

Diplomarbeit

**Formale Abbildung der regulatorischen
Compliance auf Security Policies**

Elena-Crina Bostan
21. Mai 2011

Gutachter:

Prof. Dr. Jan Jürjens

Prof. Dr. Martin Hirsch

Fakultät für Informatik
Lehrstuhl Software Engineering (LS14)
Otto-Hahn Straße 14
44227 Dortmund

Fraunhofer-Institut für
Software- und Systemtechnik (ISST)
Emil-Figge-Straße 91
44227 Dortmund

meiner Schwester, Monica

Inhaltsverzeichnis

Abbildungsverzeichnis	vi
Tabellenverzeichnis	vii
1 Einleitung	1
1.1 Motivation: Compliance, Informationstechnologie und Automatisierung . . .	1
1.2 Aufgabe und Ziel der Diplomarbeit	2
1.3 Aufbau der Arbeit	3
2 Grundlagen: Compliance und IT-Security	5
2.1 Compliance	6
2.1.1 Die normative/legalistische Dimension der Compliance	7
2.1.2 Die handlungsorientierte Dimension der Compliance	11
2.1.3 Die nachweisorientierte Dimension der Compliance	13
2.2 Compliance und IT	14
2.2.1 IT-gestützte Compliance	14
2.2.2 IT-Compliance	16
2.2.3 Compliance und IT-Security	16
2.3 IT-Security-Policies	20
2.3.1 Informationsmodelle für IT-Security Policies	23
2.3.2 Policy-Sprachen	23
2.3.3 Beitrag der IT-Security-Standards zur Erstellung der IT-Security-Policies	25
2.4 Zusammenfassung	28
3 Die Analyse der regulatorischen Texte	29
3.1 Eigenschaften der juristischen Sprache	29
3.2 Probleme bei der Analyse der juristischen Texte	32
3.2.1 Ambiguität und Vagheit	32
3.2.2 Die Intertextualität des Gesetzestextes	33
3.3 Zusammenfassung	34

4	Compliance Management: Stand der Forschung	35
4.1	Systematische Darstellung des juristischen Wissens	36
4.2	Systematische Darstellung des juristischen Textes	39
4.3	Regulatorische Compliance und Requirements Engineering	41
4.4	Zusammenfassung	43
5	Von der MaRisk VA zu IT-Security Policies	45
5.1	Vorüberlegungen	45
5.1.1	Die Rolle der IT in Versicherungsunternehmen	45
5.1.2	Struktur und Inhalt von MaRisk VA	47
5.2	Abbildung von MaRisk VA auf IT-Security-Policies	49
5.2.1	Die Analysekomponente	51
5.2.2	Die Abbildungskomponente	59
5.3	Zusammenfassung	61
6	Anwendung des Frameworks	63
6.1	Anwendung der Analysekomponente	63
6.1.1	Identifizierung der Compliance Anforderungen	63
6.1.2	Analyse der Anforderungen an die IT-Security	65
6.2	Anwendung der Abbildungskomponente	70
6.3	Zusammenfassung	76
7	Erfahrungen und Diskussion	79
7.1	Anwendungsbereich des Frameworks	79
7.2	Wirkungsbereich des Frameworks	79
7.3	Anforderungen an das Benutzerprofil	80
7.4	Unterstützung der Benutzer durch (Teil-)Automatisierung	81
7.5	Zusammenfassung	84
8	Zusammenfassung und Ausblick	85
8.1	Zusammenfassung	85
8.2	Ausblick	87
A	Gefährdungen für verschiedene Aktivitäten	89
	Literaturverzeichnis	100
	Erklärung	100

