Anforderungen an ein strategisches GRC-Management

Wolfgang Marekfia, Volker Nissen
Fachgebiet Wirtschaftsinformatik für Dienstleistungen
Technische Universität Ilmenau
98684 Ilmenau
wolfgang.marekfia@googlemail.com, volker.nissen@tu-ilmenau.de

Abstract: Obwohl zunehmend integrierte Ansätze für Corporate Governance, Risiko- und Compliance-Management (GRC) gefordert werden, ist weitestgehend unklar, welche Anforderungen ein solcher Ansatz erfüllen sollte. Dieser Beitrag arbeitet daher Anforderungen an einen strategischen GRC-Management-Ansatz heraus und diskutiert diese anhand einschlägiger Theorien.

1 Motivation

Die Vernachlässigung von GRC kann, wie einschlägige Beispiele zeigen, für Unternehmen zu gravierenden ökonomischen Konsequenzen führen. GRC ist von hoher Komplexität und steigenden Kosten geprägt [AIS10, 252]. Gleichzeitig erfordert die zunehmende Marktdynamik eine agile und kontextspezifische Anpassung der Geschäftsprozesse, was für GRC eine Herausforderung darstellt [Mü07, 109; Sa08b, 1137-1138]. GRC ist derzeit durch eine Vielzahl von Themen geprägt, die sich in der Unternehmenspraxis oft in isolierten Initiativen widerspiegeln [Ge09, 1]. Bestehende Abhängigkeiten werden nicht berücksichtigt, was die Nutzung von Synergien verhindert. Zwischen Normkonformität und strategischer Zielerreichung wird ein „trade-off“ [BGJ09, 7] vermutet und GRC als „Kostenverursacher“ betrachtet, wodurch eine Ausrichtung von GRC an den Geschäftszielen erschwert wird. Durch reaktives und isoliertes Vorgehen bleiben außerdem Nutzenpotentiale oftmals ungenutzt. In Forschungsarbeiten werden derzeit überwiegend Detailfragen diskutiert, wobei unbeantwortet bleibt, wie die vereinzelten Vorschläge in einen umfassenden Ansatz zu integrieren sind. Obwohl erste Arbeiten zu intergierten GRC-Ansätzen existieren [Me06; Op09; RWS10b] fehlt ein Gesamtüberblick ebenso wie abgestimmte Vorgehensweisen, Methoden und Werkzeuge. Außerdem ist nicht klar, welchen Anforderungen ein GRC-Management-Ansatz genügen muss. Neben den IT-bezogenen Vorarbeiten sind hierbei auch organisatorische Aspekte zu berücksichtigen, da der Wertbeitrag von IT langfristig signifikant steigt, wenn ihr Einsatz durch geeignete Organisationskonzepte komplementär unterstützt wird [TKG04].

Die ursprünglich abgegrenzten Konzepte für die Teilaufgaben von GRC weiten sich auf Grund aktueller Herausforderungen aus und konvergieren. Die jeweils gewählten Perspektiven bleiben jedoch noch recht verschieden. Ein hohes Integrationspotential zwischen den GRC-Teilaufgaben lässt sich konstatieren, da eine Vielzahl von Berührungspunkten existieren [TF08], wobei sich die Konzepte auf verschiedene Hierarchieebenen konzentrieren [Me06, 334-336]. Racz [RWS10a, 8] schlägt eine Definition für GRC vor, die sehr allgemein bleibt und im Wesentlichen den Integrationsaspekt von GRC heraus-

stellt. Weitere mögliche Anforderungen werden vernachlässigt. Von besonderer Bedeutung für das Thema GRC ist die IT-Unterstützung, nicht zuletzt, da heute praktisch alle Geschäftsprozesse IT-gestützt ablaufen. Die Berechtigung separater Ansätze für ausschließlich IT-bezogene Aspekte von GRC wird aufgrund der ähnlichen methodischen Vorgehensweise mit unternehmensweiten, generellen GRC-Ansätzen in der Literatur in Frage gestellt [RWS10c]. Dem hier dargestellten Forschungsvorhaben liegt neben der Integration von GRC die Idee eines proaktiven und strategisch ausgerichteten GRC-Managements zugrunde, das als strategisches GRC-Management bezeichnet wird. Strategisches GRC-Management fokussiert im Kern nicht die Normerfüllung und die Durchführung der risikosteuernden Maßnahmen, sondern Ziel ist es, eine umfassende Planung und Steuerung des GRC-Status zu ermöglichen, die Teilaspekte zu integrieren, an den strategischen Zielen des Unternehmens auszurichten und kontinuierlich zu verbessern.

Die Forschung zu integrierten GRC-Ansätzen befindet sich noch am Anfang. Daher ist es das Gesamtziel des hier in Ausschnitten beschriebenen Forschungsvorhabens, die Entwicklung einer umfassenden Forschungsagenda. Die in diesem Beitrag dargestellten Anforderungen an einen strategischen GRC-Management-Ansatz stellen eine Vorarbeit zur Entwicklung der Forschungsagenda dar. Die Anforderungen sollen zur Diskussion des Forschungsstandes und zur Herleitung des weiteren Forschungsbedarfs dienen und sicherstellen, dass hierbei keine relevanten Forschungsbereiche vergessen werden. In diesem Beitrag wird die Forschungsmethode des Literatur-Reviews adaptiert [Fe06; BSN09], wobei als Ziel die Herleitung von Anforderungen an ein strategisches GRC-Management verfolgt wird. Die Vorgehensweise und dieser Beitrag gliedern sich wie folgt. Zuerst wird eine systematische Literatursuche vorgenommen. Hierauf aufbauend werden, die relevanten Theorien in der GRC-Literatur identifiziert. Anschließend werden Anforderungen an das strategische GRC-Management aus der Literatur hergeleitet und anhand der relevanten Theorien diskutiert. Der Beitrag schließt mit einem Fazit.

2 Literatursuche

Da sich die Forschung zu integrierten GRC-Ansätzen noch in einem frühen Stadium befindet, werden neben Publikationen zu integrierten GRC-Management-Ansätzen auch Arbeiten aus den Teildisziplinen von GRC berücksichtigt. Für die Literatursuche wird die Methode von vom Brocke et al. [BSN09] aufgegriffen, wobei die Empfehlung der Fokussierung auf qualitativ-hochwertige Veröffentlichungen (wissenschaftliche Zeitschriften bzw. Konferenz-Proceedings) berücksichtigt ist. In einem ersten Schritt erfolgt die Auswahl von wissenschaftlichen Zeitschriften und Konferenzen. Diese Auswahl ermöglicht die Identifikation von geeigneten Datenbanken für eine Suche mit Schlagwörtern. Die hierbei gefundenen Veröffentlichungen werden dann inhaltlich auf ihre Relevanz geprüft. Auf Grund der Vielzahl der durch die bisher beschriebenen Schritte gefundenen Publikationen wird auf eine Vorwärts- und Rückwärtssuche verzichtet. Außerdem ist die Suche zeitlich auf die Jahre 2005 bis 2011 beschränkt, was durch die Neuigkeit des Themas begründet werden kann. Als Zeitschriften wurden die mit A bewerteten Journale der WKWI-Journalliste und des VHB-JOURQUAL2 Zeitschriftenrankings ebenso wie die ersten zehn gelisteten Journale des MIS Journal Rankings ausgewählt. Als Konferenzen wurden die der Kategorie A zugeordneten Konferenzen der

