-P.; Franczyk, B. (Hrsg): INFORMATIK 2010 Service Science – Neue Perspektiven für die Informatik Band 2. Lectures Notes in Informatics (LNI), Leipzig, S. 127-138. (#)

Schryen, G. (2010): Ökonomischer Wert von Informationssystemen. In: Wirtschaftsinformatik (52, 4), S. 225-237.

Schütte, R. (1997): Die neuen Grundsätze ordnungsmäßiger Modellierung. Paper zum Forschungsforum 1997, Leipzig 16.09-20.09.97.

Schwaiger, M.; Meyer, A. (2009): Theorien und Methoden der Betriebswirtschaft. Vahlen, München.

Schwering, B. (2010): Die Relevanz von IT-Compliance-Prüfstandards bei IT-Auslagerungen im deutschen Banksektor. In: Fähnrich, K.-P.; Franczyk, B. (Hrsg): INFORMATIK 2010 Service Science – Neue Perspektiven für die Informatik Band 2. Lectures Notes in Informatics (LNI), Leipzig, S. 231-238. (#)

Scott, W.A. (1955): Reliability, Ambiquity and Content Analysis. In: Psychological Review (59, 2), S. 119-129.

Seddon, P.B. (2005): Are ERP systems a source of competitive advantage? In: Strategic Change (14, 5), S. 283-293.

Setiono, R.; Mues, C.; Baesens, B. (2006): Risk Management and Regulatory Compliance: A Data Mining Framework Based on Neural Network Rule Extraction. In: Proceedings of the 27th International Conference on Information Systems (ICIS 2006). Milwaukee, Paper 7. (#)

Sidhu, K. (2005): Die Regelung zur Compliance im Corporate Governance Kodex. In: Zeitschrift für Corporate Governance (1, 1), S. 13-16. (#)

Sienou, A.; Lamine, E.; Pingaud, H. (2008): A Method for Integrated Management of Process-risk. In: Sadiq, S.; Indulska, M.; zur Muehlen, M.; Franch, X.; Hunt, E.; Coletta, R. (Hrsg.): Proceedings of the 1st International Workshop on Governance, Risk and Compliance − Applications in Information Systems (GRCIS 2008). CEUR, Montpellier, S. 16-30. (#)

Silveira, P.; Rodriguez, C.; Casati, F.; Daniel, F.; D' Andrea, V.; Worledge, C.; Taberi, Z. (2009): On the Design of Compliance Governance Dashboards for Effective Compliance and Audit Management. In: Dan, A.; Gittler, F.; Toumani, F. (Hrsg.): Proceedings of the International Workshops on Service Orientied Computing (ICSOC Workshops). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 208-217. (#)

Simonsson, M.; Johnson, P. (2006): Defining IT Governance – a Consolidation of Literature. In: Proceedings of the 18th Conference on Advanced Information Systems Engineering (CAISE 2006). Springer, Luxemburg. (#)

Singh, R.; Keil, M.; Kasi, V. (2009): Identifying and overcoming the challenges of implementing a project management office. In: European Journal of Information Systems (18, 5), S. 409-427.

Siponen, M.; Pahnila, S.; Mahmood, A.M. (2006): A New Model for Understanding Users' IS Security Compliance. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS). Kuala Lumpur. (#)

Siponen, M.; Vance, A. (2010): Neutralization: New Insights into the problem of Employee Information Systems Security Policy Violations. In: MIS Quarterly (34, 3), S. 487-502. (#)

Skulmoski, G.; Hartman F.T.; Krahn, J. (2007): The Delphi Method for Graduate Research. In: Journal of Information Technology Education (6, 1).

Slaughter, S.; Levine, L.; Ramesh, B.; Pries-Heje, J.: Aligning software processes with strategy. In: MIS Quarterly 30 (2006) 4, S. 891-918.

Smith, H.A.; McKeen, J.D. (2006): Developments in Practice XXI: IT in the World of Corporate Governance Reforms. In: Communications of the Association for Information Systems (17, Article 32), S. 714-727. (#)

Son, J.-Y. (2011): Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. In: Information and Management (48, 7), S. 296-302. (#)

Spanaki, K.; Papazafeiropoulou, A. (2013): Analysing the Governance, Risk and Compliance (Grc) Implementation Process: Primary Insights. In: Proceedings of the 21st European Conference on Information System (ECIS 2013). Utrecht, Paper 64. (#)

Spears, J.L.; Barki, H. (2010): User Participation in Information Systems Security Risk Management. In: MIS Quarterly (34, 3), S. 503-522. (#)

Staehle, W.; Conrad, P. (1999): Management: eine verhaltenswissenschaftliche Perspektive. 8. Auflage, Vahlen, München.

