Forschungsberichte zur Unternehmensberatung
- Reports on Consulting Research -

Herausgegeben von
Prof. Dr. Volker Nissen

Wolfgang Marekfia, Volker Nissen

Strategisches GRC-Management - Grundzüge eines konzeptionellen Bezugsrahmens

Forschungsbericht Nr. 2009-02,

November 2009

Technische Universität Ilmenau
Fakultät für Wirtschaftswissenschaften, Institut für Wirtschaftsinformatik
Fachgebiet Wirtschaftsinformatik für Dienstleistungen (WI-2)

Autoren: Wolfgang Marekfia, Volker Nissen

Titel: Strategisches GRC-Management - Grundzüge eines konzeptionellen Bezugsrahmens.

Forschungsberichte zur Unternehmensberatung Nr. 2009-02, 1. Aufl., November 2009

Technische Universität Ilmenau, FG Wirtschaftsinformatik für Dienstleistungen

ISSN 1862-1805

ISBN **978-3-938940-24-2**

urn:nbn:de:gbv:ilm1-2009200180

© 2009 FG Wirtschaftsinformatik für Dienstleistungen, TU Ilmenau

Dieses Material ist urheberrechtlich geschützt.

Anschrift: Technische Universität Ilmenau, Fakultät für Wirtschaftswissenschaften, Institut für Wirtschaftsinformatik, PF 100565, D-98684 Ilmenau.
http://www.tu-ilmenau.de/fakww/Forschungsberichte_z.1664.0.html

Inhaltsverzeichnis

Abbildungsverzeichnis

Zusammenfassung:

Der Beitrag erläutert die Notwendigkeit, im GRC-Management proaktiv und strategisch denkend vorzugehen, anstatt, wie heute vorherrschend der Fall, Einzelfall-bezogen und reaktiv zu handeln. Als Hilfsmittel zur Strukturierung des Anwendungsfeldes wird ein konzeptioneller Bezugsrahmen in Grundzügen entwickelt, der einerseits den unterschiedlichen Teilgebieten des GRC-Managements und ihren Synergiepotenzialen gerecht werden will und andererseits verschiedene Management-Perspektiven als relevante Gestaltungsfelder identifiziert.

Schlüsselwörter: Governance, Risk, Compliance, Strategisches Management, Informationsmanagement, Management-Perspektiven, Proaktives Handeln

1 Ausgangssituation

Governance, Risk und Compliance (GRC) sind eng zusammenhängende Themen, deren Vernachlässigung für Unternehmen zu gravierenden ökonomischen Konsequenzen führen kann. In Folge von Bilanzskandalen wie jenen bei Enron, Paramlat und Telekom kam es zu einer Verschärfung der gesetzlichen Bestimmungen. Als bedeutsamstes Beispiel hierfür kann der Sarbanes Oxley Act (SOX) angeführt werden. Allgemein ist als Konsequenz aus der Subprime-Krise und dem dadurch induzierten ökonomischen Abschwung eine weitere Verschärfung regulatorischer Anforderungen an Unternehmen zu erwarten, auch außerhalb des Finanzsektors.

Neben diesen regulatorischen Anforderungen sind Unternehmen mit einer hohen Marktdynamik, die bspw. aus schnellen technologischen Entwicklungen, Käufermärkten, kurzen Produktlebenszyklen und Internationalisierung entstehen, konfrontiert. Daraus resultieren zwei Konsequenzen, die hier relevant sind. Erstens müssen Unternehmen ihre Geschäftsrisiken genauer im Blick behalten, womit nicht nur die regulatorischen Risiken gemeint sind. Zweitens ergibt sich ein Handlungsdruck, die Kerngeschäftsprozesse von Unternehmen sehr agil zu halten, um auf marktliche Veränderungen schnell reagieren zu können. Agile Geschäftsprozesse erfordern auch eine agile und kundenorientierte IT-Unterstützung (Papazoglou et al. 2006; Nissen und Mladin 2009). Neue IT-Modelle, wie

Service-orientierte Architekturen und IT-Service Management sind ein Resultat dieser veränderten Situation. Gerade diese Flexibilität in den Geschäftsprozessen und der unterliegenden IT stellt das GRC-Management aber vor große Herausforderungen.

Gleichzeitig ist der Bereich GRC durch eine Vielzahl von Themen geprägt, die sich in der Unternehmenspraxis derzeit oft noch in unvernetzten Ad-hoc-Initiativen widerspiegeln. Bestehende Abhängigkeiten werden nicht berücksichtigt, was die Nutzung von Synergiepotentialen verhindert. Der Bereich GRC wird außerdem überwiegend als „Kostenverursacher“ wahrgenommen. Durch die reaktive und isolierte Vorgehensweise bleiben potentielle Nutzeneffekte, die sich z.B. im Rahmen der Geschäftsprozessoptimierung ergeben könnten, oftmals ungenutzt. Bestehende Forschungsarbeiten in diesem Kontext diskutieren häufig ebenfalls Einzelfragen. Hierbei bleibt bislang unbeantwortet, wie die vereinzelten Vorschläge und Methoden in einen umfassenden organisatorischen Ansatz zu integrieren sind. Im Rahmen des Beitrags wird daher ein strategischer und integrierter Ansatz für das GRC-Management entwickelt, wobei bestehende Ansätze und Methoden in diesen Gesamtzusammenhang eingegliedert werden.

