Entwicklung eines fachkonzeptionellen Referenzmodells für ein strategisches GRC-Management

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

Abstract: Obwohl zunehmend integrierte Ansätze für Corporate Governance, Risiko- und Compliance-Management (GRC-Management) gefordert werden, ist bislang nur unzureichend geklärt, welche Informationsstruktur ein integriertes und strategisch ausgerichtetes GRC-Management haben sollte. In diesem Beitrag wird daher ein fachkonzeptionelles Referenzmodell für ein strategisches GRC-Management entwickelt und anhand von publizierten Fallbeispielen evaluiert.

1 Motivation

Governance, Risiko- und Compliance-Management werden auf Grund ihrer vielfältigen Überschneidungen und Abhängigkeiten [RWS10a; TF08] zunehmend unter dem Akronym GRC als ein zusammenhängendes Thema betrachtet. Eine kürzlich durchgeführte Studie der Open Compliance & Ethics Group [Op12] zeigt, dass die Integration von GRC in der Praxis weiter voranschreitet und Unternehmen hierin eine Möglichkeit für Performanceverbesserungen sehen. Obwohl erste integrierte GRC-Ansätze vorliegen [Me06; MS09; RWS10b] bleibt die Eingrenzung des Themengebiets insgesamt recht vage. Einerseits existiert eine Vielzahl von Literatur aus den Teilbereichen von GRC, die sich überwiegend mit Detailfragen auseinandersetzt. Andererseits existieren bereits einige Arbeiten, die versuchen, GRC als integrierten Ansatz zu strukturieren und terminologisch einzugrenzen [RWS10a]. Ganzheitlich betrachtet kann das GRC-Management nicht auf den Integrationsaspekt beschränkt werden, sondern hat vielfältige Anforderungen zu erfüllen [MN12]. Dem hier in Auszügen 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. Hierbei steht nicht die operative Normerfüllung und Risikosteuerung im Fokus, sondern die umfassende Planung und Steuerung des GRC-Status, die Integration der Teilaspekte sowie die strategische Ausrichtung und kontinuierliche Verbesserung. Sowohl Racz et al. [RWS10b] als auch das „GRC Capability Model“ von Mitchell und Switzer [MS09] stellen den Prozess des GRC-Managements ins Zentrum ihrer Betrachtungen. Das “GRC Capability Model” der OCEG stellt zwar detailliert mögliche GRC-Aktivitäten dar. Kritisch zu sehen ist jedoch, dass im Modell Management-Aufgaben und operative Aktivitäten nicht unterschieden und die Integration von GRC in den einzelnen Aktivitäten nicht explizit herausgestellt wird. Es bleibt ebenso unklar, wie der Ansatz in bestehende Rahmenwerke integriert werden kann. Letztlich werden Governance-Aspekte nur einge-

schränkt einbezogen [RWS10b, 2]. Racz et al. [RWS10b] entwickeln ein Prozessmodell für „IT GRC“. Hierbei wird zwar deutlich, dass in den einzelnen GRC-Teildisziplinen eine ähnliche methodische Vorgehensweise angewendet werden kann, konkrete Überschneidungen und Interdependenzen werden jedoch nur am Rande thematisiert.

Zur Entwicklung eines GRC-Management-Ansatzes ist eine Analyse der strukturellen Zusammenhänge der relevanten Informationen notwendig. Ziel dieses Beitrags ist daher die Entwicklung eines fachkonzeptionellen Referenzmodells für das strategische GRC-Management. Hiermit sollen insbesondere zwei Forschungsfragen beantwortet werden. (1) Welches sind die konstituierenden Informationsobjekte eines strategischen GRC-Managements? (2) Welche Beziehung weisen die Informationsobjekte auf? Informationsobjekte sind hierbei als IT-technisch motivierte Abbildungen von Informationen zu verstehen. Das 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 GRC-Informationssystemen als auch hinsichtlich der GRC-Organisationsgestaltung nützlich sein. Es kann weiterhin als Bezugsrahmen für die Entwicklung unternehmensspezifischer Modelle dienen. Der Beitrag ist wie folgt strukturiert. In Abschnitt 2 wird die Forschungsmethodik erläutert. Anschließend wird das Modell entwickelt, dargestellt und evaluiert. Der Beitrag schließt mit einem Fazit.

2 Grundlegende Begriffe und Forschungsmethode

Referenzmodelle sind allgemeingültige Empfehlungen, die in einer konkreten Modellierungssituation genutzt werden können [Br03, 31]. Im Unterschied zu Ontologien, die ebenfalls geeignet sind, die Semantik von Konzepten und somit die Struktur von GRC zu explizieren [MG10], besitzen Referenzmodelle einen Empfehlungscharakter (zur Abgrenzung der Begriffe siehe [Ze99, 11-13]). Für die Referenzmodellierung existieren verschiedene Methodensysteme. Die Architektur integrierter Informationssysteme (ARIS) [Sc02] unterscheidet zwischen der Organisations-, Funktions-, Daten- und Steuerungssicht als Zusammenführung der vorgenannten Sichten. Jede dieser Sichten wird in den Ebenen Fachkonzept, DV-Konzept und Implementierung betrachtet. ARIS ordnet jeder Sichten-Ebenen-Kombination Darstellungstechniken zu. 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 [Br03, 112]. Wir argumentieren, dass ein Referenzmodell für das GRC-Management nur auf dem Verständnis der Struktur im Sinne der konstituierenden Informationsobjekte und Beziehungen aufbauen kann. Daher fokussieren wir die Datensicht auf fachkonzeptioneller Ebene. Die Unified Modeling Language (UML) [OMG10] beinhaltet verschiedene objektorientierte Diagrammarten, die sowohl die Struktur, als auch das Verhalten und die Interaktion darstellen. Klassendiagramme sind Kernbestandteil der UML, wobei die Struktur fokussiert und eine fachkonzeptionelle Datenmodellierung unterstützt wird.