Stachowiak, H. (1974): Allgemeine Modelltheorie. Springer, Wien et al.

Stelzer, D. (2010): Enterprise Architecture Principles: Literature Review and Research Directions. In: Bankhofer, U.; Nissen, V.; Stelzer, D.; Straßburger, S. (Hrsg.): Ilmenauer Beiträge zur Wirtschaftsinformatik, Working Paper No. 1, September 2010, Ilmenau.

Stölzle, W. (1999): Industrial Relationships. Oldenbourg, München, Wien.

Stölzle, W. (2002): Logistikforschung – Entwicklungszüge und Integrationsperspektiven. In: Stölzle, W.; Gareis, K. (Hrsg.): Integrative Management- und Logistikkonzepte. Gabler, Wiesbaden, S. 511-527.

Straub, D.W.; Welke, R.J. (1998): Coping with Systems Risk: Security Planning Models for Management Decision-Making. In: MIS Quarterly (22, 4), S. 441-469.

Strecker, S.; Heise, D.; Frank, U. (2011): RiskM: A multi-perspective modeling method for IT risk assessment. In: Information Systems Frontiers (13, 4), S. 595-611. (#)

Strohmeier, G. (2007): Ganzheitliches Risikomanagement in Industriebetrieben. Grundlagen, Gestaltungsmodell und praktische Anwendung. DUV, Wiesbaden.

Tallon, P. (2007): Does IT pay to focus? An analysis of it business value under single and multi-focussed business strategies. In: Journal of Strategic Information Systems (16, 3), S. 278–300.

Tallon, P.; Kreamer, K.L.; Gurbaxani, V. (2000): Executives' perception of the business value of information technology. In: Journal of Management Information Systems (16, 4), S. 145-173.

Tanriverdi, H.; Du, K. (2009): Disintegrating Information Technology in Corporate Divestures: Implications for Regulatory Compliance Risks and Costs. In: Proceedings of the 30th International Conference on Information Systems (ICIS 2009), Phoenix, Paper 50. (#)

Tarantino, A. (2007): Governance, risk and compliance handbook: technology, finance, environmental, and international guidance and best practices. Wiley, Hoboken. (#)

Tashakkori, A.; Teddlie, C. (2003): Handbook of Mixed Methods in Social & Behavioral Research. Sage, Thousand Oaks et al.

Termer, F.; Nissen, V. (2014): Zum Begriff der Agilität − Betrachtungen und Implikationen aus etymologischer Perspektive. In: Bankhofer, U.; Nissen, V.; Stelzer, D.; Straßburger, S. (Hrsg.): Reihe Ilmenauer Beiträge zur Wirtschaftsinformatik Nr. 2014-04.

Teubner, A.; Feller, T. (2008): Informationstechnologie, Governance und Compliance. In: Wirtschaftsinformatik (50, 5), S. 400-407. (#)

Teubner, R.A. (2007): Strategic information systems planning: a case study from the financial services industry. In: Journal of Strategic Information Systems (16, 1), S. 105-125.

Teuteberg, F.; Freundlieb, M. (2009): Compliance Management mit betrieblichen Umweltinformationssystemen. In: wisu – das wirtschaftsstudium (38, 4), S. 550-557. (#)

Teuteberg, F.; Wittstruck, D. (2010): A Systematic Review of Sustainable Supply Chain Management Research: What is there and what is missing? In: Schumann, M.; Kolbe, L.M.; Breitner, M.H.; Frerichs, A. (Hrsg.): Tagungsband der Multikonferenz Wirtschaftsinformatik 2010 (MKWI 2010). Universitätsverlag Göttingen, Göttingen, S. 1001-1015.

The Institute of Internal Auditors (IIA, Hrsg., 2009): Internationale Standards für die berufliche Praxis der Internen Revision. Wien.