Der Beitrag ist wie folgt strukturiert. In Abschnitt 2 werden die Begriffe Governance, Risiko und Compliance definiert, hinsichtlich der Integration untersucht sowie der Begriff des strategischen GRC-Managements erläutert. Anschließend wird auf bestehende GRC-Ansätze eingegangen. In Abschnitt 4 wird ein konzeptioneller Bezugsrahmen entwickelt sowie ein kurzer Ausblick auf weiteren Forschungsbedarf gegeben.

2 Begriffliche Grundlagen

Der Begriff Corporate Governance kann in einer engen Abgrenzung aus der Sicht des Shareholder-Ansatzes (US-amerikanisches Verständnis bspw. SOX) und in einer weiten Abgrenzung aus der Sicht des Stakeholder-Ansatzes (deutsches Verständnis, bspw. deutscher Corporate Governance Kodex) erklärt werden (Witt 2003, S. 61-116; Mallin 2007, S. 159-265). 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). Der

Begriff Risiko wird kontrovers diskutiert, kann jedoch als negative Abweichung eines tatsächlichen von einem erwarteten Ereignis definiert werden (bspw. KonTraG). Im Rahmen der Risikoaggregation ist es aber auf Grund von Kompensationseffekten sinnvoll, positive und negative Abweichungen zu betrachten (Gleißner 2008, S. 8-9 Strohmeier 2007, S.34). Risikomanagement soll hier als ein Prozess definiert werden, 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). Die Definition des Begriffs Compliance wird in ein enges und ein weites Begriffsverständnis 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). Compliancemanagement ist dem weiten Begriffsverständnis folgend ein System, welches die Einhaltung von internen und externen sowohl verpflichtenden als auch freiwilligen Vorgaben sicherstellt.

GRC ist heute dadurch gekennzeichnet, dass ursprünglich abgegrenzte Problemstellungen durch aktuelle Herausforderungen ausgeweitet werden und dabei konvergieren. Für die drei Teilbereiche werden auf Grund der steigenden praktischen Bedeutung zunehmend ganzheitliche und unternehmensweite Ansätze vorgeschlagen. Hierbei bleiben jedoch die jeweils gewählten Perspektiven noch recht verschieden. Im Unterschied dazu lässt sich ein hohes Integrationspotential zwischen den GRC-Teilaufgaben konstatieren, da eine Vielzahl von Berührungspunkten existieren (Teubner und Feller 2008) und sich die Konzepte auf verschiedene Hierachieebenen konzentrieren. Während die Corporate Governance an der Unternehmensspitze den Vorstand und den Aufsichtrat (im Fall einer Aktiengesellschaft) tangiert, konzentriert sich das Risikomanagement auf den Managementbereich und ist somit zwischen der Corporate Governance und der Compliance einzuordnen. Letztere betrifft alle Mitarbeiter im Rahmen der Ausführung von operativen Tätigkeiten (Menzies 2006, S. 334-336).

Der Ansatz in diesem Beitrag greift die wechselseitigen Beziehungen der Elemente von GRC auf und zeichnet sich durch eine integrative und strategische Perspektive aus. Unter Hervorhebung der Managamentaufgaben und des Kriteriums der strategischen Relevanz

wird der Ansatz in Abgrenzung zu bestehenden Ansätzen daher als „strategisches GRC-Management“ bezeichnet.

Das Merkmal „integrativ“ kann in verschiedene Richtungen untergliedert werden. *Vertikale* Integration bedeutet die Integration der einzelnen Bestandteile von GRC. *Horizontale* Integration umfasst die Integration aller GRC-Projekte zu einer unternehmensweiten GRC-Initative. Pupke (2008, S. 132) fordert außerdem die Integration der Erfüllung von Compliance-Anforderungen in die Primärorganisation, was auch als *operative* Integration bezeichnet wird (PwC 2007, S. 7-8; Menzies 2006, S. 332-334). Das Merkmal „strategisch“ kann in die langfristige Ausrichtung und die proaktive Aktionsorientierung untergliedert werden. Das Konzept der *proaktiven Aktionsorientierung* steht im Gegensatz zur bisher in der Praxis dominierenden reaktiven und projektbasierten Vorgehensweise, wobei Anforderungen ungeplant und ad hoc umgesetzt werden. Die proaktive Aktionsorientierung ist durch eine geplante, frühzeitige und unmittelbare Handlung gekennzeichnet und kann als „die bewusste Gestaltung strategisch relevanter Tatbestände, um die Zukunft in eine für die Organisation günstige Richtung zu lenken“ (Scholz 2000, S. 52-56) konkretisiert werden. Für GRC bedeutet ein proaktiver Ansatz somit insbesondere die geplante Verwirklichung, der durch GRC entstehenden Nutzenpotentiale. Demnach wird unter strategischem GRC-Management ein unternehmensweiter und strategischer Ansatz verstanden, der die GRC-bezogenen Aktivitäten vertikal und horizontal sowie in die Primärorganisation integriert. Die Ziele des GRC-Managements sind die langfristige Erfüllung der Stakeholderanforderungen und die Verwirklichung, der aus GRC entstehenden Nutzenpotentiale für das Unternehmen.