Die Referenzmodellierung ist der gestaltungsorientierten Forschung zuzuordnen [He04]. und lässt sich hinsichtlich des Forschungsprozesses wie folgt gliedern. 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) [Be02, 36]. Die Festlegung der Modellierungstechnik sollte insbesondere zwei Aspekte beinhalten, die als „way of modeling“ und „way of working“ bezeichnet werden [VHW91]. Ersteres betrifft die Auswahl der Modellierungssprache. Basierend auf dem dargestellten Projektziel werden hierfür UML-Klassendiagramme verwendet, da diese eine fachkonzeptionelle Datenmodellierung unterstützen und mehrheitlich bei den Modellen in der GRC-Literatur eingesetzt wurden. Eine Modellierung in Entity-Relationsship-Modellen [Ch76] wäre ebenso angemessen. Der „way of working“ spricht die Vorgehensweise der Modellerstellung an. Grundsätzlich sind bei der Konstruktion von Referenzmodellen induktive und deduktive Ansätze möglich. Hinsichtlich der induktiven Vorgehensweise ist darauf hinzuweisen, dass Referenzmodelle allgemeingültig in dem Sinne sein sollen, dass sie für eine Klasse unternehmensspezifischer Modelle gültig sein sollen [Br03, 31]. Um der besonderen Bedeutung von Referenzmodellen Rechnung zu tragen, werden im vorliegenden Forschungsvorhaben induktive und deduktive Elemente bei der Entwicklung des Referenzmodells kombiniert. Daher findet in einem ersten Schritt eine Auswertung von existierenden Modellen aus der GRC-Literatur statt, welche auf empirischen Fällen und konzeptionellen Überlegungen basieren. In einem zweiten Schritt findet dann deduktiv ein Abgleich der gefundenen Modellelemente mit den strategischen GRC-Anforderungen aus [MN12] statt.

3 Entwicklung des Referenzmodell

3.1 Auswertung der existierenden Modelle der GRC-Literatur

Zur Identifikation von relevanten Modellen in der Literatur wurde die Literatursuche in [MN12] verwendet. Diese basiert, angelehnt an vom Brocke et al. [BSN09] auf qualitativ-hochwertigen Publikationen aus Journalen und Konferenz-Proceedings, wobei zusätzlich auch GRC-spezifische Publikationsorgane und praxisnahe Publikationen berücksichtigt wurden. In den dort gefundenen 191 für das strategische GRC-Management relevanten Veröffentlichungen wurden 21 relevante Modelle identifiziert (Tab. 1).

Titel	Gegenstand	Quelle
(1) Interrelationships of COBIT Components	IT-Governance	[Th07, 8]
(2) Relationships between Process Modeling and Control Modeling Concepts	Compliance	[SGN07, 5]
(3) Selected correspondences between Business process and Risk	Risikomanagement	[SLP08, 24]
(4) Conceptual model of the compliance management problem	Compliance	[Si09, 5]
(5) A basic high level model for regulatory compliance	Compliance	[KSP08, 180]
(6) Policy Ontology	Compliance	[KSP08, 187]
(7) Rule Ontology	Compliance	[KSP08, 188]
(8) A MOF/UML metamodel of a business protocol model	Compliance	[GV06, 562]
(9) A MOF/UML metamodel of an obligation	Compliance	[GV06, 563]
(10) A MOF/UML metamodel of a conditional commitment	Compliance	[GV06, 563]
(11) Rule ontology (constraints)	Compliance	[WHH11, 794]
(12) The upper domain model of the Internal Controls Compliance	Compliance	[NS07, 62]
(13) Relationship between an Application Control and a Business Process	Compliance	[NS07, 62]
(14) A Semi-formalization of the control implementation	Compliance	[NS07, 63]
(15) IT Risk Reference Model	Risikomanagement	[Sa08a, 4]

(16) Meta-Referenzmodell zum Compliance-Management	Compliance	[TF09, 555]
(17) A Classification Model for Automating Compliance	Compliance	[Sa08b, 41]
(18) Beispielhafter Auszug einer (initialen) Corporate Rule Base	GRC	[Me06, 364]
(19) ISO 27001 Metamodell	Risikomanage-ment/Compliance	[MG10]
(20) The oracle corporate analysis flow	Compliance	[Po08, 42]
(21) The regulatory mandate and compliance framework control domain relationship	Compliance	[Po08, 43]

Tabelle 1: Übersicht der konzeptionellen Modelle in der GRC-Literatur

Die Auswertung der Modellelemente erfolgte folgendermaßen. 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 Modelle Rechnung getragen. Modellelemente, die eine Teilmenge eines anderen darstellen und für die konzeptionelle Modellierung des strategischen GRC-Managements nicht zwingend notwendig sind, wurden diesem 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 bzw. 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. 2 zeigt die Zuordnung der Informationsobjekte nach sprachlicher Vereinheitlichung zu den synonymen und untergeordneten Begriffen aus den ausgewerteten Modellen (Modellnummern gemäß Tab. 1 in Klammern). Ebenso ist die Anzahl der Modelle, die zugeordnete Elemente zu einem Informationsobjekt aufweisen, dargestellt (Spalte „Anz.“).

Info.objekt	**Synonyme Begriffe**	**Untergeordnete Begriffe**	**Anz.**
Kontrolle	Control Practices (1), Internal Control(s) (2, 5), rule (4), Procedures (5), business rule (11), Control (12, 19), Regel (18), Business Rule (20)	RiskTreatmentMesure (3), operational business rule (11), declarative business rule (11), CompanyLevelControl (12), ITControl (12), ApplicationControl (12)	14
Rolle	Responsibility and Accountability Chart (1), PersonProfile (3), OrganisationalUnit (3), FunctionalEntity (3), Actor (4), Role (4, 6, 8, 9, 10, 19), Business Function (6), Agent (11, 13), authority (13), Organisationsmodell (16), Verantwortlich (18)	N/A	12
Geschäfts-prozess	Business Process (1, 5, 12, 13, 15, 20), Process (2), ProcessModel (6), Geschäftsprozess (18)	IT Processes (1), Key Activities (1), Task (2), EnterpriseActivity (3), ProcessStructure (3), Activity (4, 6, 13), ProcessFragment (6), ProcessConstruct (6), operation (11)	12
Kontrollziel	Control Objective(s) (1, 2, 12, 17, 19), Requirement (4), RuleGoal (7), Measures & Directives (16), Anforderung / Vereinbarung (18), Requirement (19), Directive (20)	ApplicationControlStrategy (13, 14)	11
Richtlinie	Policy(ies) (4, 6, 11, 17), Richtlinie / Arbeitsanweisung (18), Business Policy (20)	Meta-Policy (6)	7