The IT Governance Institute (ITGI, Hrsg., 2007) COBIT 4.1. (#)

The Open Group (Hrsg., 2013): ArchiMate® 2.1 Specification. http://pubs.opengroup.org/architecture/archimate2-doc/toc.html, Abruf am 2014-11-12.

Thomas, O. (2006): Management von Referenzmodellen. Entwurf und Realisierung eines Informationssystems zur Entwicklung und Anwendung von Referenzmodellen. Logos-Verlag, Berlin.

Thomas, O.; Kaffai, B.; Loos, P. (2005): Referenzmodellbasiertes Event-Management mit Ereignisgesteuerten Prozessketten. In: Nüttgens, M.; Rump, F.J. (Hrsg.): Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten. 4. Workshop der Gesellschaft für Informatik e.V. (GI) und Treffen ihres Arbeitskreises "Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten (WI-EPK)", GI, Bonn.

Tolbert, P.S.; Zucker, L.G. (1983): Institutional sources of change in the formal structure of organizations: The diffusion of civil service reform, 1880-1935. In: Administrative Science Quarterly (28, 1), S. 22-39.

Torraco, R.J. (2005): Writing integrative literature reviews: Guidelines and examples. In: Human Resource Development Review (4, 3), S. 356-367.

Tosi, H.L.; Brownlee, A.L.; Silva, P.; Katz, J.P. (2003): An empirical exploration of decision-making under agency controls and stewardship structure. In: Journal of Management Studies (40, 8), S. 2053-2071.

Tracy, S.J. (2010): Qualitative Quality: Eight „Big-Tent" Criteria for Excellent Qualitative Research. In: Qualitative Inquiry (16, 10), S. 837-851.

Tüllner, J. (2012): Integration von Governance, Risikomanagement und Compliance. Erfahrungsbericht über ein Projekt zur Optimierung der Unternehmenssteuerung und einen ganzheitlichen Lösungsansatz. In: Zeitschrift für Corporate Governance (7, 3), S. 118-121. (#)

Turetken, O.; Elgammal, A.; van den Heuvel, W.-J.; Papazoglou, M. (2011): Enforcing Compliance on Business Processes through Use of Patterns. In: Proceedings of the 19th European Conference on Information System (ECIS 2011). Helsinki, Paper 5. (#)

Turetken, O.; Elgammal, A.; van den Heuvel, W.-J.; Papazoglou, M.P. (2012): Capturing Compliance Requirements: A Pattern-Based Approach. In: IEEE Software (29, 3), S. 28-36. (#)

Urbach, N.; Buchwald, A.; Ahlemann, F. (2013): Understanding IT Governance Success and its Impact: Results from and Interview Study. In: Proceedings of the 21st European Conference on Information System (ECIS 2013). Utrecht. (#)

U.S. Food and Drug Administration (FDA, Hrsg., 2013): CFR − Code of Federal Regulations Title 21. http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm, Abruf am 2015-03-24.

U.S. Securities and Exchange Comission (SEC, Hrsg., 2002): Sarbanes-Oxley Act of 2002. https://www.sec.gov/about/laws/soa2002.pdf, Abruf am 2015-05-21.

van Aken, J.E. (2004): Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules. In: Journal of Management Studies (41, 2), S. 219-246.

van Aken, J.E.; Romme, G. (2009): Reinventing the future: adding design science to the repertoire of organization and management studies. In: Organization Management Journal (6, 1), S. 5-12.

van Grembergen, W.; De Haes, S.; Guldentops, E. (2004): Structures, processes and relation mechanisms for information technology governance: Theories and practices. In: Van Grembergen, W. (Hrsg.): Strategies for IT governance. Idea Group Publishing, London, S. 1-36.

van der Veen, P.; Hartmann, I.; Ortwein, G. (2011): Governance, Risiko und Compliance. In: Zeitschrift für Führung und Organisation (80, 4), S. 265-271. (#)

van der Werf, J.; Verbeek, E.; van der Aalst, W. (2012): Context-Aware Compliance Checking. In: Barros, A.; Gal, A.; Kindler, E. (Hrsg.): Business Process Management: Proceedings of the 10th International Conference on Business Process Management (BPM 2012). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 98-113. (#)

Vance, A.; Siponen, M.; Pahnila, S. (2012): Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. In: Information & Management (49, 3-4), S. 190-198. (#)

Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. (2003): User Acceptance of Information Technology: Toward a Unified View. In: MIS Quarterly (27, 3), S. 186-204.