3 Kurzer Abriss existierender GRC-Ansätze

Eine Reihe von Autoren aus Wissenschaft und Praxis haben bereits ein integriertes Management von GRC gefordert. Neben Software- und Beratungshäusern (Götz et al. 2008; Kranawetter 2009; PwC 2007; Menzies 2006; Deloitte 2008) gehören hierzu auch Klotz und Dorn (2008), welche den engen Verflechtungsgrad von GRC erkennen und auf Grund der inhaltlichen Zusammenhänge „eine integrierte Strategie und ein gemeinsames Management“ fordern (Klotz und Dorn 2008, S.7). Ein Gesamtansatz zum integrierten Management von GRC wird von PwC vorgeschlagen, wobei die Darstellung innerhalb der

einzelnen Arbeiten unterschiedlich ist (PwC 2007; Menzies 2006). Die Darstellung in Menzies (2006) besteht im Kern aus dem GRC-Stufenmodell, welches auf den drei Stufen „Compliance“, „Transformation & Optimierung“ und „Integration & Optimierung“ basiert und übergreifend von der „Compliance-Driven Optimization“ ergänzt wird. Gemäß diesem Modell soll ausgehend von der projektbasierten Umsetzung einzelner Anforderungen, die Compliance durch die Überführung in den Regelbetrieb sichergestellt werden. Letztlich wird durch die Integration von GRC eine ganzheitliche, unternehmensweite Vorgehensweise verwirklicht. Pupke (2008, S. 79) identifiziert auf der Grundlage einer Transaktionskostenanalyse den Hybrid Compliance Approach als beste Koordinationsform des Compliancemanagements. Die „hybrid coordination“ ist eine dezentralisierte Form der Koordination und integriert die Compliance-Aktivitäten in die Primärorganisation. Außerdem empfiehlt Pupke im Rahmen des Ansatzes alle Aktivitäten und speziell die Implementierung von neuen Anforderungen zentral zu koordinieren.

In der Wirtschaftsinformatik-Forschung wird insbesondere die Automatisierung der Compliance-Sicherung (bspw. Sackmann und Kähmer 2008; El Kharbili et al. 2008), die Erweiterung von Modellierungsmethoden um Compliance- und Risiko-Aspekte (bspw. Karagiannis 2008; Rieke und Winkelmann 2008) sowie GRC im Kontext von serviceorientierten Architekturen (SOA, bspw. Loosli 2008, Sackmman et al. 2009, Lotz 2008) diskutiert. Die Bandbreite der behandelten Problemstellungen ist ebenso heterogen wie das Themengebiet insgesamt. Die bestehenden Ansätze sind jedoch punktuell und es bleibt offen, wie sich die entwickelten Methoden in einen übergeordneten, prozessorientierten Gesamtansatz integrieren lassen.

4 Konzeptioneller Bezugsrahmen

4.1 Motivation und Leitidee des Bezugsrahmens

Im Folgenden wird ein konzeptioneller Bezugsrahmen für das strategische GRC-Management in seinen Grundzügen vorgestellt. Die mit dem Bezugsrahmen verfolgten Ziele sind zweigeteilt:

- Er dient zur Strukturierung des Vorverständnisses und liefert einen Rahmen, um das Denken über die komplexen Themenzusammenhänge zu ordnen. Ihm kommt

eine Selektions- und Steuerungsfunktion für spätere Untersuchungen zu, die über den Rahmen dieser Arbeit hinausgehen.

- Er bildet die Basis, um fundierte Gestaltungshinweise für die Unternehmenspraxis ableiten und Managementinstrumente entwickeln zu können. So unterstützt er die Weiterentwicklung von bestehenden Managementsystemen im Bereich GRC, in dem er Lücken aufzeigt, und bietet einen Anknüpfungspunkt, um bereits existierende Konzepte und Methoden in einen Gesamtzusammenhang einzuordnen.

Stölzle (2002) nennt in seinem Forderungskatalog an eine Forschungskonzeption den Gedanken der Leitidee hilfreich, da sie eine erste Vorstellung über das Problemfeld vermittelt. Unsere Leitidee ist, dass Unternehmen einen integrierten Ansatz für das GRC-Management benötigen, der von den Stakeholderanforderungen ausgeht, in die strategische Planungsebene eingebunden sowie proaktiv angelegt ist und mit dem Synergien und Nutzenpotenziale von GRC bestmöglich realisiert werden sollen. Stattdessen dominiert nach den Erfahrungen unserer GRC-Beratungspraxis heute ein überwiegend extern motivierter und einzelthemengetriebener Ad-hoc-Aktionismus. Wesentliche weitere Leitgedanken unserer Forschung sind die Berücksichtigung der gestiegenen Anforderungen an die Agilität der Geschäftsprozesse sowie eine konsequente Prozessorientierung und Harmonisierung der Aufgaben von GRC und Geschäftsprozessmanagement (sowie von weiteren Managementsystemen).