Risiko	Risk (2, 3, 4, 11, 12)	Event (3), Vulnerabilities (15), Threats (15, 19)	7
GRC-Vorgabe	Source (4), Regulation (5, 6, 20), authority (11), Laws and regulations (17), Gesetzlich (18)	N/A	7
Ressource	asset (3, 19), Resource (3, 6), EnterpriseObject (3), Business subject (Sub-subject) (4), Subject (6)	Produktgruppe (18)	5
Ziel	objective (3, 20), Goal (6, 11, 20), Desired Result (20)	Business Goals (1), IT Goals (1)	5
Anwendungs-bereich	Domain (3), Jurisdiction (6), Scope (6, 7), Scope (Global, Before, After, Between, AfterUntil) (14)	Control Domain (21)	5
Dokumenta-tion	BusinessProtocol (8), BusinessDocument (13), Dokumentenmodell (16)	N/A	5
Assessment	Audit (17), Assessment (20)	Control Outcome Tests (1), Control Design Tests (1), RiskAssessment (12)	4
IT Kompo-nente	IT Applications / IT Infrastructure (15), IT-Architekturmodell (16), Datenbankmodell (16), IT-System (17), Application (21)	Packaged Service (21)	4
Kennzahl	Performance Indicator(s) (1, 3), Kennzahl (16)	RiskIndicator (3)	3
Stakeholder	Stakeholder (3, 18)	Indirekte Stakeholder (18)	2
Strategie	Strategy (6), Strategiemodell (16)	N/A	2
Reifegrad	Maturity Models (1), Reifegradmodell (16)	N/A	2
Rahmenwerk	Rahmenwerk (18), Compliance Frameworks (21)	N/A	2
Ausführung	Performance (9, 10)	N/A	2
Monitor	Monitor(s) (4, 17)	N/A	2
Verletzung	Violation (4)	Security Breach (19)	2
Implemen-tierungslogik	RuleLogic (7)	N/A	1

Tabelle 2: Geordnete Übersicht zu den Modellelementen

Zur Analyse der Beziehungen zwischen den Informationsobjekten sind die existierenden Modelle nur eingeschränkt geeignet, da bis auf Menzies [Me06] keines der Modelle explizit eine Integration von GRC betrachtet. 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 bzw. die Abstraktionsebene des jeweiligen Modells hat 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. Bspw. 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. Zum einen 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. Die Ergebnisse der hier angesprochenen Analyse sind auf Grund der gebotenen Kürze nicht in diesem Beitrag dargestellt. Im Rahmen der Darstellung des Referenzmodells (Abschnitt 4) wird die Analyse jedoch in der Weise aufgegriffen, dass die identifizierten Beziehungen in den existierenden Modellen an entsprechenden Stellen zur Begründung der Beziehungen im entwickelten Modell referenziert sind.

3.2 Abgleich der Modellobjekte mit den strategischen GRC-Anforderungen

Die Herleitung der Anforderungen an ein strategisches GRC-Management wurde in [MN12] dargestellt. Anforderungen sind Bedingungen oder Fähigkeiten, die benötigt werden, um ein Problem zu lösen bzw. Ziel zu erreichen (vgl. IEEE Standardglossar). Zur Herleitung der Anforderungen wurden Publikationen, die sowohl Ergebnisse aus empirischer Forschung als auch konzeptionelle Überlegungen beinhalten und somit derzeit als geeignetste Quelle erscheinen, mit Hilfe der qualitativen Inhaltsanalyse [BMM06] ausgewertet. Ergebnis dieser Analyse sind Anforderungskategorien, welche theoriebasiert diskutiert und durch Guidelines verdichtet wurden. Nachfolgend werden relevante Aspekte der Anforderungskategorien erörtert und in Tab. 3 zusammengefasst.

Strategische Ausrichtung: Die strategische Ausrichtung fordert 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 [MN12]. Somit werden Informationsobjekte wie Strategie bzw. Ziel angesprochen. GRC, d.h. konkret die Kontrollziele, sollte demnach an den Zielen ausgerichtet werden, wodurch auch der genannte Zielkonflikt berücksichtigt wird. Governance sollte die Strategie- und Zieldefinition unterstützten und die integrierte Steuerung von „Performance“ und „Conformance“ [In08] mittels Assessments und Kennzahlen ermöglichen. 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. Die Stakeholder-Orientierung fordert eine Ausrichtung der Strategie und Ziele und somit mittelbar auch der Kontrollziele an den Stakeholderinteressen.

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 gefordert [MN12]. Für das mit dem Referenzmodell verfolgte Forschungsziel ist die Integration der GRC-Disziplinen als Teil der inhaltlichen Integration und die Integration der Kontrollen in die operativen Geschäftsprozesse relevant. Zur Beziehung von Compliance- und Risikomanagement existieren zwei Sichtweisen. Compliance wird zum einen als Teil das Risikomanagements verstanden, wobei das Non-Compliance-Risiko als

Risikokategorie betrachtet wird [In10; Wi10, 100]. Zum anderen wird Risikomanagement als Teil von Compliance verstanden und somit das regulatorisch geforderte Risikomanagement betrachtet. Risikomanagement und die damit verbundene Etablierung eines internen Kontrollsystems ist somit eine GRC-Vorgabe, zu deren Umsetzung Kontrollmodelle, wie für die IT-Prozesse bspw. COBIT, ITIL oder ISO 27001/2, eingesetzt werden [JG06, 16]. Es können jedoch auch Kontrollziele für risikosteuernde Maßnahmen aus Risikoanalysen im Hinblick auf Ziele definiert werden. Kontrollziele lassen sich somit einerseits aus Risiken und andererseits aus GRC-Vorgaben ableiten. Zwischen Corporate Governance und Compliance existiert eine Überschneidung hinsichtlich der Einhaltung von regulatorischen Vorgaben [TF08]. Der Begriff Governance wird darüber hinaus mit der wertorientierten Unternehmensführung in Verbindung gebracht [TF08, 400], was auch vom IT-Governance-Begriff gestützt wird [TH07, 5]. Nach Racz et al. [RWS10b, 11-12] unterstützen sich Corporate Governance sowie Risiko- und Compliance-Management gegenseitig, indem durch das Risiko- und Compliance-Management wichtige Informationen für die Governance geliefert und die Governance die Steuerung des Risiko- und Compliance-Managements übernimmt.

Geschäftsprozessorientierung: Ein geschäftsprozessorientierter Ansatz wird in der Literatur auf Grund der Bedeutung der Geschäftsprozesse für GRC sowie der Bedeutung eines geschäftsprozessorientierten Ansatzes für die Automatisierung der Compliance-Sicherung gefordert [MN12]. Hieraus ergibt sich die Forderung einer Integration von GRC- und Geschäftsprozessmanagement. Geschäftsprozesse stehen in einem direkten Zusammenhang mit Risiken [Sa08b, 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 einem geschäftsprozessorientierten Ansatz ist der Geschäftsprozess ein zentrales Element des GRC-Managements. Die Verantwortlichkeit (Ownership, Informationsobjekte Rolle) für Geschäftsprozesse kann somit die Ownership an einer Reihe weiterer Informationsobjekte determinieren.