Venkatraman, N. (1999): Valuing the IS contribution to the business. Computer Sciences Corporation.

Verhoef, T.F.; Hofstede, A.H.M.T.; Wijers, G.M. (1991): Structuring Modelling Knowledge for CASE Shells. In: Andersen, R.; Bubenko, J.A.; Solvberg, A. (Hrsg.): Advanced Information Systems Engineering (CAISE 1991). Lecuture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 502-524.

Vessey, I.; Ramesh, V.; Glass, R.L. (2002): Research in information systems: an empirical study of diversity in the discipline and its journals. In: Journal of Management Information Systems (19, 2), S. 129-174.

Vicente, P.; da Silva, M.M. (2011a): A Business Viewpoint for Integrated IT Governance, Risk and Compliance. In: Proceedings IEEE World Congress on Services (SERVICES 2011). IEEE, Washington. (#)

Vicente, P.; da Silva, M.M. (2011b): A Conceptual Model for Integrated Governance, Risk and Compliance. In: Mouratidis, H.; Rolland, C. (Hrsg.): Advanced Information Systems Engineering (CAISE 2011). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 199-213. (#)

Vogler, K.; Lelke, F. (2006): IT-Governance - Projekterfahrungen der RAG Coal International. In: Zeitschrift für Controlling & Management (50, 2), S. 80-85.

Volonio, L.; Gessner, G.; Kernis, G. (2004): Holistic Compliance with Sarbanes-Oxley. In: Communications of the Association for Information Systems (14, 1), Article 11, S. 219-233. (#)

vom Brocke, J. (2003): Referenzmodellierung. Gestaltung und Verteilung von Konstruktionsprozessen. Logos, Berlin.

vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Platffaut, R.; Cleven, A. (2009): Reconstructing the Giant: On the Importance of rigour in documenting the literature search process. In: Proceedings of the 17th European Conference on Information System (ECIS 2009). Verona.

von der Gracht, H.A. (2012): Consensus measurement in Delphi studies. Review and implications for future quality assurance. In: Technological Forecasting & Social Change (79, 8), S. 1525-1536.

von Rennenkampff, A. (2015): Management von IT-Agilität – Entwicklung eines Kennzahlensystems zur Messung der Agilität von Anwendungslandschaften. In: Nissen, V. (Hrsg.): Ilmenauer Schriften zur Wirtschaftsinformatik. Band 2, Universitätsverlag Ilmenau, Ilmenau.

von Werder, A.; Grundei, J. (2006): Konzeptionelle Grundlagen des Organisations-Controllings. In: von Werder, A.; Stöber, H.; Grundei, J. (Hrsg.): Organisations-Controlling. Konzepte und Praxisbeispiele. Gabler, Wiesbaden, S. 15-50. (#)

Wade, M.; Hulland, J. (2004): Review: The resource-based view and information systems research: Review, extension, and suggestions for future research. In: MIS Quarterly (28, 1), S. 107-142.

Walgenbach, P. (2006): Neoinstitutionalistische Ansätze in der Organisationstheorie. In: Kieser, A.; Ebers, M. (Hrsg.): Organisationstheorien. 6. Auflage, Kohlhammer, Stuttgart, S. 353-401.

Walls, J.G.; Widmeyer, G.R.; El Sawy O.A. (1992): Building an information systems design theory for vigilant EIS. In: Information Systems Research (3, 1), S. 36-59.

Walls, J.G.; Widmeyer, G.R.; El Sawy, O.A. (2004): Assessing information system design theory in perspective: how useful was our 1992 initial rendition? In: Journal of Information Technology Theory and Application (6, 2), S. 43-58.