4.2 Gesamtproblemkomplex, Einflussfaktoren und Strukturierung

Den Ausgangspunkt von GRC stellen die Interessen der Stakeholder dar (Bild 1). Freeman (1984, S. 46) bezeichnet Individuen oder Gruppen als Stakeholder, wenn diese einen materiellen oder immateriellen Anspruch an das Unternehmen haben. Der Stakeholder-Ansatz ist zu unterscheiden vom Shareholder-Ansatz, der sich lediglich an den Interessen der Eigentümer (Shareholder) orientiert (Rappaport 1999, S. 39). Der Begriff Stakeholderanforderung dient zur Zusammenfassung von Anforderungen aus den Teilbereichen von GRC. Die Ziele der Stakeholder (bspw. Datenschutz, Produktsicherheit, Umweltschutz, finanzielle Transparenz) stellen für das Unternehmen Anforderungen dar, welche sich sowohl in wirtschaftlich-ethischen Anforderungen der Corporate Governance, im Risikomanagement sowie in regulatorischen Vorgaben und Standards (Compliance) manifestieren.

Der Gegenstandsbereich von GRC erstreckt sich auf die gesamte Unternehmensarchitektur, die ein Rahmenwerk zur Anpassung an geänderte geschäftliche Anforderungen ist und sich in die Ebenen Strategie, Geschäftsprozesse und IT-Systeme unterteilt (Österle und Blessing 2003, S .81). GRC steht mit diesen Ebenen in einem vielfältigen Zusammenhang. Die Geschäftsprozesse müssen dabei ebenso wie die IT-Systeme flexibel an neue fachliche Erfordernisse angepasst werden können. Hierbei gewinnt das Architekturparadigma SOA verstärkt an Bedeutung. Das GRC-Management nimmt eine Schnittstellenfunktion zwischen der strategischen Ebene und der Ableitung der Geschäftsprozesse sowie deren IT-seitiger Implementierung ein. Es ist mit strategischen Zielen abzustimmen sowie mit den weiteren Managementsystemen, welche GRC beeinflussen. Zu diesen Managementsystemen gehören bspw. das Qualitätsmanagement, die Revision, Geschäftsprozessmanagement (GPM) und Controlling. Das GRC-Management muss in die bestehenden Managementsysteme integriert werden und somit die etablierten Strukturen, Methoden und Werkzeuge aufgreifen.