WKWI-Liste der Konferenzen, Proceedings und Lecture Notes berücksichtigt. Weitere Konferenzen und Zeitschriften wurden nach Relevanz und Qualität (bspw. sichergestellt durch Peer-Reviews) ausgewählt, wodurch auch GRC-spezifische Publikationsorgane berücksichtigt wurden. Zu den identifizierten Datenbanken gehören u.a. ACM Digital Library, AISeL, EBSCOhost, ScienceDirect und SpringerLink. Zeitschriften bzw. Konferenz-Proceedings, die nicht mit Hilfe einer wissenschaftlichen Datenbank durchsucht werden konnten, wurden an Hand der jeweiligen Homepage analysiert. Zur Identifikation potentiell relevanter Arbeiten wurde nach Möglichkeit eine Suche in Titeln, Schlüsselwörtern und Abstracts vorgenommen, um Arbeiten die GRC nur am Rande thematisieren auszuschließen. Zusätzlich erfolgte eine manuelle Suche in den Table of Contents der Zeitschriften, um auch relevante Arbeiten zu finden, die nicht explizit die Begriffe Governance, Risk bzw. Risiko und Compliance verwenden. Inhaltlich wurden Arbeiten ausgewählt die allgemein relevant für das GRC-Management sind bzw. bei welchen zu erwarten ist, dass sie zur Herleitung von Anforderungen an das GRC-Management beitragen. Zusätzlich wurden selektiv weitere besonders relevante Veröffentlichungen bspw. zu integrierten GRC-Ansätzen, praxisnahe Publikationen (White Papers, Handbücher, Standards und Best Practices) und Dissertationen durch eine Online-Recherche identifiziert. Hierbei wurden allgemeine Suchmaschinen wie google bzw. googlescholar sowie Bibliotheksdatenbanken wie der Gemeinsame Verbundkatalog (GVK) herangezogen. Insgesamt liegen dem Literatur-Review 191 relevante Publikationen zu Grunde.

3 Theoretische Grundlagen

Theorien dienen allgemein der Erklärung und Vorhersage. Weiterhin können Abstraktion und Verallgemeinerung, Interaktion sowie Kausalbeziehungen als bedeutende Eigenschaften von Theorien genannt werden [FWW10, 383; Gr06a, 614-618]. Die Bedeutung der Anwendung von Theorien als Grundlage zur Konstruktion von Artefakten wird in der gestaltungsorientierten Forschung explizit betont (bspw. [WWS92, 42]). Welche Theorien für das strategische GRC-Management relevant sind, ist bislang nicht eindeutig geklärt. Es existiert jedoch eine Vielzahl potentiell relevanter Theorien. Die Auswahl von Theorien für ein neues Forschungsgebiet ist schwierig, da sich die Theorien kaum anhand formaler Kriterien strukturieren lassen und etablierte Kriterien für die Prüfung der Relevanz nicht verfügbar sind (bspw. [Wo05, 434-443]). Bei der Durchsicht der relevanten Literatur konnte festgestellt werden, dass eine Vielzahl theoretischer Perspektiven angewendet und somit als relevant erachtet wird. Diese Theorien wurden zunächst erfasst und grob in die drei Gruppen strategisch, ökonomisch und verhaltenswissenschaftlich strukturiert. Anhand der Verwendung der Theorien in der Literatur konnten diese in einem zweiten Schritt den Anforderungen an ein strategisches GRC-Management zugeordnet werden. Es ist anzumerken, dass einige der in der Literatur verwendeten Theorien im vorliegenden Review nicht berücksichtigt wurden, da sie ein nur geringes Erklärungspotential hinsichtlich der hier fokussierten strategischen GRC-Anforderungen aufweisen. Nachfolgend werden die aus der gesichteten GRC-Literatur extrahierten Theorien in sehr kurzer Form charakterisiert und eingeordnet.

Strategische Theorien erklären die Entwicklung und Implementierung von Strategien zur Erreichung der Unternehmensziele. Als strategische Theorien erklären der Market-based

view [Po80] und der Resource-based-view [Pe59, We84, Ba91], aus der Perspektive der Marktpositionierung bzw. der Ressourcen die Entstehung von strategischen Wettbewerbsvorteilen. Die Stakeholdertheorie [Fr84] fordert eine Ausrichtung der unternehmerischen Entscheidungen an den Interessen aller Stakeholder (bspw. Mitarbeiter, Eigentümer, Kunden). Der Shareholder-Ansatz orientiert sich lediglich an den Interessen der Eigentümer (Shareholder) und fordert die Maximierung des Shareholder Values [Ra99, 39]. *Ökonomische Theorien* betrachten die Koordination von Akteuren. Die Transaktionskostentheorie [Wi85] besagt, dass für die effiziente Koordination einer Transaktion neben den Produktionskosten auch die Transaktionskosten entscheidend sind. Die Prinzipal-Agenten-Theorie [JM76] geht von unterschiedlichen Interessen des Prinzipals und Agenten aus. Daher ist durch Kontrollen (bspw. Überwachung oder Anreizsysteme) sicherzustellen, dass der Agent im Interesse des Prinzipals handelt. Die Organizational Control Theorie [Ou79] setzt sich konkret mit der Ausgestaltung dieser Kontrollen auseinander. Die Stewardship-Theorie ist ein alternativer Vorschlag, wobei eine Vertrauensbeziehung und Zielkonformität zwischen Prinzipal und „Steward" unterstellt wird. *Verhaltenswissenschaftliche Theorien* erklären Beziehungen zwischen Individuen und Gruppen bzw. das menschliche Verhalten im Allgemeinen. Die institutionalistische Theorie [DP83] trägt zur Erklärung von organisatorischen Strukturen bei, die der Theorie folgend Ergebnis der Institutionalisierung von Anforderungen verschiedener Anspruchsgruppen und nicht ausschließlich Ergebnis rationaler Überlegungen sind. Die Theory of Reasoned Action [FA75] postuliert eine Kausalbeziehung zwischen Meinungen, Einstellungen, Verhaltensintentionen und dem tatsächlich ausgeführten Verhalten. Die Theory of Planned Behavior [Aj85] erweitert diese Theorie, welche nur auf willentliches Verhalten anwendbar ist, um die wahrgenommene Verhaltenskontrolle. Das Technology Acceptance Model [Da86] ist eine Adaption der Theory of Reasoned Action zur Erklärung der Akzeptanz von Informationssystemen. Die Protection Motivation Theory [Ro83] erklärt ablehnendes Verhalten durch die Schutzmotivation (protection motivation) und betont insbesondere die Bedeutung der persönlichen Betroffenheit und das gegenseitige Abwägen von Handlungsalternativen für das Verhalten. Die General Deterrance Theorie untersucht die Funktionsfähigkeit von Gegenmaßnahmen [SW98] und betont die Bedeutung der Zuverlässigkeit, Härte und Schnelligkeit von Sanktionen.