Abbildungsverzeichnis

2.1	Regulatorische Anforderungen im Jahr 2007 [66].	9
2.2	Die GRC-Trias (vgl. [33]).	12
2.3	Rolle der IT in Unternehmen nach einer Deloitte-Studie aus 2009 [19].	15
2.4	Wechselbeziehung zwischen IT und Compliance.	16
2.5	Klassen des CIM/PCIM von IETF [45].	23
2.6	Ziele beim Einsatz von Security Standards.	26
3.1	Die gesetzliche Taxonomie von Hohfeld.	31
3.2	Querverweise im Gesetzestext.	33
4.1	<i>Semantic parameterization</i> (vgl. [13]).	38
4.2	XML-Baum eines Gesetzes nach REGNET-Konzept [46].	40
4.3	Modellierung der Compliance Anforderungen mit Secure Tropos [40].	42
4.4	Unterstützung der IT-Security-Ziele durch UMLsec.	43
5.1	Vorgehen in der Diplomarbeit (rote Pfeile)	51
5.2	Elemente bei der Analyse der Compliance Anforderungen.	53
6.1	Querverweis § 64a Abs.3 VAG aus <i>10 Information und Dokumentation</i> von <i>MaRisk VA</i>	66
6.2	Lebenszyklus eines Dokumentes.	70
6.3	Gefährdungen im Lebenszyklus eines Dokumentes.	71
6.4	Gefährdungen für die Aktivität <i>Dokument verfassen</i>	71
6.5	Der Geschäftsprozess <i>Dokument editieren</i> mit Berücksichtigung der Anforderungen an die IT-Security.	77
7.1	Relevante Stellen aus den <i>BSI-IT-Grundschutzkatalogen</i> für die IT-Security-kritischen Aktivitäten (vgl. [65]).	83
A.1	Gefährdungen für die Aktivität <i>Dokument speichern</i>	89
A.2	Gefährdungen für die Aktivität <i>Dokument aufbewahren</i>	90
A.3	Gefährdungen für die Aktivität <i>Dokument bearbeiten</i>	91

A.4	Gefährdungen für die Aktivität <i>Dokument digitalisieren</i>	91
A.5	Gefährdungen für die Aktivität <i>Dokument ausdrucken</i>	92

Tabellenverzeichnis

2.1	Beispiel einer <i>high-level</i> -IT-Security-Policy für Passwörter.	21
2.2	IT-Security-Policies [51].	22
4.1	Anwendung der <i>semantic-parameterization</i> -Methode (vgl. [13]).	39
6.1	<i>10 Information und Dokumentation</i> aus der <i>MaRisk VA</i>	64
6.2	IT-Security Anforderungen in der <i>MaRisk VA</i> §10 und in den darin enthaltenen Querverweisen.	69
6.3	IT-Security-Policies für den Teilprozess <i>Dokument erstellen</i>	75
7.1	Anforderungen an die Ausbildung des Benutzers.	81

Kapitel 1

Einleitung

1.1 Motivation: Compliance, Informationstechnologie und Automatisierung

30 Mrd. US-Dollar Schulden, alle 22 000 Beschäftigte ohne Arbeitsplatz und der Aktienpreis sinkt von 90 Dollar auf ein paar Cents: das war der Stand der Firma Enron, als diese im Dezember 2001 Konkurs angemeldet hat. Damit erlebte die US-Wirtschaft einen der bisher größten Unternehmensskandale [22]. Dem Insolvenzverfahren von Enron folgte im Juni 2002 der Bilanzskandal von WorldCom: in diesem Fall wurden Falschbuchungen im Wert von 11 Mrd. US-Dollar durch die Börsenaufsicht aufgedeckt [6].

Das Ausmaß des Konkurses dieser Firmen, die zu den größten Unternehmen der USA zählten, haben zu einem Reformdruck im Bereich der Wirtschafts- und Bilanzprüfung von börsennotierten Unternehmen geführt [80]. Die Reaktion des US-Kongresses war die Verabschiedung des *Corporate Responsibility Act 2002* am 30 Juli 2002, auch als *Sarbanes-Oxley-Act (SOX)* bekannt. Es gab auch vor diesem Zeitpunkt gesetzliche Vorgaben, welche die Unternehmen erfüllen mussten. Das *Bundesdatenschutzgesetz (1977)* und die *GoBS (1977)* in Deutschland, oder die *Europäische Datenschutzrichtlinie 1995/46/EG* auf europäischer Ebene, sind nur einige der Anforderungen dieser Art. *SOX* unterscheidet sich von den bisherigen Gesetzen dadurch, dass es die Einführung, die Überwachung und die Dokumentation von IT-Security- und Kontrollmechanismen in den Unternehmen verlangt. Für diese Kontrollen haften der Geschäftsführer, der Leiter der Finanzabteilung und der Abschlussprüfer persönlich.