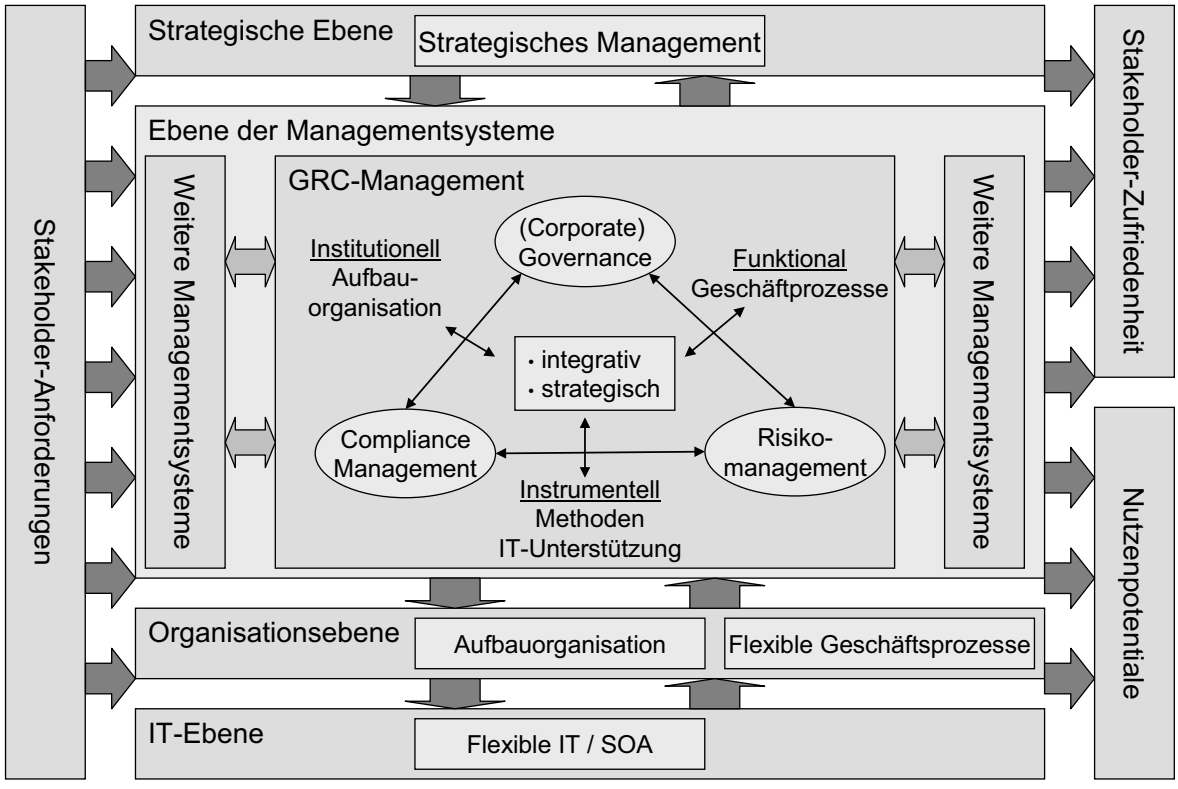

Bild 1: Bezugsrahmen des strategischen GRC-Managements

Das strategische GRC-Management verfolgt die Ziele der Stakeholder-Zufriedenheit (Erfüllung der Anforderungen) und der Verwirklichung von Nutzenpotentialen. Der Bereich GRC wird mit einer Vielzahl von potentiellen Nutzeneffekten in Verbindung gebracht (Bace und Rozwell 2006; Kranawetter 2009, S. 28; PwC 2007, S. 7-8;). Nutzenpotentiale bestehen hierbei in verschiedenen Bereichen. Hierzu gehören Nutzeffekte für die internen und externen Stakeholder (GRC-bewusste Unternehmenskultur, höhere Unternehmensreputation, gesteigerter Markenwert), die strategische Ebene (bspw. Flexibilitätssteigerung bei M&A-Aktivitäten, Markteintritt und neuen Produkten sowie Verbesserung der Informationsversorgung), Nutzeffekte für das GPM (bspw. Anregungen zur Geschäftsprozessoptimierung) sowie Nutzen im GRC-Management selbst (bspw. durch synergiebedingte Kostensenkungen).

Inhaltlich kann das GRC-Management durch die drei Perspektiven des Begriffs Management (Reiß und Corsten 1995, S. 6-9) vollständig strukturiert werden. Die *institutionelle* Perspektive beschreibt die Aufbauorganisation sowie Rollen und Verantwortlichkeiten. Die *funktionale* Perspektive beschreibt alle Handlungen, die der Steuerung der Leistungsprozesse dienen und umfasst eine Beschreibung der GRC-bezogenen Abläufe im Unternehmen. Die *instrumentelle* Sicht umfasst die Gesamtheit der Hilfsmittel bei der Ausübung von Managementaufgaben - hier sind das Methoden, Instrumente und unterstützende IT-Systeme des GRC-Managements.

4.3 Perspektiven des strategischen GRC-Managements

Da die Erfüllung der Anforderungen im Rahmen der operativen Geschäftsprozesse erfolgt und diese das zentrale Gestaltungsobjekt sind, erscheint ein geschäftsprozessorientiertes Organisationskonzept sinnvoll. Auf der Basis der Vorschläge zur Aufbauorganisation des Risiko- und Compliancemanagements (Bace und Rozwell 2006; Menzies 2006, S. 389-393; Pupke 2008, S. 79; Wolf 2003, S. 117) können folgende einheitliche Organisationseinheiten und Rollen für GRC abgeleitet werden.

- Das *GRC-Office* als Stabsstelle der Unternehmensleitung dient zur strategischen Ausrichtung und zentralen Koordination und setzt sich aus Geschäftsführung und tangierten Funktionsverantwortlichen (CIO, CFO, Leiter Recht usw.) zusammen.

- Das *GRC-Competence-Center* ist verantwortlich für die methodische und inhaltliche Integration einzelner Anforderungen und bindet Experten anderer Managementsysteme fallweise mit ein. Hier liegt auch die Verantwortung für eine laufende Aktualisierung und Kommunikation des GRC-Wissens in der Organisation.
- *GRC-Verantwortliche* sind GRC-Experten für einzelne, von GRC-Anforderungen betroffene Geschäftsprozesse und unterstützen die Prozessbeteiligten bei der Erfüllung der GRC-Anforderungen. Sie arbeiten eng mit den Prozessverantwortlichen zusammen oder haben diese Rolle selbst inne.
- *Prozessbeteiligte* erfüllen die Anforderungen im Zuge der operativen Tätigkeiten.

Die Ablauflogik des strategischen GRC-Management lässt sich in Anlehnung an den Kreislauf des GPMs (Allweyer 2005) und Vorgehensmodelle des Risiko- (Wolf 2003, S. 51) und Compliancemanagements (Pupke 2008, S. 30-31) strukturieren (Bild 2). Ausgehend von der Identifikation der Stakeholder und ihrer Anforderungen, dem Abgleich mit der Unternehmensstrategie und der Definition von GRC-Zielen (Identifikation/ Strategie) werden die gegebenen Anforderungen analysiert und GRC-konform angepasst (Anlyse/Design). Anschließend erfolgt die organisatorische und informationstechnische Implementierung (Implementierung). In der Phase Ausführung/ Dokumentation ergeben sich aus Managementsicht die Aufgaben der Unterstützung der Prozessbeteiligten und der Datengewinnung für das Controlling, welches sich letztlich auf die Erfüllung der Anforderungen, die GRC-Ziele und da Nutzenpotentiale erstreckt (Controlling).