4 Herleitung der Anforderungen an strategisches GRC-Management

Eine Anforderung ist hier eine Bedingung oder Fähigkeit, die benötigt wird, um ein Problem zu lösen bzw. Ziel zu erreichen (vgl. IEEE Standardglossar). Es sind weiterhin Anforderungen und Lösungskomponenten zu unterscheiden. Letztere sind als gestaltungsorientierte Artefakte zu verstehen und werden auf der Basis der relevanten Anforderungen konstruiert. Walls et al. [WWS92] fordern außerdem eine theoretische Begründung der Anforderungen. Methodisch wurde zur Herleitung der Anforderungen die qualitative Inhaltsanalyse aufgegriffen. Bei der Datenanalyse sind die Kodierungstypen offenes, axiales und selektives Kodieren zu unterschieden. Im Zuge des offenen Kodierens wird der Text „geöffnet". Solche Aussagen, die einander ähneln, werden in sogenannte Kernkategorien zusammengeführt. Axiales Kodieren entwickelt diese Kategorien weiter, um eine höhere Abstraktionsebene zu erreichen und die Daten zu reduzieren. Durch selektives Kodieren erfolgt die Integration der gefundenen Konzepte und Grup-

pierung um ein Hauptthema. Dann können gezielt weitere Daten erhoben und nachkodiert werden. Die qualitative Inhaltsanalyse kann sowohl zur Auswertung von transkribierten Interviews als auch von wissenschaftlichen Publikationen dienen [BMM06, 70-75]. Im Kontext der Gewinnung von stilisierten Fakten wird ebenfalls eine Auswertung von Publikationen mit Hilfe der qualitativen Inhaltsanalyse vorgeschlagen [HFL11]. Ähnlich wie für stilisierte Fakten kann auch für die Entwicklung der Anforderungen argumentiert werden, dass der Hauptteil des vorhandenen Wissens in Form von publizierten Texten vorliegt, die sowohl Ergebnisse aus empirischer Forschung als auch konzeptionelle Überlegungen beinhalten und somit derzeit als geeignetste Quelle erscheinen. Konkret wurde zur Herleitung der Anforderungen wie folgt vorgegangen. Nach intensiver Lektüre der als relevant identifizierten Publikationen wurden besonders wichtige Textpassagen extrahiert und nach MS Excel ™ übernommen. Hier wurden die Textstellen sortiert und in einem ersten Schritt kategorisiert. Ergänzend hierzu wurden diese Unterkategorien, nach mehrfacher Überarbeitung, zu Anforderungskategorien zusammengeführt, welche die höchste Abstraktionsebene darstellen. Pro Quelle und Unterkategorie wurde nur eine Textstelle kodiert. Um ein Anzeichen der Stärke der Evidenz der Kategorien zu erhalten, ist in Tab. 1 die absolute Anzahl der kodierten Textstellen (Spalte „Kod. Textst.“) je Kategorie angegeben. Es ist zu beachten, dass durch die wörtliche Übernahme von Textstellen implizite Annahmen nicht berücksichtigt werden konnten.

Anforderungskategorie	**Unterkategorien**	**Kod. Textst.**	**Relevante Theorien**
Strategische Ausrichtung	GRC als strategische Chance, "trade-off" zwischen GRC und strategischer Zielerreichung, Nutzenpotentiale, Stakeholder-Orientierung	38	Market-based-view, Resource-based-view, Stakeholdertheorie, Shareholdertheorie
Integration	Inhaltliche Integration, Integration in die operativen Geschäftsprozesse, methodische und informationstechnische Integration	34	Transaktionskostentheorie
Geschäftsprozessorientierung	Bedeutung der Geschäftsprozesse für GRC, Integration von Geschäftsprozess- und GRC-Management, Bedeutung der Geschäftsprozessorientierung für die Automatisierung von GRC	30	Transaktionskostentheorie
Management-Systeme	N/A	8	Transaktionskostentheorie, (Neo-) Institutionalistische Theorie
Automatisierung	N/A	25	Transaktionskostentheorie, Prinzipal-Agenten-Theorie, Organisational Control Theorie
Flexible Geschäftsprozesse und IT-Systeme	N/A	15	Prinzipal-Agenten-Theorie, Stewardship-Theorie
Menschliche Faktoren	Compliance-Verhalten, GRC-Kultur, Kommunikation („tone at the top“)	37	Theory of Reasoned Action/Planned Behavior, Technology Acceptance Model, Protection Motivation Theory, General Deterrence Theory, Prinzipal-Agenten-Theorie, Organizational Control Theorie

Tabelle 1: Ergebnisse der qualitativen Inhaltsanalyse der einschlägigen Literatur

5 Darstellung und theoretische Analyse der Anforderungen

In diesem Abschnitt sollen die Anforderungen dargestellt und anhand relevanter Theorien aus der GRC-Literatur (vgl. Tab. 1) diskutiert werden. Zu jeder Kategorie werden Guidelines auf Basis der diskutierten Anforderungen formuliert, welche die theoretischen Erkenntnisse für weitere Forschungsvorhaben verdichten sollen.

Strategische Ausrichtung

Obwohl zwischen Normkonformität und den Geschäftszielen grundsätzlich ein „trade-off" angenommen wird [BGJ09, 7], weisen einige Autoren darauf hin, dass GRC auch als eine strategische Chance aufgefasst werden kann (bspw. [AIS10, 262; Bö08, 21; KM09, 42; Op09, Intro 16; Pr07, 11; RWS10a, 6; Ra10, 4]). In diesem Zusammenhang wird oftmals beklagt, dass GRC derzeit überwiegend als Kostenverursacher wahrgenommen wird und Nutzenpotentiale vernachlässigt werden (bspw. [AIS10, 262]). Das strategische Potential von GRC wird insbesondere im Kontext von integrierten GRC-Ansätzen betont (bspw. [Op09, Intro 16; Pr07, 11; RWS10a, 6; Ra10, 4]). Neben diesem strategischen Potential werden operative Nutzenpotentiale von GRC aufgeführt (bspw. [Bö08, 26-27; Kl09, 17-19; Kr09, 25; Op09, 18; WAM07, 56-57]). Außerdem wird eine Ausrichtung von GRC an den Stakeholderinteressen gefordert [Me06, 2; Op09, 6]. Krell und Matook [KM09] kommen im Rahmen ihrer Analyse zu zwei Erkenntnissen, die hier relevant sind. Zum einen betonen sie die inhaltliche Abhängigkeit und häufige Kombination von geschäftlichen und GRC-Investitionen. Demnach muss GRC zwangsläufig im Zusammenhang mit den Geschäftszielen betrachtet werden. Zum anderen wird anhand der generischen Wettbewerbsstrategien [Po80] die Beziehung von Compliance und Geschäftszielen aufgezeigt. So können bei einer Preisführerschaft zusätzliche Kosten von GRC, auch wenn hierdurch ein hoher Compliance-Grad ermöglicht wird, nicht an die Kunden weitergegeben werden, da für diese lediglich der Preis ausschlaggebend für die Kaufentscheidung ist. Durch höhere Kosten kann somit die strategische Position sogar gefährdet werden. Bei einer Differenzierungsstrategie kann durch einen höheren Compliance-Grad, bspw. durch Umsetzung von Standards, dann ein Wettbewerbsvorteil erwartet werden, wenn hiermit die Kaufbereitschaft der Kunden beeinflusst wird.