SOX hat die Unternehmenskultur auf der ganzen Welt entscheidend verändert, obwohl es nur für die Unternehmen gilt, die am US-Kapitalmarkt notiert und gegenüber der *Securities and Exchange Commission (SEC)* verpflichtet sind [2]. Dieses Gesetz hat einen neuen Begriff in die Unternehmenswelt eingeführt, welcher in den letzten Jahren zum Trend ge-

worden ist: *Compliance*. Mit diesem Begriff wird die Pflicht der Unternehmen zu einem gesetzmäßigen und regelkonformen Verhalten beschrieben.

Nach der Verabschiedung von *SOX* entwickelt und verstärkt sich der Compliance-Gedanke weiter. Die Anzahl der Gesetze, Verordnungen, Normen und Richtlinien, welche die Unternehmen beachten müssen, erhöht sich. Einerseits werden Reformen der Wirtschaftsprüfung durch SOX-ähnliche Gesetze in anderen Ländern durchgeführt, z. B. in Kanada (*Bill C198*), in Japan (*J-SOX*) oder in Europa (*Euro-SOX*). Diese Gesetze haben den Zweck, das Vertrauen der Anleger in Finanzzahlen und Märkte zu stärken. Andererseits haben die wachsende Globalisierung, der Technikfortschritt und der Einsatz neuer Informationstechnologien (IT) zu einer stets veränderten Risikolage geführt, was eine Anpassung der schon vorhandenen Regularien nötig gemacht hat [79]. Darüber hinaus haben sich immer mehr Unternehmen entschlossen, eigene Security- und Risikostandards einzuführen.

Verstöße gegen die regulatorischen Anforderungen können für das Unternehmen weitreichende Auswirkungen haben. Unter anderem drohen: Geldstrafen, Freiheitsstrafen, Schadens- und Strafschadensersatz, Gewinnabschöpfungen, Abbruch von Geschäftsbeziehungen, Ausschluss von Aufträgen, Imageschäden, negative Beurteilungen am Kapitalmarkt usw. Solche Gefahren müssen durch ein effizientes Compliance Management vermieden werden. Dafür können auch die Ressourcen der Informationstechnologie (IT), welche heutzutage aus dem Leben eines Unternehmens nicht mehr wegzudenken sind, ausgenutzt werden. Die IT bietet den Vorteil der Automatisierungsmöglichkeit in vielen Bereichen eines Unternehmens. Die Gestaltung einer „complianten“ Organisation durch die Automatisierung der Compliance Aktivitäten führt nicht nur zur Minimierung der Fehleranfälligkeit, die mit einer manuellen Umsetzung und Überprüfung verbunden ist, sondern auch zur Einsparung der Ressourcen und Senkung der Kosten im Betrieb.

Der Einsatz der IT in Unternehmen bringt nicht nur die Vorteile der Automatisierung, sondern stellt auch Anforderungen an den Umgang mit der Information und den Daten. Eine IT-Infrastruktur erfüllt ihren Zweck nur, wenn sie effektiv definiert, kontrolliert und verwaltet wird, um den Schutz der vorhandenen Information und der Daten zu gewährleisten (IT-Security).

1.2 Aufgabe und Ziel der Diplomarbeit

Diese Diplomarbeit hat die Aufgabe zu untersuchen, ob es möglich ist, IT-Security-Policies direkt von dem regulatorischen Text *Mindestanforderungen an das Risikomanagement in Versicherungsunternehmen (MaRisk VA)* abzuleiten.

Es ist Ziel dieser Untersuchung, ein Konzept zur Abbildung der regulatorischen Compliance auf IT-Security-Policies zu entwickeln. Solche IT-Security-Policies, welche direkt aus dem regulatorischen Text abgeleitet werden, haben den Vorteil, dass sie eine integrierte Sicht auf die Compliance und auf die IT-Security anbieten.

Damit dieses Ziel erreicht wird, muss zuerst untersucht werden, wie die Compliance Anforderungen aus dem Gesetzestext identifiziert, und welche davon auf IT-Security-Policies abgebildet werden können. Diese Aufgabe setzt die Definition der Compliance und der IT-Security voraus. Der nächste Schritt besteht darin, eine Möglichkeit zu finden, um die Abbildung der Compliance Anforderungen auf IT-Security-Policies vorzunehmen.