Für GRC existieren Treiber, die eine Anpassung des GRC-Managements erfordern. Solche Treiber können interne oder externe Einflüsse sein, die Auswirkungen auf das strategische GRC-Management haben. Zu den Treibern gehören neue Geschäftsprozesse, neue Produkte oder Märkte, M&A-Aktivitäten, neue IT-Systeme, neue Geschäftspartner und neue/veränderte GRC-Anforderungen (Menzies 2006, S. 359). Die in Bild 2 angedeutete zyklische Vorgehensweise zielt auf eine kontinuierliche Verbesserung des GRC-Managements.

Zur vollständigen Beschreibung des Ansatzes müssen alle Perspektiven des Begriffs Management berücksichtigt werden. Hierzu werden die Aktivitäten der einzelnen Phasen den verwendeten Methoden und ausführenden Rollen bzw. Organisationseinheiten zugeordnet. Im Folgenden soll die Phase Analyse und Design aus Bild 2 beispielhaft

betrachtet werden. Dabei werden die Aktivitäten und verwendeten Methoden bzw. Instrumente kurz erläutert. Bild 3 liefert hierzu einen tabellarischen Überblick.

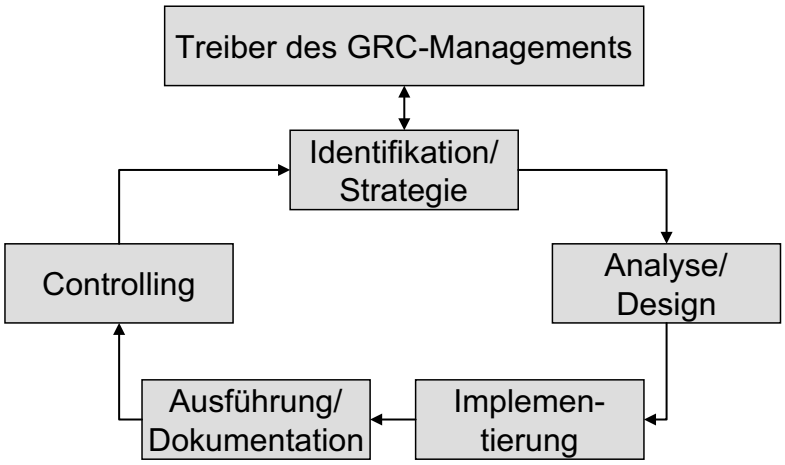

Bild 2: Managementzyklus des strategischen GRC-Managements

AKTIVITÄTEN	**METHODEN**	**BETEIIGTE ROLLEN**
Analyse der Stakeholderanforderungen	Corporate Rule Base	GRC-Office, GRC-Competence-Center
Analyse von Organisation/-Geschäftsprozessen hinsichtlich der Stakeholderanforderungen	Corporate Rule Base	GRC-Competence-Center; GRC-Verantwortliche
Analyse der Synergiepotentiale von GRC-Aktivitäten	Auswertungen der Corporate Rule Base	GRC-Competence-Center; GRC-Verantwortliche
Analyse der Prozesse hinsichtlich des Risikos der Flexibilisierung	Methoden der Risikoanalyse	GRC-Competence-Center; GRC-Verantwortliche
Ableitung von GRC-Policies	Lebenszyklus von Policies	GRC-Competence-Center; GRC-Verantwortliche
GRC-konformes Design der Geschäftsprozesse	Modellierungsmethoden	GRC-Verantwortliche, Prozessbeteiligte

Bild 3: Überblick zu der Phase Analyse und Design

Die Aktivität der Analyse der Stakeholderanforderungen sichtet die zuvor identifizierten Anforderungen (Verträge, Gesetze, freiwillige Vorgaben) und ordnet diese, soweit möglich, in Vorbereitung ihrer Umsetzung verfügbaren Best Practices zu, wie beispielsweise im IT-Bereich COBIT und ITIL. Danach werden die von den Anforderungen betroffenen Geschäftsprozessen und Organisationseinheiten identifiziert. Darauf aufbauend können die betroffenen IT-Systeme gefunden werden. Zur Unterstützung der ersten beiden Aktivitäten ist das Konzept der Corporate Rule Base (Menzies 2006) geeignet, die eine strukturierte Erfassung aller Stakeholderanforderungen erleichtert. Zusätzlich zu den bereits angeführten Informationen kann diese bspw. Informationen zur strategischen Geschäftseinheit, zum Gültigkeitsbereich, zum Non-Compliance Risiko sowie eine Priorisierung der Anforderungen enthalten.