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

Mossanen [Mo10] untersucht die Ressourcen der Compliance anhand der Kriterien von Barney [Ba91, 105-112]. Er kommt zu dem Schluss, dass durch Compliance kein strategischer Wettbewerbsvorteil erzielt werden kann, obwohl vermutlich eine strategische Bedeutung von Compliance bzw. GRC im Sinne eines Einflusses auf den Kundennutzen oder zumindest den Nutzen von weiteren Stakeholdern (bspw. Anlegern) vermutet werden kann. Dies kann auch damit begründet werden, dass für GRC zukünftig etablierte Management-Ansätze verfügbar sein werden. Für Unternehmen, die jetzt einen überlegenen GRC-Ansatz entwickeln, ist daher kaum zu erwarten, dass dieser langfristig erhalten bleibt. Anzumerken ist, dass hiermit nicht ausgedrückt wird, dass GRC nicht zur Schaffung strategisch relevanter Ressourcen beitragen kann und GRC in Kombination mit anderen Ressourcen unter bestimmten Bedingungen zu einem nachhaltigen Wettbe-

werbsvorteil führen kann. In der Literatur wird hinsichtlich der IT/Business Value Debatte teilweise ein etwas anderer Untersuchungsrahmen auf der Grundlage des Resource-based-views eingenommen. Hierbei wird in einem ersten Schritt ein Einfluss der IT-Ressourcen auf die Geschäftsprozesse angenommen. Geschäftsprozessverbesserungen gehen mit operativen Effizienzsteigerungen einher. Die Frage, ob sich diese operativen Verbesserungen auch in finanziellen Messgrößen und in einen Wettbewerbsvorteil niederschlagen, wird also von dieser Frage getrennt [MKG04]. In der Literatur wird GRC mit einer Vielzahl von potentiellen Nutzeneffekten in Verbindung gebracht, welche über das reine Einsparen von Transaktionskosten hinausgehen und somit auch geschäftliche Verbesserungen bedeuten können.

Guideline 2: Die das GRC-Management konstituierenden Ressourcen ermöglichen zwar nicht die Entwicklung langfristiger Wettbewerbsvorteile, sollten jedoch die Erzielung operativer Nutzenpotentiale ermöglichen.

Die Forderung der Ausrichtung von GRC an den Stakeholdern, stellt die Frage nach dem Ziel des GRC-Managements. Grundsätzlich existieren mit der Shareholder- bzw. Stakeholder-Theorie zwei mögliche Erklärungsansätze. Die Richtlinien der Corporate Governance sowie regulatorische Vorgaben und Risikomanagement-Rahmenwerke wie COSO stellen zweifelsfrei die Interessen der Shareholder in den Mittelpunkt. Jedoch wird hierbei nicht unmittelbar die Maximierung des Shareholder Values gefordert, sondern Kontroll- und Offenlegungspflichten, die zur Lösung der Prinzipal-Agenten-Problematik beitragen sollen. Erweitert man die Betrachtungsweise auf alle Stakeholder, so werden die verschiedenen Interessen wie bspw. Datenschutz, Produktsicherheit oder Umweltschutz relevant. Es stellt sich die Frage, zu welchem Grad diese Interessen erfüllt werden sollen. Dies kann bedeuten, dass lediglich die gesetzlichen Mindestanforderungen erfüllt werden oder dass eine Übererfüllung gesetzlicher Vorgaben bspw. im Rahmen der Implementierung von Best Practices und Standards angestrebt wird. Letztlich kann diese Frage jedoch nur auf der Grundlage der Zielfunktion des Gesamtunternehmens beantwortet werden. Im Shareholder-Ansatzes wäre der spezifische Grad der Erfüllung der Stakeholder-Interessen am Shareholder-Value auszurichten. Wird dieser nicht in der kurzfristigen Maximierung der Aktienkurses gesehen, kann der Konflikt zwischen den beiden Ansätzen aufgelöst werden. D.h. durch die Maximierung des Shareholder-Values werden langfristig die Interessen aller Stakeholder bestmöglich erfüllt [Al01].

Guideline 3: GRC sollte an den Stakeholder-Interessen ausgerichtet werden. Die Stakeholder-Interessen sollten hierbei unter der Prämisse der langfristigen Maximierung des Unternehmenswertes ausbalanciert werden.

Integration

Die Integration von GRC wird in der Literatur unter inhaltlichen (bspw. [Ge09, 1; KD08, 7; Kr09, 24-25; Me06, 63-64; Op09, VIII; Pr07, 10; Ra10, 1; RWS10a, 6; RWS10b, 12]) und methodischen bzw. informationstechnischen Aspekten (bspw. [FB05, 404; Pr07, 8; Ra10, 5]) diskutiert. Die inhaltlichen Aspekte der Integration können in die Forderung der integrierten Erfüllung mehrerer Compliance-Vorgaben (bspw. [Me06, 63-64; Ra10, 1]) und die Forderung der Integration der GRC-Disziplinen unterteilt werden (bspw.

[Ge09, 1; KD08, 7; Kr09, 24-25; Me06, 63-64; Op09, VIII; Pr07, 10; Ra10, 1; RWS10a, 6; RWS10b, 12]). Außerdem wird eine Integration der GRC-Aktivitäten in die operativen Geschäftsprozesse gefordert (bspw. [Me06, 332-333; Op09, Intro 15; Pu08, 132]). Des Weiteren wird die Integration von IT-bezogenen und unternehmensweiten Ansätzen diskutiert (bspw. [RWS10c]). Da durch die Integration von GRC eine überlegende Koordinationsform geschaffen werden soll, ist die Transaktionskostentheorie anwendbar. Um an den theoretischen Untersuchungen von Pupke [Pu08] ansetzen zu können, wird hier ebenfalls die Vorgehensweise von Picot [Pi82, 273] aufgegriffen. Diese gliedert sich in die Schritte (1) Identifikation der Transaktionen und Analyse ihrer Eigenschaften, (2) Ermittlung der möglichen Koordinationsformen und (3) Auswahl der Koordinationsform mit den minimalen Kosten.

Determinante	**Management-Aktivitäten**		**Operative Aktivitäten**	
Transaktions-spezifität	Hoch	Für jede Risikoart und GRC-Vorgabe ist spezifisches Wissen erforderlich und es existiert Umsetzungsspielraum.	Niedrig	Es existieren klare Regeln, die jeweils für einzelne Geschäftsprozesse die Normerfüllung und Risikosteuerung festlegen.
Unsicherheit	Hoch	Unternehmen sind stetig mit neuen und veränderten Normen und Umweltbedingungen konfrontiert.	Niedrig	Die gegenwärtig gültigen Regeln sind klar definiert. Änderungen werden in die Vorgabedokumente integriert und kommuniziert.
Häufigkeit	Niedrig	Management-Aktivitäten werden überwiegend zyklisch (bspw. jährlich) ausgeführt.	Hoch	Die operativen Aktivitäten sind inhärenter Bestandteil jeder Geschäftsprozessausführung.
Eff. Koord.	**Zentral**		**Hybrid**	

Tabelle 2: Analyse der Determinanten zu den GRC-Transaktionen

Zu (1): Die das GRC-Management konstituierenden Transaktionen sind derzeit unklar, da noch keine etablierten Ansätze vorliegen. Für die vorliegende Untersuchung wird daher eine Unterscheidung in Management-Aktivitäten und operative Normerfüllung und Risikosteuerung (im Weiteren als operative Aktivitäten bezeichnet) vorgenommen. Diese Unterscheidung erfolgt in Übereinstimmung mit existierenden Ansätzen [Pu08, 71; RWS10b, 12]. Management beinhaltet die Aktivitäten Planung, Organisation, Führung, Koordination und Kontrolle [Fa49, 3]. Corporate Governance stellt einen Rahmen für das Compliance- und Risikomanagement zur Verfügung und ist somit eine Management-Aufgabe [RWS10b, 11]. Im Prozessmodell für GRC von Racz et al. [RWS10b, 12] lassen sich bspw. Management-Aktivitäten (Identifikation und Analyse von Risiken und Compliance-Vorgaben, Monitoring, Kommunikation) von der operativen Normerfüllung und Durchführung der Risikomaßnahmen abgrenzen. Die Analyse der Determinanten der Transaktionen ist in Tab. 2 dargestellt und orientiert sich an Pupke [Pu08, 72-75].