1.3 Aufbau der Arbeit

Die vorliegende Diplomarbeit enthält folgende Kapitel:

Kapitel 2: Grundlagen: Compliance, IT-Security und IT-Security-Policies

In diesem Kapitel werden die Schlüsselbegriffe *Compliance*, *IT-Security* und *IT-Security-Policies* definiert, welche im Lauf der gesamten Arbeit benutzt werden. Es werden die Quellen der regulatorischen Compliance gezeigt und die Rolle der IT-Security beschrieben. Darauf folgend werden sowohl die Compliance, als auch die IT-Security innerhalb des Governance-Compliance-Risiko-Modells (GRC-Modell) betrachtet. Einige relevante Compliance Texte und IT-Security Standards werden als Beispiel für Compliance und IT-Security vorgestellt. Hier wird auch die Rolle der IT-Security-Policies in einer IT-Organisation gezeigt und ihr Entstehungsprozess wird beschrieben. Einige modellbasierte und sprachbasierte Ansätze für die Definition der Security Policies werden anschließend vorgestellt.

Kapitel 3: Die Analyse der regulatorischen Texte

Die Compliance Anforderungen werden in einer Fachsprache verfasst, welche die Mehrdeutigkeit der natürlichen Sprache mit dem Jargon der juristischen Sprache verbindet. In diesem Kapitel werden die Eigenschaften der Gesetzessprache beschrieben und die Probleme identifiziert, welche bei der Analyse solcher Texte besonders für Nicht-Juristen auftreten können.

Kapitel 4: Compliance Management: Stand der Forschung

Mehrere aktuelle Arbeiten und Forschungsrichtungen, welche die Schwerpunkte Analyse der Compliance Anforderungen, Compliance und IT-Security, oder Formalisierung des regulatorischen Textes haben, werden in diesem Kapitel vorgestellt.

Kapitel 5: Von der MaRisk VA zu IT-Security-Policies

Dieses Kapitel stellt das im Rahmen dieser Diplomarbeit entwickelte Framework zur Abbildung der regulatorischen Compliance auf IT-Security-Policies vor.

Kapitel 6: Anwendung des Frameworks

Das im vorigen Kapitel beschriebene Framework wird auf einem Abschnitt aus der MaRisk VA angewendet.

Kapitel 7: Erfahrungen und Diskussion

Dieses Kapitel stellt die Anforderungen an die Ausbildung des Benutzers, der das in dieser Diplomarbeit entwickelte Framework anwenden soll. Des Weiteren werden einige Möglichkeiten vorgestellt, Teilschritte des Verfahrens automatisiert durchzuführen.

Kapitel 8: Zusammenfassung und Ausblick

Eine Zusammenfassung der Ergebnisse der Diplomarbeit findet in diesem letzten Kapitel statt. Zuletzt kommt ein Ausblick auf mögliche Forschungen auf dem Gebiet IT-Security im Zusammenhang mit Compliance, welche auf den Ergebnissen dieser Arbeit basieren können.

Kapitel 2

Grundlagen: Compliance und IT-Security

Das Ziel dieser Diplomarbeit, regulatorische Compliance auf IT-Security-Policies abzubilden, stellt einige Herausforderungen dar: was ist regulatorische Compliance? Was ist IT-Security und wie trägt diese zur Einhaltung der Compliance bei? Was sind und welche Rolle haben die IT-Security-Policies? Die Antwort auf diese Fragen stellt die Basis der vorliegenden Arbeit dar. Die Aufgabe dieses Kapitels ist die Bedeutung von *Compliance*, *IT-Security* und *IT-Security-Policies* zu erklären, und den Zusammenhang zwischen diesen Konzepten hervorzuheben.

Begrifflichkeit Einige allgemeine Begriffe, die in dieser Arbeit verwendet werden, werden wie folgt definiert: Mit *Organisation* sind in dieser Diplomarbeit besonders Unternehmen gemeint, aber auch andere Institutionen, wie z. B. Behörden, Vereine usw., welche Compliance-Anforderungen aus unterschiedlichen Quellen erfüllen müssen.

Eine Organisation kann sich für die Erfüllung ihrer Aufgaben der IT bedienen. Dafür werden *IT-Systeme* verwendet. Ein IT-System ist, wie aus der Literatur bekannt [21], „ein dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen“.

Ein *Geschäftsprozess* ist eine Reihe von festgelegten Tätigkeiten (Aktivitäten, Aufgaben) in einer Organisation, welche von Menschen oder Maschinen ausgeführt werden, um die festgelegten Ziele dieser Organisation zu erreichen [26]. Die Geschäftsprozesse werden oft mit speziellen Tools (z. B. ARIS¹, Adonis² oder Bonapart³) modelliert, damit sie besser nachvollzogen, verwaltet oder sogar automatisiert werden können.