Die Corporate Rule Base gibt somit einen Gesamtüberblick und dient außerdem zur leichteren Nachverfolgung von Gesetzesänderungen. Es bestehen hierbei verschiedene Möglichkeiten der technischen Implementierung, wobei eine relationale Datenbank mit Auswertungswerkzeugen auf Grund der hohen fachlichen Komplexität, des moderaten technischen Pflegeaufwands und der vielfältigen Analyse- bzw. Darstellungsmöglichkeiten sinnvoll ist. Denkbar sind hierbei Auswertungen nach Geschäftsprozessen oder Organisationseinheiten und Analysen zum Umsetzungsgrad der Stakeholderanforderungen in interne Policies (Menzies 2006, S.362-366). Auf der Grundlage dieser Auswertungen erfolgt die Analyse der Synergiepotentiale bei der Erfüllung der Anforderungen. Damit soll die heute vorherrschende isolierte Umsetzung einzelner Anforderungen in separaten GRC-Initiativen überwunden werden (PwC 2007, S.15). Zur Analyse der Synergiepotentiale können die Dimensionen „inhaltliche Ausrichtung, „methodischer Ansatz“ sowie die verschiedenen Integrationsrichtungen als Bezugspunkte dienen.

Die flexible Orchestrierung von IT-Services zu Geschäftsprozessen im SOA-Kontext stellt eine Herausforderung für GRC dar. Hierbei ist es bspw. nicht möglich, alle denkbaren Workflows im Voraus bzgl. ihres Risikos zu bewerten (Sackmann 2008, S.1137-1139) oder sicherzustellen, dass alle unterstützenden IT-Services compliant sind (Loosli 2008, S.10-12). Daher ist eine Analyse der Geschäftsprozesse bzw. IT-Systeme in Bezug auf das Non-Compliance Risiko einer flexiblen Anpassung durchzuführen, um die GRC-Konformität nicht zu gefährden. In Anschluss an die Analyse sind risikomindernde Maßnahmen zu definieren, so dass bspw. ein Genehmigungsprozess für die Änderung der IT-Unterstützung und/oder des Geschäftsprozesses implementiert wird (Loosli 2008, S.11).

Zu bevorzugen wäre ein automatisierter Entscheidungsprozess, der sowohl ökonomische als auch GRC-relevante Aspekte berücksichtigt (Sackmann et al. 2009).

Anschließend erfolgt die Definition der GRC-Policies, welche als zentrales Werkzeug zur unternehmensweit einheitlichen Umsetzung der Stakeholderanforderungen dienen. Es muss für jede GRC-Anforderung eine entsprechende Policy definiert sein. Die Erstellung der Policies erfolgt auf Grundlage der Ergebnisse der Corporate Rule Base und der Analyse der Synergiepotentiale. Da GRC-Anforderungen einer kontinuierlichen Veränderung unterliegen, haben Policies einen Lebenszyklus (El Kharbili 2008, S. 186).

Letztlich erfolgt das GRC-konforme Design der Geschäftsprozesse, wobei bestehende Geschäftsprozesse an Hand der Anforderungen angepasst werden. Hierbei können an die GRC-Thematik angepasste Prozessmodellierungsmethoden eingesetzt werden (siehe z.B. Karagiannis 2008; Rieke und Winkelmann 2008). Die Anpassung der bestehenden Geschäftsprozesse kann hierbei die Prozesslogik selbst betreffen (z.B. werden weitere Prozessschritte ergänzt), die aufbauorganisatorische Ausgestaltung (z.B. bei segration of duties) aber auch die informationstechnische Ausgestaltung (z.B. Automatisierung, Prüfroutinen) betreffen.

Weitere Forschungsaktivitäten richten sich auf eine Vertiefung, Anwendung und Evaluation des konzeptionellen Bezugsrahmens, wobei die Pharmaindustrie als beispielhaftes Anwendungsfeld dienen soll, da dieser ökonomische Sektor in fast allen funktionalen Bereichen stark reguliert ist. Hierbei sind sowohl ethische Anforderungen, als auch Zulassungsvorschriften und die Bereiche Produktsicherheit und Patientenschutz von besonderer Bedeutung.

Daneben ist auch die Frage einer IT-Unterstützung im strategischen GRC-Management von Interesse. Diese kann den in Bild 2 dargestellten Managementprozess betreffen, aber ebenso einzelne Aktivitäten und Methoden. Am Ende dieses Forschungszweiges soll eine IT-Referenzarchitektur für das strategische GRC-Management stehen.

Literaturverzeichnis

Allweyer T (2005) Geschäftsprozessmanagement. Strategie, Entwurf, Implementierung, Controlling. W3L, Bochum.

Bace J, Rozwell C (2006) Understanding the components of compliance. http://logic.stanford.edu/POEM/externalpapers/understanding_the_costs_of_c_138098.pdf. Abruf am 2009-02-23.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004) Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk.. www.coso.org/documents/COSO_ERM_ExecutiveSummary_German.pdf, Abruf am 2008-10-30.

Deloitte (2008) Growing confidence (the smart way to manage governance, risk, and compliance). http://www.myexpospace.com/OracleDemogrounds2008/PDFDOCLIB/GRC-growingconfidence.pdf. Abruf am 2009-08-28.

El Kharbili M, Stein S, Pulvermüller E (2008): Policy-based semantic compliance checking for business process management. In: Proceedings Modellierung betrieblicher Informationssysteme: Modellierung zwischen SOA und Compliance Management (MobIS 2008), Saarbrücken.

Freeman RE (1984) Strategic management. a stakeholder approach. Pitman, Boston.