Walser, M.; Amberg, M.; Mossanen, K. (2007): Wirtschaftlichkeit von IT-Risk-Management-Lösungen zur Sicherstellung der Erfüllung von Compliance-Anforderungen. Vorteile und Herausforderungen IT-gestützter Compliance-Erfüllung. Friedrich-Alexander-Universität Erlangen-Nürnberg, Novell, Inc. http://www.itseccity.com/content/literatur/studien/071122_lit_stu_novell.html, Abruf am 2015-05-10. (#)

Walser, K.; Goeken, M. (2011): Möglichkeiten und Grenzen des multiplen IT-Governance- und -Management-Instrumenten-Einsatzes − Einführung eines „Intermediärs"-Metamodells. In: Heiß, H.-U.; Pepper, P.; Schlingloff, H.; Schneider, J. (Hrsg.): INFORMATIK 2011 Informatik schafft Communities. Lecture Notes in Informatics (LNI), Berlin. (#)

Wamba, S.F.; Ngai, E.W.T. (2011a): Unveiling the Potential of RFID-Enabled Intelligent Patient Management: Results of a Delphi Study. In: Proceedings of the 44th Annual Hawaii International Conference on System Sciences (HICSS 2011). IEEE, S. 1-10.

Wamba, S.F.; Ngai, E.W.T. (2012): Importance of the Relative Advantage of RFID as Enabler of Asset Management in the Healthcare: Results from a Delphi Study. In: Proceedings of the 45th Annual Hawaii International Conference on System Sciences (HICSS 2012). IEEE, S. 2879-2889.

Ward, J.; Peppard, J. (2002): Strategic Planning for Information Systems. 3. Auflage, Wiley, Chichester.

Warnecke, H.-J. (1997): Komplexität und Agilität − Gedanken zur Zukunft produzierender Unternehmen. In: Schuh, G.; Wiendahl, H.-P. (Hrsg.): Komplexität und Agilität: Steckt die Produktion in der Sackgasse? Springer, Berlin et al., S. 1-8.

Webb, P.; Pollard, C.; Ridley, G. (2006): Attempting to Define IT Governance: Wisdom or Folly? In: Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS 2006). IEEE. (#)

Webster, J.; Watson, R.T. (2002): Analyzing the past to prepare for the future: writing a literature review. In: MIS Quarterly (26, 2), S. xiii-xxiii.

Wecker, G.; van Laak, H. (Hrsg., 2008): Compliance in der Unternehmenspraxis: Grundlagen, Organisation und Umsetzung. Gabler, Wiesbaden. (#)

Weidlich, M.; Polyvyanyy, A.; Desai, N.; Mendling, J. (2010): Process Compliance Measurement Based on Behavioral Profiles. In: Pernici, B. (Hrsg.): Proceedings of the 22nd International Conference on Advanced Information Systems Engineering (CAISE 2010). Lecture Notes in Computer Science (LNCS), Springer, Berlin et al., S. 499-514. (#)

Weidlich, M.; Polyvyanyy, A.; Desai, N.; Mendling, J.; Weske, M. (2011): Process compliance analysis based on behavioural profiles. In: Information Systems (36, 7), S. 1009-1025. (#)

Weigand, H.; van den Henvel, W.-J.; Hiel, M. (2011): Business Policy Compliance in Service-oriented systems. In: Information Systems (36, 4), S. 791-807. (#)

Weill, P. (2004): Don't Just Lead, Govern: How best Performing Organizations Govern IT. In: MIS Quarterly Executive (3, 1), S. 1-17.

Weill, P.; Ross, J.W. (2004): IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business Press, Bosten.

Weinhardt, C.; Anandasivam, A.; Blau, B.; Borissov, N.; Meinl, T.; Michalk, W.; Stößer, J. (2009): Cloud-Computing – Eine Abgrenzung, Geschäftsmodelle und Forschungsgebiete. In: Wirtschaftsinformatik (51, 5), S. 453-461.

Weiss, B.; Winkelmann, A. (2011): Developing a Process-Oriented Notation for Modeling Operational Risks − A Conceptual Metamodel Approach to Operational Risk Management in Knowledge Intensive Business Processes within the Financial Industry. In: Proceedings of the 44th Annual Hawaii International Conference on System Sciences (HICSS 2011). IEEE, S. 1-10. (#)

Werner, M.; Gehrke, N.; Nüttgens, M. (2012): Business Process Mining and Reconstruction for Financial Audits. In: Proceedings of the 45th Annual Hawaii International Conference on System Sciences (HICSS 2012). IEEE, S. 5350-5359. (#)

Werner, M.; Gehrke, N.; Nüttgens, M. (2013): Towards Automated Analysis of Business Processes for Financial Audits. In: Alt, R.; Franczyk, B. (Hrsg.): Proceedings of the 11th International Conference on Wirtschaftsinformatik (WI 2013). Leipzig, S. 375-390. (#)

Westin, S.; Roy, M.; Kim, C.K. (1994): Cross-fertilization of knowledge: The case of MIS and its reference disciplines. In: Information Resources Management Journal (7, 2), S. 24-34.