¹www.ids-scheer.de (abgerufen am 20.04.2011)

²www.boc.eu.com (abgerufen am 20.04.2011)

³www.proubis.de (abgerufen am 20.04.2011)

Des Weiteren besitzt eine Organisation bestimmte *Werte* (engl. *assets*), welche für die Tätigkeiten dieser Organisation wichtig sind und aufbewahrt werden müssen. Solche Werte sind (gemäß ISO 27001, Klassifizierung aus [47]):

- Informationen: Daten, Dateien, Verzeichnisse, Datenbanken, Systembeschreibungen, Nutzerhandbüchern, Arbeitsanweisungen, Verträge, Protokolle,
- Software: Anwendungssoftware, System-Software, Entwicklungswerkzeuge,
- Physische Werte: Rechner, Firewalls, Gateways, Router, Netzkabel, Datenmedien,
- Dienstleistungen, welche durch die Organisationen erbracht oder selbst genutzt werden, wie z. B. Telekommunikation-Services oder Datenübertragung,
- Mitarbeiter, welche verschiedene Funktionen und Rollen haben und Qualifikationen und Fähigkeiten besitzen,
- Sonstige Werte, wie Reputation und Glaubwürdigkeit der Organisation.

2.1 Compliance

Der Begriff „Compliance“ Obwohl im Deutschen noch als Anglizismus betrachtet und trotz den Kontroversen und Debatten [86], die seine Verwendung verursacht, wird das Wort *Compliance* (ursprünglich aus dem Lateinischen *compleo*, *-ere* = „erfüllen, ausfüllen, ganz zum Ende führen“ [3]) seinen Übersetzungen *Erfüllung*, *Einhaltung*, *Übereinstimmung*, *Komplianz*, *Befolgung* vorangezogen. Die Bevorzugung des englischen Begriffes zeigt, dass keine der deutschen Übersetzungen die Bedeutung von *Compliance* präzise genug ausdrücken kann. In der deutschen Sprache fängt das Wort bereits in den frühen 1990er Jahren an benutzt zu werden, weil viele Unternehmen Geschäftsbeziehungen im anglo-amerikanischen Raum hatten; mit dem SOX aus 2002 wird Compliance zu einem Trend-Wort. Wie in [74] nachzulesen ist, befindet sich der Begriff *Compliance* im Stadium der Entwicklung zu einem Fachterminus, welcher alle oben genannten konkurrierenden deutschen Entsprechungen enthält.

Eine gesetzliche oder eine allgemein anerkannte, einheitliche Definition des Begriffes *Compliance* gibt es bisher nicht [30]. Wie bei [32] nachzulesen ist, kann Compliance in einfacher Form als „Befolgung, Übereinstimmung, Einhaltung bestimmter Gebote“ definiert werden. In [79] wird Compliance definiert als

„ [...] die Kenntnis und Einhaltung sämtlicher regulatorischen Vorgaben und Anforderungen an das Unternehmen, die Aufgabe und die Einrichtung

entsprechender Prozesse und die Schaffung eines Bewusstseins der Mitarbeiter für Regelkonformität, sowie die Kontrolle und Dokumentation der Einhaltung der relevanten Bestimmungen gegenüber internen und externen Adressaten.“

Diese umfangreiche Definition zeigt drei Dimensionen für die Compliance, welche im Folgenden näher erklärt werden:

- Normativ/legalistisch,
- Handlungsorientiert,
- Nachweisorientiert.

2.1.1 Die normative/legalistische Dimension der Compliance

Für eine Organisation bedeutet Compliance, alle für diese Organisation relevanten Anforderungen zu beachten und zu erfüllen. Der Umfang dieser Anforderungen ist in der Literatur unterschiedlich, daher werden im Folgenden zwei Sichtweisen auf die Compliance vorgestellt: Compliance in enger und in weiter Auffassung.