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) [Bh09; Kl09, 13-16]. Unter GRC zu subsumierende Management-Systeme beschäftigen sich im Wesentlichen mit der Prüfung der ihr anvertrauten Verantwortungsbereiche. Besonders betont wird dies in der Aufgabenstellung der Internen Revision, welche unabhängige Prüfungs- und Beratungsleistungen erbringt [De11, 5]. Mit einer ähnlichen Aufgabenstellung ist auch das Controlling konfrontiert, welches eine Managementunterstützung durch Planung, Kontrolle und entsprechende Informationsversorgung erbringt und Kennzahlensysteme eingesetzt. Neben dem Geschäftsprozessmanagement 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 relevant.

Automatisierung: Die IT ist Gegenstand und Unterstützer von GRC [TF08, 401]. Aus Sicht der IT als Unterstützer von GRC ist insbesondere die Automatisierung der Comp-

liance-Sicherung und Risikosteuerung relevant. Als Gegenstand ist die IT, bspw. im Kontext der Informationssicherheit, auch unmittelbar Gegenstand von Compliance-Vorgaben und Risiken. Relevante Informationsobjekte sind Kontrollen, Geschäftsprozesse, IT Komponenten und die Implementierungslogik. Darüber hinaus können nicht alle Kontrollen automatisiert werden, sondern sind teilweise manuell auszuführen [Sa08a].

Flexibilisierung: Die Literatur stellt flexible Geschäftsprozesse und IT-Systeme als Herausforderung für GRC dar. Auswirkungen von Compliance-Änderungen auf die Organisation bzw. organisatorische Anpassungen auf die Compliance müssen betrachtet werden [Mü07, 109]. Außerdem ist eine kontinuierliche Überwachung der Risiken notwendig [Sa08b, 1138]. Menzies [Me06, 359] identifiziert Treiber des GRC-Managements, wie neue Geschäftsprozesse, neue Produkte, M&A-Aktivitäten und IT-Systeme. Flexibilisierung kann Auswirkungen auf nahezu alle Informationsobjekte des Referenzmodells haben, insbesondere auf Strategien, Ziele, Geschäftsprozesse und andere Ressourcen, Risiken sowie Kontrollen. Von Sackmann [Sa08b] werden die Beziehungen zwischen Risiken und IT-Komponenten sowie Geschäftsprozessen betont. Die direkte Beziehung zwischen IT Komponenten und Risiken ist notwendig, da Änderungen in den IT Komponenten unmittelbar Auswirkungen auf die Risikosituation haben, diese jedoch nicht notwendigerweise auch den Ablauf des Geschäftsprozesses tangieren.

Faktoren des menschlichen Verhaltens: Die Forderung der Berücksichtigung des menschlichen Verhaltens bezieht sich auf das Mitarbeiter-Verhalten [Bo09, 160; HR09, 118], die Kultur [AIS10, 262; MS09, Intro 25] sowie die Kommunikation im Sinne des „tone at the top“ [Me06, 334; MS09, 10; Wi10, 101]. 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 bzw. Awareness-Kampagnen durchgeführt werden, welche die Mitarbeiter in ihren Rollen zu GRC-konformen Verhalten befähigen und ermutigen. Kontrollen haben somit eine direkte Beziehung zum Informationsobjekte Rolle.

Anforderungs-kategorie	**Relevante Info.objekte**	**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.
Integration	Kontrollziel, Risiko, GRC-Vorgabe, Kennzahl, Assessment, Geschäftsprozess, Kontrolle	(B4) Kontrollziele ergeben sich aus Risiken und GRC-Vorgaben.
		(B5) Kennzahlen und Assessments messen Conformance und Performance der Geschäftsprozesse.
		(B6) Kontrollen werden in den operativen Geschäftsprozessen umgesetzt (operative Integration).
Geschäfts-prozess-orientierung	Kontrolle, Geschäftsprozess, Implementierungslogik, Rolle	(B7) Kontrollen werden in Geschäftsprozessen implementiert und mit Hilfe der Implementierungslogik mit dem Geschäftsprozess automatisiert.
		(B8) Über Geschäftsprozesse wird die verantwortliche Rolle (Ownership) determiniert.
Management-Systeme	Assessment, Kennzahl, Geschäftsprozess	(B9) Geschäftsprozesse werden durch Assessments und Kennzahlen im Hinblick auf GRC gesteuert.

Automatisierung	Kontrolle, Geschäftsprozess, IT Komponente, Implementierungslogik	(B10) IT Komponenten sind direkt durch Kontrollen betroffen.
		(B11) Kontrollen werden durch eine Implementierungslogik automatisiert.
Flexibilisierung	Alle insb. Geschäftsprozess, IT Komponente, GRC-Vorgabe, Risiko	(B12) 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	(B13) Kontrollen haben eine direkte Beziehung zum Informationsobjekte Rolle.

Tabelle 3: Info.objekte und Beziehungen aus den strategischen GRC-Anforderungen

4 Darstellung des Referenzmodells

Das in diesem Abschnitt dargestellte Referenzmodell basiert auf den in den vorgegangenen Abschnitten angestellten Analysen. Die Darstellung nimmt außerdem bereits die Ergebnisse der Evaluierung in Abschnitt 5 vorweg. 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. Die Beziehungen zwischen den Informationsobjekten werden aus den vorhandenen Modellen (Nummer gemäß Tab. 1) sowie den strategischen GRC-Anforderungen (Nummer B1 bis B13 gemäß Tab. 3) hergeleitet. Aufgrund der Komplexität des Modells wurde eine weitere Untergliederung in die strategische, konzeptionelle und operative Ebene vorgenommen, welche lediglich die Lesbarkeit des Modells erhöhen soll und nicht Gegenstand der Herleitung bzw. Evaluierung ist.