Westkämper, E. (1997): Produktion in Netzwerken. In: Schuh, G.; Wiendahl, H.-P. (Hrsg.): Komplexität und Agilität: Steckt die Produktion in der Sackgasse? Springer, Berlin et al., S. 275-291.

Wiesche, M.; Berwing, C.; Schermann, M.; Krcmar, H. (2011a): Patterns for Understanding Control Requirements for Information Systems for Governance, Risk Management, and Compliance (GRC IS). In: Salinesi, C.; Pastor, O. (Hrsg.): Advanced Information Systems Engineering Workshops (CAISE 2011 International Workshops). Lecture Notes in Business Information Processing (LNBIP), Springer, Berlin et al., S. 208-217. (#)

Wiesche, M.; Bodner, J.; Schermann, M. (2012): Antecedents of IT-Enabled Organizational Control Mechanisms. In: Proceedings of the 20th European Conference on Information System (ECIS 2012). Barcelona, Paper 176. (#)

Wiesche, M.; Schermann, M.; Krcmar, H. (2011b): Exploring the Contribution of Information Technology to Governance Risk Management and Compliance (GRC) Initiatives. In: Proceedings of the 19th European Conference on Information System (ECIS 2011). Helsinki, Paper 4. (#)

Wiesche, M.; Schermann, M.; Krcmar, H. (2013): When IT Risk Management Produces More Harm than Good: The Phenomenon of Mock Bureaucracy. In: Proceedings of the 46th Annual Hawaii International Conference on System Sciences (HICSS 2013). IEEE, S. 4502-4511. (#)

Wilde, T.; Hess, T. (2006): Methodenspektrum der Wirtschaftsinformatik: Überblick und Portfoliobildung. In: Arbeitsbericht Nr. 2/2006, Institut für Wirtschaftsinformatik und Neue Medien der Ludwig-Maximilians-Universität München.

Wilde, T.; Hess, T. (2007): Forschungsmethoden der Wirtschaftsinformatik: Eine empirische Untersuchung. In: Wirtschaftsinformatik (49, 4), S. 280-287.

Williamson, O.E. (1985): The Economic of Institutions of Capitalism. The Free Press, New York.

Williamson, O.E. (1991): Comparative economic organization: The analysis of discrete structural alternatives. In: Administrative Science Quarterly (36, 2), S. 269-296.

Willson, P.; Pollard, C. (2009): Exploring IT Governance in Theory and Practice in a Large Multi-National Organisation in Australia. In: Information Systems Management (26, 2), S. 98-109. (#)

Wilson, B. (1990): Systems: concepts, methodologies and applications. 2. Auflage, John Wiley & Sons, Chichester.

Wipawayangkool, K. (2009): Information Security Compliances and Knowledge Management Capabilities in International Diversification. In: Proceedings of the 15th Americas Conference on Information Systems (AMCIS 2009). San Francisco, Paper 604. (#)

Withus, K.-H. (2010): Sicherstellung der Compliance durch wirksame Managementsysteme. In: Zeitschrift für Interne Revision (45, 3), S. 99-108. (#)

Witt, P. (2003): Corporate Governance-Systeme im Wettbewerb. DUV, Wiesbaden.

Witte, T. (1973): Simulationstheorie und ihre Anwendungen auf betriebliche Systeme. Gabler, Wiesbaden, 1973.

Wöhe, G.; Döring, U. (2013): Einführung in die Allgemeine Betriebswirtschaftslehre. 25. Auflage, Vahlen, München.

Wolf, J. (2005): Organisation, Management, Unternehmensführung: Theorien, Praxisbeispiele und Kritik. 2. Auflage, Gabler, Wiesbaden.

Wolf, K. (2003): Risikomanagement im Kontext der wertorientierten Unternehmensführung. Deutscher Universitäts-Verlag, Wiesbaden.