Compliance in enger Auffassung In diesem Fall bezieht sich der Begriff *Compliance* nur auf die Erfüllung der rechtlich vorgeschriebenen Anforderungen der gesetzlichen Vorgaben (z. B. in [83]). Diese werden sowohl von nationalen oder internationalen Gesetzgebern erlassen, als auch von supranationalen Gesetzgebern. In Deutschland muss z. B. das *Bundesdatenschutzgesetz* oder das *Versicherungsaufsichtsgesetz (VAG)* beachtet werden. *SOX*, das in den USA erlassen wurde, muss nicht nur von den amerikanischen Kreditinstituten, sondern auch von ausländischen Firmen, die an der amerikanischen Börse notiert sind, erfüllt werden. Ein supranationaler Gesetzgeber ist z. B. die Europäische Union (EU). Die EU erlässt regelmäßig Verordnungen, Beschlüsse und Empfehlungen, welche unterschiedlich in das nationale Recht der Mitgliedsstaaten in einem bestimmten Zeitraum umgesetzt werden müssen oder sollen [1]. Die *8. EU-Richtlinie* über die Prüfung von Jahresanschlüssen, welche als *Euro-SOX* bekannt ist, wurde in 2006 von der Europäischen Kommission erlassen und ist für alle Staaten der EU verbindlich.

Als gesetzliche Vorgaben zählen auch: Verordnungen, welche von den Verwaltungen auf Basis der Gesetze erlassen werden; Verwaltungsvorschriften und weitere Regelwerke, auf die in Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften verwiesen wird oder von der Rechtsprechung zur Auslegung herangezogen werden.

Compliance in weiterer Auffassung Im diesen Sinne zählen nach [31] zu den Compliance Anforderungen nicht nur die Gesetze, sondern auch:

- *Unternehmensexterne Vorgaben:*

Die unternehmensexternen Regelwerke sind diejenigen *Frameworks*, *Referenzmodelle* oder *Best-Practice-Modelle*, welche als Standards gehalten werden. Hier sind *IT Infrastructure Library (ITIL)*, *Capability Maturity Model Integration (CMMI)*, *Control Objectives for Information and Related Technology (CobiT)* oder *ISO 2700** zu erwähnen. Des Weiteren zählen zu den unternehmensexternen Regelwerken Normen, Zertifikate oder branchenspezifische Vorgaben. Die Einhaltung dieser Vorgaben kann verpflichtend sein, wenn z. B. die Qualität eines Produktes oder einer Dienstleistung garantiert werden muss. Diese Vorgaben können aber auch freiwillig in Organisationen eingeführt und beachtet werden, wenn diese als Basis für Testierungen oder Zertifizierungen dienen.

- *Verträge mit Geschäftspartnern:*

Im Besonderen sind dies kommerzielle Verträge im Business-to-Business (B2B)-Bereich, welche Service-Level-, Non-Disclosure-, Datenschutz- oder Datenübertragung-Vereinbarungen enthalten, die Einhaltung von Meilensteinen vereinbaren oder zur ausführlichen Dokumentation verpflichten.

- *Unternehmensinterne Vorgaben:*

Hierbei handelt es sich um unternehmenseigene Verhaltenskodizes, Unternehmensrichtlinien, Hausstandards, Organisations- oder Verfahrensanweisungen, *Best Practices* oder interne Festlegungen, welche zur Unternehmenskultur gehören. Wie aus der Abbildung 2.1 zu entnehmen ist, passiert es oft, dass eine Organisation mehrere Gesetze, Standards und Vorgaben gleichzeitig beachten muss. In der Literatur [68] wird die Bemerkung gemacht, dass die Compliance mit allen passenden existierenden Vorgaben eine anspruchsvolle Aufgabe sei: „*compliance with security laws, regulations, policies and standards is a task beyond the powers of mere mortals, all right, maybe not impossible, but certainly very difficult*“. Diese holistische Sicht über die Compliance ergibt sich einerseits aus der Tatsache, dass die Anzahl der gesetzlichen, vertraglichen und normativen Anforderungen groß ist, und andererseits daraus, dass diese Anforderungen sich ständig ändern; manche Quellen wie z. B. [33] sprechen sogar von einer „Überregulierung“.