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 dienen zur Unterstützung der Zielerreichung (6, 16) und beeinflussen die Entscheidungsfindung (siehe Evaluierung). Abzugrenzen von der strategischen Ebene ist die konzeptionelle Ebene, welche die Management-Aktivitäten von GRC beinhaltet. Hier sind die Kontrollziele aus den GRC-Vorgaben (4, 5, 17, 18, B4) und den Risiken (2, 4, 12, B4) zu entwickeln. Die Anforderungskategorie „strategische Ausrichtung“ legt außerdem nahe, dass die Kontrollziele mit den Zielen der strategischen Ebene abzustimmen sind (1, B1). Aus den Kontrollzielen werden die Richtlinien abgeleitet (4, 5, 17, 18, 20), welche einen eingeschränkten Anwendungsbereich haben (6). Zur Herleitung unternehmensspezifischer Richtlinien können Rahmenwerke in Form von Standards und Best Practices herangezogen werden (4, 18), welche die Erfüllung von GRC-Vorgaben unterstützen (18). Geschäftsprozesse sind an den Unternehmenszielen auszurichten (3, 20, B2, B9). Der Fokus dieses Modells legt es nahe, Assessments hinsichtlich der Risiken (12) sowie der „Conformance“ und „Performance“ (B5) auf der Ebene der Geschäftsprozesse durchzuführen (1, 12, B5, B9). Hierfür können auch Reifegradmodelle verwendet werden, welche 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, B6, B7) und Risiken (3, 12, 15, 19) verknüpft. Risiken können sich weiterhin auch unmittelbar aus den IT Komponenten ergeben (15, B12) ohne das hierbei die Geschäftsprozesse betroffen sind. Risiken beziehen sich weiterhin auf Ziele und gefährden die Zielerreichung (11). Kennzahlen messen Geschäftsprozesse (1, B5, B9) hinsichtlich der Erreichung der Ziele (1, 3, 16, B2) und unterstützen hierdurch, ebenso wie Assessments, Entscheidungen auf strategischer Ebene (siehe Evaluierung).

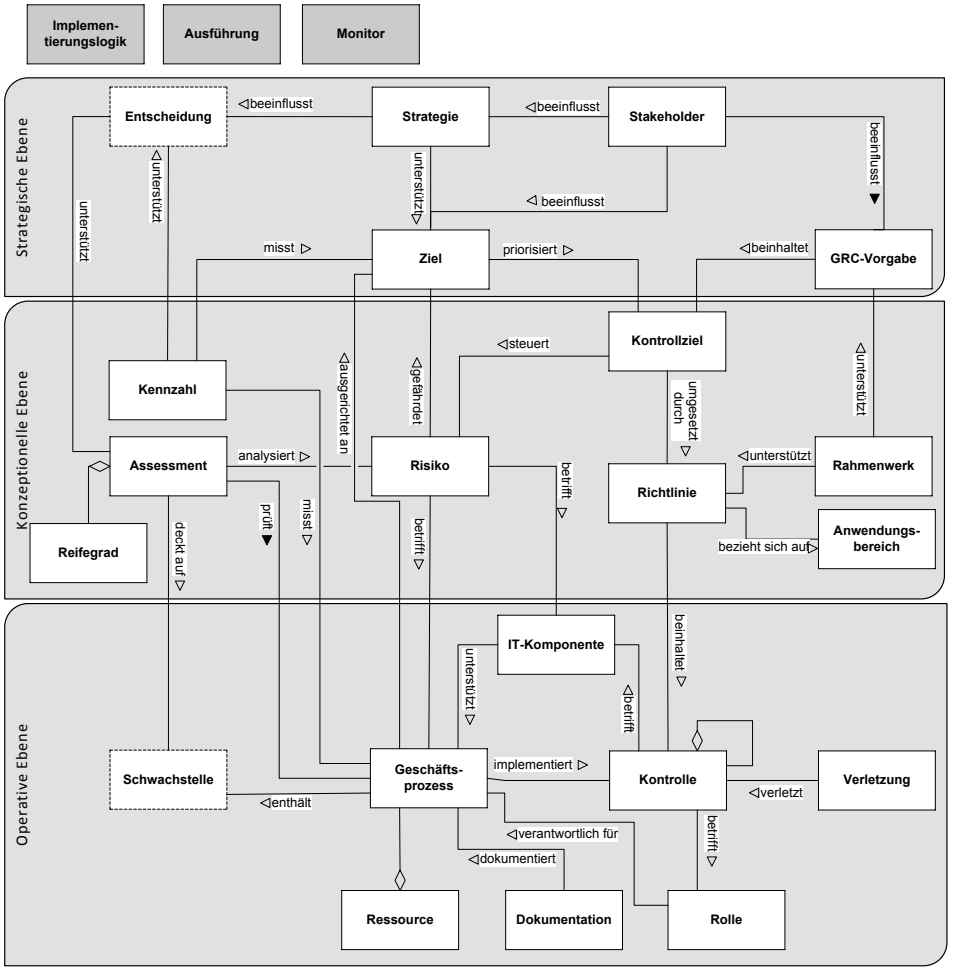

Abb. 1: Fachkonzeptionelles Referenzmodell für ein strategisches GRC-Management

Auf operativer Ebene werden Kontrollen, die in den Richtlinien formuliert sind (4, 5, 6, 11, 18, 20), im Sinne einer operativen Integration in den Geschäftsprozessen implementiert (2, 3, 5, 6, 11, 12, 13, 18, B6, B7). Zwischen den Kontrollen selbst können Abhängigkeiten bestehen (6, 11, 19). Kontrollen können weiterhin durch Verletzungen gefährdet werden (4, 19) und neben Geschäftsprozessen auch direkt die IT Komponenten be-

treffen (B10), welche die Geschäftsprozesse unterstützen (15). IT Komponenten dienen darüber hinaus zur Automatisierung der Kontrollen (B11). Geschäftsprozesse werden als Unternehmensressourcen betrachtet, wobei auch weitere Gegenstände wie Produkte, Projekte oder Informationen für GRC relevant sind (3, 6, 18). IT Komponenten und Kontrollen sind im Rahmen der Geschäftsprozesse zu dokumentieren (13). Das Modell definiert die Verantwortlichkeiten mittels der Rollen, welche an den Geschäftsprozessen beteiligt sind (1, 4, 6, 11, 13, 18, B8). Kontrollen können, wie die Analyse der verhaltensspezifischen Aspekte zeigt, auch direkt Mitarbeiter betreffen (11, B13). Letztlich sind Schwachstellen relevant, die sich auf die Geschäftsprozesse beziehen und im Rahmen der Assessments auf konzeptioneller Ebene aufzudecken sind (siehe Evaluierung).