Zu (2) und (3): Bzgl. der möglichen Koordinationsformen von GRC unterscheidet Pupke [Pu08, 75-80] im Kontext von Compliance zwei Ebenen. Die erste Ebene beschreibt die Koordinationsformen für die Umsetzung einzelner Compliance-Vorgaben. Hierbei ist eine zentrale, hybride oder duale Koordination möglich. Bei der zentralen Koordination ist eine zentrale organisatorische Einheit für GRC verantwortlich, was auch einheitliche Managementprozesse, Methoden und Werkzeuge bedeutet. Im dualen Ansatz werden für GRC Organisationseinheiten der Sekundärorganisation (bspw. Projektorganisationen) einschließlich entsprechender Prozesse, Methoden und Werkzeuge geschaffen. Der hyb-

ride Ansatz integriert GRC direkt in die Primärorganisation. In einer zentralen Organisationseinheit kann spezifisches Wissen für GRC aufgebaut und schnell Entscheidungen getroffen werden. Wissen zu den Geschäftsanforderungen muss jedoch außerhalb dieser Einheit beschafft werden. Die duale Form nutzt teilweise Ressourcen der Primärorganisation und kann daher auch Wissen zu den Geschäftsanforderungen integrieren. Spezifisches GRC-Wissen kann jedoch nur bedingt aufgebaut werden. Die hybride Koordination nutzt vollständig die Ressourcen der Primärorganisation und hat somit bestmögliches Wissen über die Geschäftsanforderungen. GRC-Wissen lässt sich jedoch besonders schwierig aufbauen. Unter Einbeziehung der Transaktionsdeterminanten ergeben sich als effiziente Koordinationsformen der zentrale Ansatz für die Management-Aktivitäten und der hybride Ansatz für die operativen Aktivitäten (vgl. Tab. 2). Die zweite Ebene bezieht sich auf das Management verschiedener Compliance-Vorgaben, wobei ein integrierter von einem nicht-integrierten Ansatz unterschieden werden kann. Für diese Untersuchung wird mit der Integration der GRC-Teildisziplinen eine weitere Ebene relevant. Hierbei ist ebenfalls ein integrierter bzw. ein nicht-integrierter Ansatz denkbar. Für die Vorteilhaftigkeit der integrierten Erfüllung verschiedener Compliance-Vorgaben und der Integration der GRC-Teildisziplinen lassen sich folgende Gründe nennen.

Integrierte Erfüllung von Compliance-Vorgaben:

- *Allgemeine Überschneidungen:* Allgemeine Anforderungen an Vorgabedokumente (bspw. Arbeitsanweisungen), Dokumentationsstandards, Durchführung von Reviews und Audits
- *Synergien zwischen spezifischen Vorgaben:* Synergien zwischen Vorgaben in einer Domäne (bspw. SOX und Basel II zur Finanzberichterstattung [Pu08, 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 [AIS10] (bspw. SOX und KonTraG)

Integration der GRC-Teildisziplinen:

- 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 I bzw. im IT-Bereich Cobit, ITIL und ISO 27001/2)
- Non-Compliance als bedeutsame Risikokategorie [Wi10, 100].
- Governance als Rahmen für Risiko- und Compliance-Management [RWS10b, 11-12]

Guideline 4: Die für GRC relevanten Management-Aktivitäten sollten mit einem zentralen Ansatz (einschließlich integrierten Informationssystemen und Methoden) erfolgen. Die operativen Aktivitäten sollten in die operativen Geschäftsprozesse und IT-Systeme integriert werden (hybrider Ansatz).

Guideline 5: GRC sollte über verschiedene Compliance-Vorgaben als auch über die GRC-Disziplinen integriert werden.

Geschäftsprozessorientierung

Ein geschäftsprozessorientierter Ansatz wird in der Literatur auf Grund des direkten Zusammenhangs der Geschäftsprozesse mit dem ökonomischen Ergebnis sowie den Compliance-Vorgaben und Risiken gefordert (bspw. [Sa08b, 1137]). Außerdem wird die Bedeutung eines geschäftsprozessorientierten Ansatzes für die Automatisierung der Compliance-Sicherung betont [KSP08, 181]. Insgesamt wird auch eine Integration von GRC- und Geschäftsprozessmanagement (GPM) vorgeschlagen, da sich beide Konzepte

gegenseitig ergänzen (bspw. [KSP08; Me06, 333; RW08, 347]). So können Geschäftsprozessmodelle zur Identifikation von Risiken bzw. GRC-relevanten Bereichen herangezogen werden und dienen zur Kommunikation und Dokumentation [RW08, 347]. Außerdem ermöglichen diese neben der Automatisierung der Geschäftsprozesse auch die Automatisierung der relevanten Risiko- bzw. Compliance-Kontrollen [KSP08]. Das GPM nimmt eine ablauforientierte Sichtweise des Unternehmens ein, wofür etablierte Vorgehensmodelle, Methoden und Werkzeuge mit hohem Reifegrad existieren. Geschäftsprozessorientierte Ansätze haben sich in vielen Bereichen (bspw. Einführung von ERP-Systemen, Qualitätsmanagement) durchgesetzt. Aus Sicht der Transaktionskostentheorie ist ein wesentliches Ziel des GPMs die Senkung von Transaktionskosten.

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

Management-Systeme

In der Literatur wird eine Harmonisierung von GRC mit weiteren Management-Systemen gefordert, da GRC sich derzeit auf verschiedene Management-Systeme aufteilt. Zu diesen gehören 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) (bspw. [Bh09; Kl09, 13-16]). Hierbei stellt sich die Frage, wie die Aufgaben abgestimmt und koordiniert werden können. Grundsätzlich ist festzustellen, dass durch die Abstimmung und Koordination Transaktionskosten entstehen, die für die Management-Aktivitäten von GRC höher sind als bei zentraler Koordination und Integration über GRC-Vorgaben und -Disziplinen (siehe Anforderung Integration). Die Management-Systeme können jedoch aus verschiedenen Gründen nicht in das GRC-Management integriert werden. Der institutionalistischen Theorie folgend versuchen Unternehmen den Anforderungen unterschiedlicher Gruppen gerecht zu werden. Um eine Erfüllung dieser Anforderungen zu signalisieren, liegt die Implementierung separater Management-Systeme und entsprechender Stellen wie bspw. Datenschutz nahe. Hiermit ist teilweise jedoch auch nur eine symbolische Erfüllung verbunden (siehe im Kontext von Compliance [MB10]). Das Qualitätsmanagement oder die Interne Revision verlangen außerdem aufgrund ihrer Aufgabenstellung eigenständige Organisationseinheiten. Daher ist zu erwarten, dass weiterhin für Teilaufgaben von GRC eigenständige Organisationseinheiten erhalten bleiben, was geeignete Vorgehensweisen, Methoden und Werkzeuge zur Abstimmung erforderlich macht.