Gleißner W (2008) Grundlagen des Risikomanagements. Vahlen, München.

Götz B, Köhntopp F, Mayer B, Wagner G (2008) Einsatz einer ganzheitlichen GRC-Softwarelösung. In: HMD – Praxis der Wirtschaftsinformatik 45(5):89-98.

Hauschka C (2007) Handbuch der Haftungsvermeidung im Unternehmen. Beck, München.

Johannsen W, Goeken M (2006) IT-Governance – neue Aufgaben des IT-Managements. In: HMD – Praxis der Wirtschaftsinformatik 43(4):7-20.

Karagiannis D (2008) A business process-based modeling extension for regulatory compliance. In: Tagungsband der Multikonferenz Wirtschaftsinformatik 2008, München, S.1159-1173.

Klotz M (2007) IT-Compliance auf den Kern reduziert. In: IT-Governance 1(1):14-18.

Klotz M, Dorn DW (2008) IT-Compliance – Begriff, Umfang und relevante Regelwerke. In: HMD – Praxis der Wirtschaftsinformatik 45(5):5-14.

Kranawetter M (2009) Nutzenpotentiale regulatorischer Anforderungen zur Geschäftsoptimierung. IT-Infrastruktur Compliance Reifegradmodell für Geschäftsführung, Compliance- und IT-Verantwortliche. http://download.microsoft.com/download/0/8/2/082A3349-3E6B-4D5D-9A65-70B3F2C3E705/Compliance_Whitepaper_13_FINALE.PDF. Abruf am 2009-08-28.

Loosli G (2008) Compliance-Prüfung bei Anwendung dynamischer Bindung in serviceorientierten Architekturen. In: Proceedings Modellierung betrieblicher Informationssysteme: Modellierung zwischen SOA und Compliance Management (MobIS 2008), Saarbrücken.

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):383-391.

Mallin CA (2007) Corporate Governance. 2. Auflage, Oxford University, Oxford.

Menzies C (2006) Sarbanes-Oxley und Corporate Compliance – Nachhaltigkeit, Optimierung, Integration. Schäffer-Poeschel, Stuttgart.

Nissen V, Mladin, A (2009) Messung und Management von IT-Agilität. In: HMD – Praxis der Wirtschaftsinformatik 269: 42-51.

Papazoglou M, Traverso P, Dustdar S, Leymann F (2006) Service-Oriented Computing Research Roadmap. In: Service Oriented Computing - Dagstuhl Seminar Proceedings, Dagstuhl.

PricewaterhouseCoopers AG (PwC) (2007) White Paper. Governance, Risikomanagement und Compliance: Nachhaltigkeit und Integration unterstützt durch Technologie, Frankfurt am Main.

Pupke D (2008) Compliance and corporate performance: the impact of compliance coordination on corporate performance. Books on Demand, Norderstedt.

Österle H, Blessing D (2003) Business Engineering Modell. In: Österle H, Winter, R (Hrsg): Business Engineering. Auf dem Weg zum Unternehmen des Informationszeitalters. 2.Auflage, Springer, Berlin.

Rappaport A (1999) Shareholder Value. Wertsteigerung als Maßstab für die Unternehmensführung. 2.Auflage, Schäffer-Poeschel, Stuttgart.

Reiß M, Corsten H (1995) Schnittstellenfokussierte Unternehmensführung. In: Corsten, H.; Reiß, M. (Hrsg.): Handbuch Unternehmensführung. Konzepte – Instrumente – Schnittstellen. Gabler, Wiesbaden.

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):346-356.

Sackmann, S (2008) Assessing the effects of IT Changes on IT Risk – A business process-oriented view. In: Proceedings MKWI 2008: 1137-1148.

Sackmann S, Kähmer, M (2008) ExPDT: A Layer-based approach for automating compliance. In: Wirtschaftsinformatik 50(5): 366-374.

Sackmann S, Lowis L, Kittel, K (2009) A risk based approach for selecting services in business process execution. In: Proceedings WI 2009: 357-366.

Scholz C (2000) Strategische Organisation. Multiperspektivität und Virtualität. 2.Auflage, Moderne Industrie, Landsberg.

Stölzle W (2002) Logistikforschung – Entwicklungszüge und Integrationsperspektiven. In: Stölzle W, Gareis K. (Hrsg) Integrative Management- und Logistikkonzepte. Gabler, Wiesbaden: 511 – 527.

Strohmeier G (2007) Ganzheitliches Risikomanagement in Industriebetrieben. Grundlagen, Gestaltungsmodell und praktische Anwendung. DUV, Wiesbaden.

Tarantino A (2007) Governance, risk and compliance handbook: technology, finance, environmental, and international guidance and best practices. Wiley, Hoboken.

Teubner A, Feller T (2008) Informationstechnologie, Governance und Compliance. In: Wirtschaftsinformatik 50(5): 400-407.

Witt P (2003) Corporate Governance-Systeme im Wettbewerb. DUV, Wiesbaden.

Wolf K (2003) Risikomanagement im Kontext der wertorientierten Unternehmensführung. DUV, Wiesbaden.