5 Evaluierung

Die Evaluierung von Referenzmodellen kann hinsichtlich unterschiedlicher Kriterien wie bspw. den Grundsätzen ordnungsmäßiger Modellierung [Sc97] erfolgen und verschiedene Evaluierungsmethoden anwenden [FL04]. Hier soll die Nützlichkeit des Referenzmodells bei der Modellierung von Informationen eines strategischen GRC-Managements evaluiert werden. Dies beinhaltet die Adäquanz der Informationsobjekte bspw. hinsichtlich des Abstraktionsniveaus und der verwendeten Begrifflichkeiten, die Vollständigkeit der Informationsobjekte und die korrekte Modellierung der Beziehungen zwischen den Informationsobjekten. Des Weiteren soll eine weitere Detaillierung der Informationsobjekte, bspw. durch Attribute, hinsichtlich von Praxisanforderungen erfolgen. Da die GRC-Integration auf strategischer Ebene in der Forschung noch wenig betrachtet wurde [Ge09], werden Praxisbeschreibungen aus der Literatur zu den GRC-Teilbereichen zur Evaluierung herangezogen. Diese beziehen sich auf erfolgreiche Implementierungen und ermöglichen ein relativ großes Spektrum an Fällen mit ausreichender inhaltlicher Tiefe einzubeziehen. Weitere Evaluierungen bspw. hinsichtlich der korrekten Syntax und eine Anwendung des Modells in der Praxis sind wünschenswert. Der Erfolg der Anwendung ist jedoch auch von weiteren Faktoren wie dem Reifegrad des Geschäftsprozessmanagements des Unternehmens, der Verfügbarkeit geeigneter GRC-Management-Methoden und eingesetzten Informationssystemen abhängig. Die Vorgehensweise der Evaluierung ist wie folgt. Zuerst wurden Implementierungsbeispiele identifiziert. Hierfür wurde praxisnahe Literatur in der Literaturrecherche von [MN12] und durch die Suche in allgemeinen Suchmaschinen sowie in praxisnahen Publikationsorganen identifiziert. Insgesamt wurden 21 relevante Praxisbeispiele aufgenommen. Anschließend erfolgte die Auswertung der Praxisbeispiele hinsichtlich allgemeiner Beobachtungen und der angesprochenen Evaluierungsziele.

Allgemeine Beobachtungen: Grundsätzlich zeigt sich bei der Auswertung der Praxisbeispiele, dass eine einheitliche Terminologie in der Praxis fehlt. 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. Auf Grund der hohen branchenübergreifenden Bedeutung des Sarbanes-Oxley-Acts hat Finanzberichter-

stattung insgesamt eine hohe Bedeutung. Weiterhin wird die Involvierung des Top Managements für viele Aufgaben als wichtig angesehen. Explizit wird auf die Unsicherheit hinsichtlich der Management-Methoden für GRC hingewiesen [Me06, 445]. Rahmenwerke, wie COSO und COBIT, werden als zu abstrakt bewertet und lassen sich nicht immer eindeutig von den eigentlichen regulatorischen GRC-Vorgaben unterscheiden.

Adäquanz und Vollständigkeit der Informationsobjekte: Tab. 4 zeigt die Anzahl von Praxisbeispielen, welche Begriffe verwenden, die den Informationsobjekten des Referenzmodells zugeordnet werden können. Es zeigt sich eine Übereinstimmung von Begriffen und eine ähnliche Verteilung wie bei der Auswertung der existierenden Modelle in der Literatur. Es ist jedoch anzumerken, dass keines der Beispiele alle Informationsobjekte bestätigt. Die Modelle aus der GRC-Literatur sind oftmals mit dem Ziel der Automatisierung entwickelt worden, was nicht Gegenstand der Praxisbeispiele ist. Die Informationsobjekte Monitor und Implementierungslogik werden daher nicht bestätigt. Das Informationsobjekt Ausführung wurde nur in einem Fallbeispiel bestätigt und wird daher mit Geschäftsprozess zusammengefasst. Das Abstraktionsniveau des Modells erscheint angemessen, erfordert jedoch hinsichtlich der Ausprägung der Attribute zu den Informationsobjekten eine weitere Detailierung. Kontrollen sind auf unterschiedlichen Ebenen relevant und werden in Company Level, Business und IT Controls unterschieden [Me06, 435]. Außerdem wird der Fokus auf Key Controls gerichtet, wodurch eine Konzentration auf kritische Bereiche erfolgen soll. Geschäftsprozesse werden in allen Beispielen erwähnt, wobei auch Management-Prozesse von GRC gemeint sind. Prozesse werden in den Praxisbeispielen in Kern- und Unterstützungsprozesse unterteilt. Verantwortlichkeiten sind auf allen Hierarchieebenen relevant. Geschäftsdokumente werden hinsichtlich der Dokumentation von Kontrollen und des Berichtwesens genannt. Für Risiken wird eine Unterteilung in Risikokategorien vorgeschlagen [Kl11]. Die Beispiele zeigen, dass auch finanziellen Kennzahlen wie Rentabilität und Kosten von Bedeutung für GRC sind. Ebenso ist der Wert bzw. Wertbeitrag von GRC als Kennzahl relevant.

Kontrolle	Rolle	Geschäfts-prozess	Kontrollziel	Richtlinie	Risiko	GRC-Quelldokument	Ressource	Ziel	Anwendungs-bereich	Geschäfts-dokument	Assessment	IT Komponente	Performance Indicator	Stakeholder	Strategie	Reifegrad	Rahmenwerk	Ausführung	Monitor	Verletzung	Implemen-tierungslogik
16	16	21	13	11	13	6	2	11	5	15	13	14	7	6	9	3	7	1	0	2	0

Tabelle 4: Anzahl von Praxisbeispielen mit zugeordneten Begriffen zu den Informationsobjekten

Einige weitere Begriffe sind in den Praxisbeispielen von hoher Relevanz, lassen sich jedoch nicht direkt den Informationsobjekten zuordnen und werden daher näher diskutiert. Begriffe wie Konzern, Division und Landesgesellschaft verdeutlichen die Komplexität internationaler Konzerne. Das Referenzmodell kann dies durch mehrere Modelle auf unterschiedlichen Ebenen abbilden. Der Begriff Projekt bezieht sich in den Beispielen zum einen auf Projekte zur Umsetzung von GRC-Vorgaben. Andererseits werden Geschäftsinitiativen, insbesondere auch im IT-Bereich, durch Projekte umgesetzt und sind somit Gegenstand der Steuerung von GRC. Mehrere Praxisbeispiele erwähnen die Durchführung von Schulungen, welche eine Kontrollart sind, die eine direkte Beziehung zum Informationsobjekt Rolle haben (siehe Anforderung „Faktoren des menschlichen

Verhaltens“). Der Begriff Steuerung ist in den Beispielen von herausragender Bedeutung. Er bezieht auf den Governance-Begriff und bildet die Aufgabe von GRC zur Steuerung von „Perfomance“- und „Conformance“ ab. Außerdem wird mehrfach der Begriff Schwäche genannt, welcher im Sinne von Kontrollschwächen verwendet wird und dem Referenzmodell hinzuzufügen ist. Weitere Begriffe, die im Zusammenhang der Finanzberichterstattung genannt werden, sind Finanzdaten und Konto. Beide Begriffe stellen einen Gegenstand von Kontrollen dar und werden im Referenzmodell daher unter Ressourcen subsumiert. GRC soll auf strategischer Ebene Entscheidungen unterstützen. Zur Entscheidungsunterstützung sind insbesondere Informationen aus Assessments und Kennzahlen relevant. Hierzu ist auch eine Meeting-Struktur, die Entscheidungsgremien beinhaltet, notwendig. Entscheidung wird dem Modell daher als Informationsobjekt hinzugefügt. Die Begriffe Service Level Agreement und Service werden ebenfalls genannt, sind jedoch speziell für die IT-Governance von Relevanz und werden daher nicht in das generische Modell aufgenommen. Sie stellen die Bedeutung von Services als Gegenstand von Kontrollen und die Bedeutung von Verträgen als GRC-Vorgabe heraus.