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

Automatisierung

Die IT kann als Gegenstand und Unterstützer von GRC angesehen werden [KD08, 9-10; TF08, 401]. Aus Sicht der IT als Unterstützer von GRC ist die Forderung der Automatisierung der Compliance-Sicherung und Risikosteuerung relevant. Automatisierung soll den manuellen Aufwand bei der Durchführung von Kontrollen und menschliche Fehler reduzieren (bspw. [Sa08a, 39]). Zur Analyse des Einflusses der Automatisierung auf die

GRC-Kosten kann die Transaktionskostentheorie angewendet werden [Pi82, 271-273]. Hierbei sind die Gesamtkosten im Sinne von Produktions- und Transaktionskosten relevant [Jo01, 18-22]. Als Produktionskosten sind im Kontext von GRC im Wesentlichen die Kosten für die Ausführung der Risiko- und Compliance-Kontrollen zu nennen. Die Automatisierung kann zum einen zur Senkung dieser Produktionskosten beitragen, da die Kosten einer automatisierten Ausführung geringer als bei einer manuellen Ausführung sind. Als Transaktionskosten sind im Kontext von GRC insbesondere die Kosten für die Beschaffung von Informationen entscheidend. Durch geeignete IT können den beteiligten Mitarbeitern relevante Informationen bedarfsgerecht zur Verfügung gestellt werden, wobei ein signifikanter Effekt auf Abstimmungs- und Informationssuchkosten zu erwarten ist. Dieser Aspekt ist auch für die Ausführung der GRC-Management-Aktivitäten relevant. Die IT 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 komplementär unterstützt wird [TKG04].

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

Im Kontext von GRC existiert ein Prinzipal-Agenten-Problem, da bspw. das Management das konforme Verhalten der Mitarbeiter sicherstellen muss. Hierdurch werden die Prinzipal-Agenten-Theorie und die Organisational Control Theorie relevant. Automatisierungs-Methoden 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. „Compliance by detection“ ist dem ergebnisorientierten Kontrollansatz zuzuordnen und stellt Fehlverhalten durch Kontrollen nachträglich fest [Sa08a, 43]. Es wird deutlich, dass die Automatisierung lediglich einige der von Lange [La08, 711] angeführten Kontrolltypen abdeckt. So können informelle Kontrollen, welche durch Werte und Normen wirken, nicht automatisiert und bestenfalls durch IT unterstützt werden. Für Anreizsysteme erscheint jedoch eine Automatisierung der Aufdeckung von Fehlverhalten geradezu notwendig [Sa08a, 44], da für die Wirksamkeit eine hohe Aufdeckungswahrscheinlichkeit sowie eine zeitnahe Aufdeckung notwendig sind (vgl. auch General Deterrence Theory [SW98]).

Guideline 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.

Flexible Geschäftsprozesse und IT-Systeme

In der Literatur wird die flexible Anpassung der Geschäftsprozesse und IT-Systeme als Herausforderung für GRC darstellt. Einerseits müssen Auswirkungen von Compliance-Änderungen auf die Organisation bzw. organisatorische Anpassungen auf die Compliance betrachtet werden [Mü07, 109]. Andererseits ist eine kontinuierliche Überwachung

der Risiken notwendig, da die Risikovermeidung zum Entwurfszeitpunkt der Geschäftsprozesse nur noch begrenzt möglich ist [Sa08b, 1138]. Außerdem wird Flexibilisierung im Kontext von serviceorientierte Architekturen behandelt [Lo08]. Grundei [Gr06b] diskutiert darüber hinaus die Beziehung zwischen vertrauens- und kontrollbasierten Ansätzen der Organisationsgestaltung, wobei vertrauensbasierte Organisationskonzepte als ein Instrument der Flexibilitätssteigerung angesehen werden. Kontrollbasierte Ansätze basieren auf agenturtheoretischen Überlegungen und sollen sichergestellten, dass die Mitarbeiter konform zu den relevanten Normen handeln. Da die Prinzipal-Agenten-Theorie grundsätzlich opportunistisches Verhalten unterstellt, werden zur Erreichung von konformen Verhalten Kontrollmechanismen in Form von Überwachung und Anreizsystemen vorgeschlagen. Vertrauensbasierte Ansätze gehen auf die Stewardship-Theorie zurück, welche grundsätzlich unterstellt, dass die Akteure im Interesse der Organisation handeln. Kontrollmechanismen werden hierdurch überflüssig. Gerade durch Konzepte, die auf einer solchen Verhaltensannahme aufbauen (bspw. Dezentralisierung, Empowerment), kann jedoch eine Flexibilitätssteigerung erreicht werden. Flexibilität wird allgemein auf Grund von Internationalisierung, kurzen Produktlebenszyklen und kleinen Losgrößen bereits seit Jahren thematisiert. Zentral für die Flexibilität ist die Möglichkeit der schnellen Reaktion auf geänderte geschäftliche Anforderungen [NM09]. Der Konflikt zwischen GRC und Flexibilität lässt sich in den allgemeinen Konflikt zwischen GRC und den Geschäftszielen eingliedern [BGJ09, 7; Gr06b, 43]. Es ist zu vermuten, dass auch andere Geschäftsinitiativen vor dem Hintergrund neuerer technischer Entwicklungen, wie Cloud-Computing oder dem Einsatz mobiler Endgeräte, in Konflikt zu GRC stehen können. Zur Lösung des Zielkonflikts sind unterschiedliche Vorschläge gemacht worden. Sowohl Böhm et al. [BGJ09] für die IT-Abteilung als auch Grundei [Gr06b] für die Organisationsgestaltung schlagen ein situationsspezifisches Ausbalancieren des Zielkonflikts vor, wobei die spezifischen strategischen Aspekte ebenso wie die GRC-Situation zu analysieren sind.

Guideline 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.

Faktoren des menschlichen Verhaltens

In der Literatur werden als menschliche Faktoren die Berücksichtigung des Verhaltens der beteiligten Mitarbeiter (bspw. [Bo09, 160; HR09, 118; JW10, 550]), die Berücksichtigung der GRC-bezogenen Kultur (bspw. [AIS10, 262; La08, 712; Op09, Intro 25]) sowie die Etablierung einer effizienten Unternehmenskommunikation im Sinne eines „tone at the top“ (bspw. [Me06, 334; Op09, 10; Pr07, 13-14; Wi10, 101]) gefordert. Die Determinanten für das Compliance-Verhalten, welche im Kontext der Informationssicherheit (bspw. [Bo09, 160; HR09, 118; JW10, 550]) und auf Basis der verhaltenswissenschaftlichen Theorien in der Literatur hergeleitet und untersucht wurden, beinhalten die eigene Einstellung, Erwartungen des sozialen Umfeldes (subjektive Norm), die Verhaltensabsicht und -kontrolle sowie das tatsächliche Compliance-Verhalten. Diese werden wiederum bspw. von der intrinsischen und extrinsischen Motivation sowie der Awareness für Compliance beeinflusst. Im Kontext der IT ist darüber hinaus die Akzeptanz

des Informationssystems (wesentlich beeinflusst durch wahrgenommenen Nutzen und Bedienungskomfort) relevant. Vergleicht man diese Erkenntnisse mit den Implikationen der Organisational Control Theorie wird erneut deutlich, dass GRC nicht auf die Automatisierung von präventiven und detektiven Kontrollen reduziert werden kann. Vielmehr sind solche prozessorientierte Kontrollen einerseits durch ergebnisorientierte Kontrollen auf der Basis von Anreizsystemen zu ergänzen. Andererseits sollten jedoch auch soziale/kulturelle Kontrollen im Sinne der Organisational Control Theorie nicht vernachlässigt werden. Die Frage die sich stellt ist, welche Verhaltensdeterminanten durch welche Kontrollen beeinflusst werden können. Lange [La08] vermutet außerdem, dass die Kombination der Kontrollen nicht in beliebiger Weise erfolgen kann, sondern das konfliktäre Konstellationen entstehen können. Des Weiteren ist zu vermuten, dass der Kontrollansatz nicht unabhängig von der jeweiligen Situation konzipiert werden kann.