Die Dynamik der regulatorischen Vorgaben, welche zu einer Situation der Unübersichtlichkeit führen [79], ist eine Konsequenz der dynamischen Natur der Gesellschaft und ihrer Bedürfnisse. Die Globalisierung, die industrielle Entwicklung und der technische Fortschritt führen nicht nur dazu, dass neue Gesetze erlassen werden, sondern auch zur Anpassung alter Gesetze an neue Bedingungen. Mit der *SOX* begann eine Welle von *SOX*-ähnlichen Gesetzen, z. B. in Kanada (*Bill C198*), in Japan (*J-SOX*) oder in Europa (*Euro-SOX*), welche das Ziel hatten, das Vertrauen der Kunden und der Investoren in die Kreditinstitute

D e u t s c h l a n d	Gesetzliche / Behördliche Anforderungen				Selbstregulierung		Sektorspezifische Anforderungen		
	Steuerrecht	Datenschutz	Anleger-schutz	Sonstige Gesetze und Verordnungen	Experten	Industrie	Finanzdienst-leister	Medizin	u.w.m.
	- UStG / SigG, SigV - AO BaFin: - GDPdU - GOB - GoBS	- BDSG - TMG - TKG - UrnG (GoBS/ GDPdU) - ZKDSG	- HGB - KonTraG - AktG - UMAG - IFRS	- BetrVG - BildSch - ArbVO - UWG - SGB - SRVwV - BGB - VwVfG - StGB - ElektroG	- IDW FAIT - BSI - AWV	- ITIL - HBVI - ISO	BaFin: - RS 11/2001 Outsourcing - RS 18/2005 MaRisk - KWG - WpHG Umsetzung Basel-II	- MPG - HIPAA	- PCI DSS - AIS - CISP - SDP
I n t e r n a t.		EU-Richtlinie Vorratsdaten- speicherung	- Gramm- Leach- Bliley Act (GLBA)	- IASB - IAS - IFRS - IFRIC - SOX - EU-Anti Terror-VC - US Patriot Act - Security Breach Information Act		- COSO - CobiT	- Basel II - Solvency II - Banken-RiLi - Kapital- adäquanz-RiLi - FISMA - GLBA		

Abbildung 2.1: Regulatorische Anforderungen im Jahr 2007 [66].

wieder aufzubauen. Der Beitritt eines Staates zur Europäischen Union z. B., setzt die Umgestaltung des nationalen Rechtes voraus, damit dieses mit dem Unionsrecht konvergiert.

Compliance bedeutet, nicht nur alle für ein Unternehmen relevante Gesetze, sondern auch die Änderungen, die unter Umständen an solchen Gesetzen durchgeführt werden, zu kennen und zu beachten. Der pessimistische Compliance Officer aus [68] ist der Meinung, dass eine Datenbank, welche alle existierenden Compliance Anforderungen enthalten würde, „*is probably out of date the moment it is populated*“.

Im Folgenden werden als Beispiel einige relevante regulatorische Vorgaben erwähnt (nach [9]):

- Der *Sarbanes-Oxley Act*⁴ (*SOX*) regelt die Verantwortlichkeiten der Unternehmensführung und der Wirtschaftsprüfer neu und definiert Regeln für die Zusammenarbeit zwischen Wirtschaftsprüfern und Unternehmensleitung. Die Unternehmen müssen nachweisen, dass sie ein funktionsfähiges internes Kontrollsystem haben. Der Vorstand haftet für die Richtigkeit der Jahresabschlüsse. Die Sektion 404 aus *SOX* ist für die IT-Security relevant, weil in diesem Abschnitt die Ordnungsmäßigkeit der Verarbeitung und die Integrität der verarbeiteten Finanzdaten verlangt wird. Der Zugriff auf die Finanzdaten muss jederzeit möglich sein und eine Missbrauchserkennung muss ermöglicht werden. Ähnliche Ziele hat die *8.EU-Richtlinie*, welche als *Euro-SOX* bekannt ist.

⁴<http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR>: (abgerufen am 08.05.2011)