Beziehungen der Informationsobjekte: Beziehungen werden allgemein wenig betrachtet und deren Analyse durch die ungenaue Terminologie erschwert. So wird bspw. mehrmals von Scoping (Informationsobjekt Anwendungsbereich) gesprochen, jedoch nicht deutlich, ob sich dies auf GRC-Vorgaben, Kontrollziele, Kontrollen, Risiken oder Richtlinien bezieht. Teilweise werden die Beziehungen selbst aber auch sehr allgemein beschrieben. So sollen Abteilungen bspw. an Zielen ausgerichtet werden [FG07, 282]. Lediglich das Praxisbeispiel in [Tü12] diskutiert explizit die Integration von GRC, fokussiert hierbei jedoch nicht die Informationsstruktur, sondern die Organisation und Berichterstattung. Die Unterscheidung zwischen den Informationsobjekten Kontrollziel und Kontrolle wird nicht in allen Praxisbeispielen explizit getroffen. Daher werden Kontrollen wie bspw. in [Me06, 440] nicht immer den Kontrollzielen zugeordnet, sondern teilweise direkt den Risiken [Me06, 443 und 467]. Beziehungen zwischen Kontrollen [Me06, 440, GUB07], Kontrollen und Prozessen [Me06, 443], Risiken und Zielen [Kl11, 106] sowie Prozessen und Assessments [JT07, 236; FG07, 268] werden bestätigt.

6 Fazit

In diesem Beitrag wurde ein fachkonzeptionelles Referenzmodell für ein strategisches GRC-Management entwickelt, welches die relevanten Informationsobjekte und strukturellen Zusammenhänge aufzeigt. Aus der praxisorientierten Evaluierung an Beispielen ergaben sich nur geringfüge Anpassungen und einige Hinweise zur Detailierung des Modells. Die gewählte Art der Evaluierung erscheint angemessen, da die Forschung zur GRC-Integration noch sehr am Anfang steht und die dokumentierten Beispiele eine ausreichende inhaltliche Tiefe aufweisen. Außerdem wurden bereits im Entwurfsprozess des Referenzmodells existierende Modellpublikationen und allgemeine Anforderungen in den betrachteten Bereichen integriert. Es ist zu beachten, dass die Evaluierung der Beziehungen zwischen den Informationsobjekten durch die Fallbeispiele nur eingeschränkt möglich war. Obwohl durch die Modelle aus der Literatur und auch durch die strategischen GRC-Anforderungen eine Begründung für die Zusammenhänge der Modellelemente geliefert wurde, sollten die Beziehungen Gegenstand weiterer Forschung

sein. Ziel des hier dargestellten Forschungsvorhabens war die Entwicklung eines fachkonzeptionellen Referenzmodells. Zur Umsetzung in einem Informationssystem bedarf dieses weiterer Verfeinerung bspw. hinsichtlich der Attribute der Informationsobjekte. Außerdem sind hinsichtlich der organisatorischen Unternehmenshierarchie in großen Konzernen zukünftig weitere Detaillierungen der Informationsobjekte zweckmäßig. Weiterer Forschungsbedarf besteht beispielsweise auch hinsichtlich der Anwendbarkeit des Modells in unterschiedlichen Branchen.

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.

[Be02] Becker, J.; Delfmann, P.; Knackstedt, K.; Kuropka, K.: Konfigurative Referenzmodellierung. In (Becker, J.; Knackstedt, R. Hrsg.): Wissensmanagement mit Referenzmodellen. Konzepte für die Anwendungssystem- und Organisationsgestaltung. Heidelberg, 2002, S. 25-144.

[Bh09] Bhimani, A.: Risk Management, corporate governance and management accounting. Emerging interdependencies. In: Management Accounting Research 20 (2009) 1, S. 2-5.

[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.

[BMM06] Bohnsack, R.; Marotzki, W.; Meuser, M.: Hauptbegriffe qualitativer Sozialforschung. 2. Aufl., Budirch, Opladen, 2006.

[Ch76] Chen, P.P.-S.: The entity-relationship model - toward a unified view of data. In: ACM Transactions on Database Systems 1 (1976) 1, S. 9-36.

[De11] Deutsches Institut für Interne Revision (Hsg.): Internationale Standards für die berufliche Praxis der Internen Revision 2011. Frankfurt am Main, 2011.

[KSP08] El Kharbili, M.; Stein, S.; Pulvermüller, E.: Policy-Based Semantic Compliance Checking for Business Process Management. In : Proc. MobIS, Saarbrücken, 2008, S. 178-192.

[FL04] Fettke, P.; Loos, P.: Entwicklung eines Bezugsrahmens zur Evaluierung von Referenumodellen – Langfassung eines Beitrages. In (Loos, P. Hrsg.): Working Papers of the Research Group Information Systems & Management. Mainz, 2004.

[FG07] Fröhlich, M.; Glasner, K.: IT Governance. Leitfaden für eine praxisgerechte Implementierung. Gabler, Wiesbaden, 2007.

[Ge09] Gericke, A.; Fill, H.-G.; Karagiannis, D.; Winter, R.: Situational Method Engineering for Governance, Risk and Compliance Information Systems. In: Proc. DESRIST, 2009.

[GUB07] Gigerl, T.; Unger, C.; Baumgartner, C.: Umsetzung eines integrierten IT-Compliance-Frameworks - am Beispiel ALTANA Pharma. In: Information Manageent & Consulting 22 (2007) 4, S. 70-77.

[GV06] Goedertier, S.; Vanthienen, J.: Business Rules for Compliant Business Process Models. In: Proc. International Conference on Business Information Systems (BIS), 2006, S. 558-572.