Guideline 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.

6 Fazit

In diesem Beitrag wurden an Hand eines Literaturreviews von 191 relevanten Arbeiten Anforderungen an einen strategischen GRC-Management-Ansatz hergeleitet, kategorisiert und theoretisch eingeordnet. Die Erkenntnisse wurden in Form von 11 Guidelines verdichtet. Die Vorgehensweise ist insbesondere mit den bekannten Problemen qualitativer Forschung konfrontiert. Die Interkoderreliabilität sollte in zukünftigen Forschungsvorhaben adressiert werden. Weiterer Forschungsbedarf besteht außerdem hinsichtlich der Validität im Sinne der Glaubwürdigkeit. Weitere eigene Forschungsanstrengungen richten sich aktuell auf die Entwicklung einer Forschungsagenda. Hierbei soll der Forschungsbedarf in eine sachlogische Bearbeitungsfolge gebracht und priorisiert werden. Zur Priorisierung und Begründung des Forschungsbedarfs ist ebenso wie für die Steigerung der Validität der Anforderungen eine Delphi-Befragung unter GRC-Experten geplant. Eine Liste der dem Literatur-Review zu Grunde liegenden relevanten Publikationen kann, ebenso wie die Ergebnisse des Kodierungsprozesses, bei Bedarf von den Autoren angefordert werden.

Literaturverzeichnis

[AIS10] Abdullah, S.N.; Indulska, M.; Sadiq, S.: Emerging Challenges in Information Systems Research for Regulatory Compliance Management. In (Hutchinson et al. Hrsg.): Proc. CAISE, Hammamet, 2010, S. 251-265.

[Aj85] Ajzen, I.: From Intensions to Actions: A Theory of Planned Behavior. In (Kuhl, J.; Beckmann, J. Hrsg.): Action Control. Springer, Berlin et al., 1985, S. 11-39.

[Al01] Albach, H.: Shareholder Value und Unternehmenswert - Theoretische Anmerkungen zu einem aktuellen Thema. In: Zeitschrift für Betriebswirtschaft 71 (2001) 6, S. 643-674.

[Ba91] Barney, J.: Firm Resources and Sustained Competitive Advantage. In: Journal of Management 17 (1991) 1, S. 99-120.

[Bh09] Bhimani, A.: Risk Management, Corporate Governance and Management Accounting. Emerging Interdependencies. In: Management Accounting Research 20 (2009) 1, S. 2-5.

[BGJ09] Böhm, M.; Goeken, M.; Johannsen, W.: Compliance und Aligment: Vorgabenkonformität und Strategieabgleich als Erfolgsfaktoren für eine wettbewerbsfähige IT. In: HMD - Praxis der Wirtschaftsinformatik 46 (2009) 269, S. 7-17.
[BMM06] Bohnsack, R.; Marotzki, W.; Meuser, M.: Hauptbegriffe qualitativer Sozialforschung. 2. Aufl., Budirch, Opladen, 2006.
[Bö08] Böhm, M.: IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT. In: HMD - Praxis der Wirtschaftsinformatik 45 (2008) 263, S. 15-29.
[Bo09] Boss, S.R. et al..: If someone is whatching, I' ll do what I' m asked: mandatories, control, and information security. In: EJIS 18 (2009) 2, S. 151-164.
[Da86] Davis, F.D.: A technology acceptance model for empirically testing new end-user information systems: theory and results. Sloan School of Management, MIT, 1986.
[DP83] DiMaggio, P.J.; Powell, W.W.: The Iron Cage Revisited - Institutional Isomorphism and Collective Rationality in Organizational Fields. In: American Sociological Review 48 (1983) 2, S. 147-160.
[KSP08] El Kharbili, M.; Stein, S.; Pulvermüller, E.: Policy-Based Semantic Compliance Checking for Business Process Management. In (Loos, P. et al.): Proc. MobIS, Saarbrücken, 2008, S. 178-192.
[FB05] Faisst, U.; Buhl, H.-U.: Integrated Enterprise Balancing mit integrierten Ertrags- und Risikodatenbanken. In: Wirtschaftsinformatik 47 (2005) 6, S. 403-412.
[Fa49] Fayol, H.: General and Industrial Management. Sir Isaac Pitman & Sons, London, 1949.
[Fe06] Fettke, P.: State-of-the-Art des State-of-the-Art – Eine Untersuchung der Forschungsmethode "Review" innerhalb der Wirtschaftsinformatik. In: Wirtschaftsinformatik 46 (2006) 4, S. 257-266.
[FA75] Fishbein, M.; Ajzen, I.: Belief, Attitude, Intention and Behavior - An Introduction to Theory and Research. Addison-Wesley, Massachusetts, 1975.
[FWW10] Fischer, C.; Winter, R.; Wortmann, F.: Gestaltungstheorie. In: Wirtschaftsinformatik 52 (2010) 6, S. 382-386.
[Fr84] Freeman, R.E.: Strategic Management. A Stakeholder Approach. Pitman, Boston, 1984.
[Ge09] Gericke, A.; Fill, H.-G.; Karagiannis, D.; Winter, R.: Situational Method Engineering for Governance, Risk and Compliance Information Systems. In: Proc. DESRIST, 2009.
[Gr06a] Gregor, S.: The Nature of Theory in Information Systems. In: MISQ 30 (2006) 3, S. 611-642.
[Gr06b] Grundei, J.: Examining the Relationship Between Trust and Control in Organizational Design: (How) Can Divergent Requirements be Reconciled? In (Burton, R.M. et al. Hrsg.): Organization Design. Springer, New York, 2006, S. 43-65.
[HR09] Herath, T.; Rao, R.: Protection motivation and deterence: a framework for security policy compliance in organizations. In: EJIS 18 (2009) 2, S. 106-125.
[HFL11] Houy, C.; Fettke, P.; Loos, P.: Stilisierte Fakten in der gestaltungsorientierten Wirtschaftsinformatik. In: Proc. WI 2011, Zürich, S. 1157-1166,
[JM76] Jensen, M.C.; Meckling, W.H.: Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. In: Journal of Financial Economics 3 (1976) 4, S. 305-360.
[JW10] Johnston, A.C.; Warkentin, M.: Fear Appeals and Information Security Behaviors: An Empirical Study. In: MISQ 34 (2010) 3, S. 548-566.
[Jo01] Jost, P.J. : Der Transaktionskostenansatz in der Betriebswirtschaftslehre. Schaeffer-Poeschel, Stuttgart, 2001.
[Kl09] Klotz, M.: IT-Compliance. Ein Überblick. Dpunkt, Heidelberg, 2009.
[KD08] Klotz, M.; Dorn, D.W.: IT-Compliance – Begriff, Umfang und relavante Regelwerke. In: HMD – Praxis der Wirtschaftsinformatik (2008) 263, S. 5-14.
[Kr09] Kranawetter, M.: Nutzenpotentiale regulatorischer Anforderungen zur Geschäftsoptimierung.. 2009. http://download.microsoft.com/download/D/5/8/D58EEC38-FBAC-42BC-9C3C-C88C042103DE/IT_Infrastruktur_Compliance_Reifegradmodell_Microsoft_Kranawetter.pdf., Abruf am 2009-07-31.
[KM09] Krell, K.; Matook, S.: Competitve advantage from mandatory investments: An empirical study of Australian firms. In: Journal of Strat. IS18 (2009) 1, S. 31-45.
[La08] Lange, D.: A Multidimensional Conceptualization of Organizational Corruption Control. In: Academy of Management Review 33 (2008) 3, S. 710-729.
[Lo08] Loosli, G.: Compliance-Prüfung bei der Anwendung dynamischer Bindung in service-orientierten Architekturen. In (Loos, P. et al.): Proc. MobIS, Saarbrücken, 2008, S. 7-21.
[MB10] MacLean, T.; Behnam, M.: The Dangers of Decoupling: The Relationship between Compliance Programs, Legitimacy Perceptions, and Institutionalized Misconduct. In: Academy of Management Journal 53 (2010) 6, S. 1499-1520.
[MKG04] Melville, N., Kraemer, K.; Gurbaxani, V.: Review: Information Technology and Organizational Performance: An Integrative Model of IT Business Value. In: MISQ 28 (2004) 2, S. 283-322.