Wolf, P.; Gehrke, N. (2009): Continuous Compliance Monitoring in ERP-Systems – A Method for Identifying Segregation of Duties Conflicts. In: Hansen, H.R.; Karagiannis, D.; Fill, H.-G. (Hrsg.): Business Services: Konzepte, Technologien, Anwendungen. 9. Internationale Tagung Wirtschaftsinformatik 25.-27. Februar 2009, Wien. Österreichische Computer Gesellschaft, Wien, Band 1, S. 347-356. (#)

Wolf, P.; Goeken, M. (2010): Integration von IT- und unternehmensweitem Risikomanagement auf Konzeptebene. In: Fähnrich, K.-P.; Franczyk, B. (Hrsg): INFORMATIK 2010 Service Science – Neue Perspektiven für die Informatik Band 2. Lectures Notes in Informatics (LNI), Leipzig, S. 239-244. (#)

Wolf, P.; Goeken, M. (2011): Ontologiebasierte Integration von Informations- und unternehmensweitem Risikomanagement − Motivation, Grundlagen, Vorgehen und erste Ergebnisse. In: Heiß, H.-U.; Pepper, P.; Schlingloff, H.; Schneider, J. (Hrsg.): INFORMATIK 2011 Informatik schafft Communities. Lecture Notes in Informatics (LNI), Berlin. (#)

Wrona, T. (2006): Fortschritts- und Gütekriterien im Rahmen qualitativer Sozialforschung. In: Zelewski, S.; Naciye, A. (Hrsg.): Fortschritt in den Wirtschaftswissenschaften. DUV, Wiesbaden, S. 189-216.

Xue, Y.; Liang, H.; Wu, L. (2011): Punishment, Justice, and Compliance in Mandatory IT Settings. In: Information System Research (22, 2), S. 400-414. (#)

Yayla, A. (2011): Enforcing Information Security Policies through Cultural Boundaries: A Multinational Company Approach. In: Proceedings of the 19th European Conference on Information System, (ECIS 2011). Helsinki, Paper 243. (#)

Yang, Y.N. (2003): Testing the stability of experts' opinions between successive rounds of Delphi studies. In: Proceedings Annual Meeting of the American Educational Research Association, Chicago. http://files.eric.ed.gov/fulltext/ED472166.pdf, Abruf am 2014-08-21.

Yin, R.K. (2009): Case Study Research. Design and Methods. 4. Auflage, SAGE, Los Angeles et al.

Zafar, H.; Clark, J.G.; Ko, M.; Au, Y.A. (2011): Critical Success Factors for an Effective Security Risk Management Program: An Exploratory Case Study at a Fortune 500 Firm. In: Proceedings of the 17th Americas Conference on Information Systems (AMCIS 2011). Detroit, Paper 35. (#)

Zelewski, S. (2007): Kann Wissenschaftstheorie behilflich für die Publikationspraxis sein? Eine kritische Auseinandersetzung mit den "Guidelines" von Hevner et al. In: Lehner, F., Zelewski, S. (Hrsg.): Wissenschaftstheoretische Fundierung und wissenschaftliche Orientierung der Wirtschaftsinformatik. GITO, Berlin, S. 74-123.

Zelewski, S. (1999): Ontologien zur Strukturierung von Domänenwissen – Ein Annäherungsversuch aus betriebswirtschaftlicher Perspektive. Arbeitsbericht Nr. 3, Institut für Produktion und Industrielles Informationsmanagement, Essen.

Zmud, R.W. (1984): Design Alternatives for Organizing Information Systems Activities. In: MIS Quarterly (8, 2), S. 79-93.

Zoet, M.; Versendaal, J.; Ravesteyn, P. (2011): A Business Rules Viewpoint on Risk and Compliance Management. In: Proceedings of the 24th BLED eConference, Paper 25. (#)

Zorn, T.; Campbell, N. (2006): Improving the Writing of Literature Reviews through a Literature Integration Exercise. In: Business Communication Quarterly (69, 2), S. 172-183.

Zucker, L.G. (1983): Organizations as institutions. In: Bacharach, S.B. (Hrsg.): Research in the Sociology of Organizations. JAI Press, Greenwich, S. 1-42.

zur Muehlen, M.; Rosemann, M. (2005): Integrating Risks in Business Process Models. In: Proceedings of the Australian Conference on Information Systems (ACIS). Sydney. (#)