[HR09] Herath, T.; Rao, R.: Protection motivation and deterrence: a framework for security policy compliance in organizations. In: EJIS 18 (2009) 2, S. 106-125.

[He04] Hevner, A.R.; March, S.T.; Park, J.; Ram, S.: Design science in information system research. In: MISQ 28 (2004) 1, S. 75-105.

[In10] Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW, Hrsg.): Entwurf IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW EPS 980) Stand: 11.03.2010. Düsseldorf, 2010.

[In08] International Organization for Standardizatin, International Electrotechnical Commission (ISO, IEC Hrsg.): Corporate Governance of information technology. o.O., 2008.

[JG06] Johannsen, W.; Goeken, M.: IT-Governance – neue Aufgaben des IT-Managements. In: HMD – Praxis der Wirtschaftsinformatik (2006) 250, S. 7-20.

[JT07] Just, D.; Tami, F.: Praxisbeispiel: Bewertung von Applikationsportfolios und IT-Prozessen. In (Johannsen, W.; Goeken, M.): Referenzmodelle für IT-Governance. Strategische Effektivität und Effizienz mit COBIT, ITIL & Co. Dpunkt.verlag, Heidelberg, 2007, S. 225-242.

[Kl11] Kley, W.-D.: Risiko- und Chancenmanagement der MAN SE. In: Zeitschrift für Controlling & Management 55 (2011) 2, S. 105-110.

[Kl09] Klotz, M.: IT-Compliance. Ein Überblick. Dpunkt, Heidelberg, 2009.
[MN12] Marekfia, W.; Nissen, V.: Anforderungen an ein strategisches GRC-Management. In: Proc. Informatik, 2012, S. 731-745.
[Me06] Menzies, C.: Sarbanes-Oxley und Corporate Compliance – Nachhaltigkeit, Optimierung, Integration. Schäffer-Poeschel, Stuttgart, 2006.
[MG10] Milicevic, D.; Goeken, M.: Konzepte der Informationssichereit in Standards am Beispiel der ISO 27001. In: Proc. Informatik, 2010, S. 305-310.
[MS09] Mitchell, S. L.; Switzer, C.S.: GRC capability model. Red Book 2.0. Open Compliance & Ethics Group, Phoenix, AZ, 2009.
[Mü07] Müller, G.: Für Sie gelesen. In: Wirtschaftsinformatik 49 (2007) Sonderheft, S. 107-109.
[NS07] Namiri, K.; Stojanovic, N.: A Semantic-based Approach for Compliance Management of Internal Controls in Business Process Management. In: Proc. CAISE, 2007.
[OMG10] OMG: Unified Modelling Language: Infrastructure, Version 2.3. Needham, 2010.
[Op12] Open Compliance & Ethics Group (Hrsg.): 2012 GRC Maturity Survey. 2012.
[RWS10a] Racz, N.; Weippl, E.; Seufert, A.: A frame of reference for research of integrated GRC. In: De Decker, B.; Schaumüller-Bichl, I. (Hrsg.): Communications and Multimedia Security. 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: Databases and Information Systems VI. Selected Papers from the 9th International Baltic Conference, 2010.
[Sa08a] Sackmann, S.: A Reference Model for Process-oriented IT Risk Management. In (Golden, W. et al. Hrsg.): Proc. ECIS, GITO-Verlag, Berlin, 2008, S. 1137-1148.
[Sa08b] Sackmann, S.: Automatisierung von Compliance. In: HMD – Praxis der Wirtschaftsinformatik 45 (2008) 263, S.39-46.
[SGN07] Sadiq, S; Governatori, G., Naimiri, K.: Modeling Control Objectives for Business Process Compliance. In: Proc. of the 5th Conference on Business Process Management, 2007.
[Sc02] Scheer, A.-W.: ARIS – Vom Geschäftsprozeß zum Anwendungssystem. 4. Aufl., Springer, Berlin et al., 2002.
[Sc97] Schütte, R.: Die neuen Grundsätze ordnungsmäßiger Modellierung. (Paper zum Forschungsforum `97, Leipzig 16.09-20.09.97)
[SLP08] Sienou, A.; Lamine, E.; Pingaud, H.: A Method for Integrated Management of Process-risk. In: Proceedings of GRCIS, Montpellier, 2008.
[Si09] Silveira, P.; Rodriguez, C.; Casati, F.; Daniel, F.; D' Andrea, V.; Worledge, C.; Taberi, Z.: On the Design of Compliance Governance Dashboards for Effective Compliance and Audit Management. In: Proc. ICSOC Workshops, 2009.
[Po08] Pohlman, M.: Oracle identity management: governance, risk, and compliance architecture. 3. Aufl., CRC Press, Boca Raton et al., 2008.
[TF08] Teubner, A.; Feller, T.: Informationstechnologie, Governance und Compliance. In: Wirtschaftsinformatik 50(2008) 5, S. 400-407.
[TF09] Teuteberg, F.; Freundlieb, M.: Compliance Management mit betrieblichen Umweltinformationssystemen. In: wisu – das wirtschaftsstudium (2009) 4, S. 550-557.
[Th07] The IT Governance Institute (ITGI, Hrsg.) COBIT 4.1. o.O., 2007.
[Tü12] Tüllner, J.: Integration von Governance, Risikomanagement und Compliance. Erfahrungsbericht über ein Projekt zur Optimierung der Unternehmenssteuerung und einen ganzheitlichen Lösungsansatz. In: Zeitschrift für Corporate Governance 7 (2012) 3, S. 118-121.
[VHW91] Verhoef, T. F.; Hofstede, A.H.M.T.; Wijers, G.M.: Structuring Modelling Knowledge for CASE Shells. In (Andersen, R. et al. Hrsg.): Proc. CAiSE, 1991, S. 502-524.
[Br03] vom Brocke, J.: Referenzmodellierung. Gestaltung und Verteilung von Konstruktionsprozessen. Logos, Berlin, 2003.
[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.
[WHH11] Weigand, H.; van den Henvel, W.-J.; Hiel, M.: Business Policy Compliance in Service-oriented systems. In: Information Systems 36 (2011) 4, S. 791-807.
[Wi10] Withus, K.-H.: Sicherstellung der Compliance durch wirksame Managementsysteme. In: Zeitschrift für Interne Revision 7 (2010) 3, S. 99-108.
[Ze99] Zelewski, S.: Ontologien zur Strukturierung von Domänenwissen – Ein Annäherungsversuch aus betriebswirtschaftlicher Perspektive. Arbeitsbericht Nr. 3, Institut für Produktion und Industrielles Informationsmanagement, Essen, 1999