[Me06] Menzies, C.: Sarbanes-Oxley und Corporate Compliance – Nachhaltigkeit, Optimierung, Integration. Schaeffer-Poeschel, Stuttgart, 2006.
[Mo10] Mossanen, K.: Compliance im IT-Outsourcing. Ermittlung diskriminierender Einflussfaktoren und Entwicklung von Gestaltungsempfehlungen. Kovac, Hamburg, 2010.
[Mü07] Müller, G.: Für Sie gelesen. In: Wirtschaftsinformatik 49 (2007) Sonderheft, S. 107-109.
[NM09] Nissen, V.; Mladin, A.: Messung und Management von IT-Agilität. In: HMD – Praxis der Wirschaftsinformatik (2009) 269, S. 42-51.
[Op09] Open Compliance and Ethics Group (OCEG, Hrsg.): GRC Capability Model. Red Book 2.0. http://www.oceg.org, Abruf am 2010-06-12.
[Ou79] Ouchi, W.G.: A Conceptual Framework for the Design of Organizational Control Mechanisms. In: Management Science 25 (1979) 9, S. 833-848.
[Pe59] Penrose, E.T.: The Theory of the Growth of the Firm. Wiley, New York, 1959.
[Pi82] Picot, A.: Transaktionskostenansatz in der Organisationstheorie: Stand der Diskussion und Aussagewert. In: Betriebswirtschaft 42 (1982) 2, S. 267-284.
[Po80] Porter, M.: Competitive Strategy. Free Press, New York, 1980.
[Pr07] PWC (Hrsg.): White Paper: Governance, Risikomanagement und Compliance: Nachhaltigkeit und Integration unterstützt durch Technologie. Frankfurt am Main, 2007.
[Pu08] Pupke, D: Compliance and corporate performance: the impact of compliance coordination on corporate performance. Books on Demand, Norderstedt, 2008.
[RWS10a] Racz, N.; Weippl, E.; Seufert, A.: A frame of reference for research of integrated GRC. In (De Decker, B.; Schaumüller-Bichl, I. Hrsg.): Proc. CMS, Springer, Berlin, 2010, S. 106-117.
[RWS10b] Racz, N.; Weippl, E.; Seufert, A.: A process model for integrated IT governance, risk & compliance management. In: Proc. International Baltic Conference, 2010.
[RWS10c] Racz, N.; Weippl, E.; Seufert, A.: Questioning the need for separate IT risk management frameworks. In: Proc. Informatik, 2010.
[Ra10] Racz, N. et al..: Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from a Survey among Large Enterprises. In: Proc. ACIS, Brisbane, 2010.
[Ra99] Rappaport, A.: Shareholder Value. Wertsteigerung als Maßstab für die Unternehmensführung. 2.Auflage, Schaeffer-Poeschel Stuttgart 1999.
[RW08] Rieke, T.; Winkelmann, A.: Modellierung und Management von Risiken – Ein prozess-orientierter Risikomanagement-Ansatz zur Identifikation und Behandlung von Risiken in Geschäftsprozessen. In: Wirtschaftsinformatik 50 (2008) 5, S. 346-356.
[Ro83] Rogers, R.W.: 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, 1983, S. 153-176.
[Sa08a] Sackmann, S.: Automatisierung von Compliance. In: HMD – Praxis der Wirtschaftsinformatik (2008) 263, S. 39-46.
[Sa08b] Sackmann, S.: Assessing the Effects of IT Changes on IT Risk – A Business Process-Oriented View. In: Proc. MKWI, Springer, Berlin, 2008.
[SW98] Straub, D.W.; Welke, R.J.: Coping with Systems Risk: Security Planning Models for. Management Decision-Making. In: MISQ 22 (1998) 4, S. 441-469.
[TKG04] Tallon, P.; Kreamer, K.L.; Gurbaxani, V.: Executives' perception of the business value of information technology. In: Journal of MIS 16(2004) 4, S. 145-173.
[TF08] Teubner, A.; Feller, T.: Informationstechnologie, Governance und Compliance. In: Wirtschaftsinformatik 50 (2008) 5, S. 400-407.
[BSN09] vom Brocke, J. et al..: Reconstructing the Giant: On the Importance of rigour in documenting the literature search process. In: Proc. ECIS, Verona, 2009.
[WWS92] Walls, J.G.; Widmeyer, G.R.; El Sawy, O.A.: Building an information systems design theory for vigilant EIS. In: Information Systems Research 3 (1992) 1, S. 36-59.
[WAM07] Walser, M.; Amberg, M.; Mossanen, K.: Wirtschaftlichkeit von IT-Risk-Management-Lösungen zur Sicherstellung der Erfüllung von Compliance-Anforderungen. Novell, Inc., 2007. http://www.wi3.uni-erlangen.de/fileadmin/Dateien/Forschung/Studie_Compliance_Print_Version.pdf, Abruf am 2009-07-31.
[We84] Wernerfelt, B.: A Resource-based View of the Firm. In: Strat. Mgnt Journal 5 (1984) 2, S. 171-180.
[Wi85] Williamson, O.E.: The Economic of Institutions of Capitalism. The Free Press, New York, 1985.
[Wi10] Withus, K.-H.: Sicherstellung der Complinace durch wirksame Managementsysteme. In: Zeitschrift für Interne Revision 7 (2010) 3, S. 99-108.
[Wo05] Wolf, J.: Organisation, Management, Unternehmensführung: Theorien, Praxisbeispiele und Kritik. 2. Aufl., Gabler, Wiesbaden, 2005.