- Das *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich*⁵ (*KonTraG*) hat als Ziel, eine wirtschaftliche Kontrolle und Transparenz durch die Einrichtung eines Frühwarnsystems für die Früherkennung gefährdender Entwicklungen zu sichern; dieses Ziel wird durch die Verpflichtung der Geschäftsführung erreicht, ein unternehmensweites Risikomanagement zu implementieren. Der Vorstand, der Aufsichtsrat und der Geschäftsführer haften bei Verstößen persönlich.
- *Die neue Baseler Eigenkapitalvereinbarung*, als *Basel II* bekannt, richtet sich an Kreditunternehmen und basiert auf drei Säulen: die erste Säule repräsentiert den minimalen, notwendigen Eigenkapitaleinsatz, unter der Berücksichtigung des tatsächlichen Risikos für die Banken; die zweite Säule behandelt die bankenaufsichtlichen Überführungsprozesse, und die dritte Säule hat als Schwerpunkt die Transparenz der Bilanzen für die Öffentlichkeit.
- *Das Bundesdatenschutzgesetz*⁶ (*BDSG*) regelt die Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich, so dass der Umgang mit personenbezogenen Daten das Persönlichkeitsrecht von einzelnen Personen nicht beeinträchtigt. Dafür werden in diesem Gesetz die Zulässigkeit, die Kontrollrechte und die Sanktionen beim Umgang mit personenbezogenen Daten, sowie die Rechten der Betroffenen geregelt.
- Das *Gesetz über die Beaufsichtigung der Versicherungsunternehmen (VAG)*⁷ ist die zentrale bundesrechtliche Vorschrift für Versicherungsunternehmen und wurde durch die Bundesanstalt für Finanzdienstleistungsaufsicht erlassen. Es kontrolliert die Versicherungsunternehmen, so dass die Versicherer das Vertrauen, das die Kunden in sie setzen, rechtfertigen [25]. §64 VAG stellt Anforderungen an das Risikomanagement, an die Geschäftsorganisation, an die Risikostrategie und an ein internes Steuerungs- und Kontrollsystem in dem Versicherungsunternehmen.
- Das *Handelsgesetzbuch (HGB)*⁸ regelt den Handelsverkehr in Deutschland und enthält die Rechte der Kaufleute in Wirtschaftsbeziehungen.
- Die *Finanzkonglomeratrichtlinie (Richtlinie 2002/87/EG)*⁹ gilt seit dem 01.01.2005 und gibt Vorschriften für die Beaufsichtigung von Finanzkonglomeraten und Großkonzernen, die für die Stabilität des Finanzsystems von großer Bedeutung sind. Durch diese Vorschriften ist eine gruppenweite Aufsicht von Finanzkonglomeraten vorgesehen. Die Richtlinie hat folgende Ziele: die Beurteilung der Risiken der Solvabilität,

⁵<http://beck-online.beck.de/default.aspx?typ=reference&y=100&g=KonTraG>
(abgerufen am 08.05.2011)

⁶http://www.gesetze-im-internet.de/bdsg_1990/, abgerufen am 08.05.2011

⁷<http://www.gesetze-im-internet.de/vag/> (abgerufen am 25.04.2011)

⁸<http://www.gesetze.juris.de/hgb/> (abgerufen am 25.04.2011)

⁹<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:035:0001:0001:DE:PDF> (abgerufen am 26.04.2011)

der Risikokonzentration, der gruppeninternen Transaktionen sowie des internen Risikomanagements zu verbessern und die Doppelbelegung von Eigenkapital und der gruppeninternen Schöpfung von Eigenkapital innerhalb der Kreditinstitute zu vermeiden.

2.1.2 Die handlungsorientierte Dimension der Compliance

Compliance verpflichtet zum Aufbau einer Compliance Organisation. Um die Compliance Anforderungen erfüllen zu können, muss in den meisten Fällen eine Organisation ihre Geschäftsprozesse auf einer Art (um)gestalten, dass diese Geschäftsprozesse „compliant“ durchgeführt werden können. Das heißt, die Aufbau- und die Ablauforganisation, sowie die Prozesssteuerung müssen so konzipiert werden, damit sie die Einhaltung der Compliance nicht behindern, sondern vereinfachen. Die Compliance-Organisation stellt durch Überwachung, Beratung und Berichterstattung die Einhaltung der Regelungen und gesetzlichen Vorschriften sicher. Die Einrichtung einer Compliance Organisation gehört zu den Pflichten des Vorstands und die Umsetzung der Compliance-Maßnahmen fällt in dem Verantwortungsbereich der Geschäftsführung.

Da die Anforderungen an jede Organisation variieren, wird das Thema Compliance unterschiedlich angegangen. Eine strukturierte Annäherung zum Aufbau einer Compliance Organisation besteht aus:

- Einem funktionierenden Risikomanagement,
- Der Bereitstellung eines internen Informationssystems,
- Der Bereitstellung eines externen Kommunikationssystems,
- Der Einführung eines internen Kontrollsystems.

Die Komponenten der Compliance-Organisation erlauben die Veranlassung von präventiven und reaktiven Maßnahmen für den Fall der rechtlichen und vertraglichen Verletzungen. Diese Verletzungen werden als Risiken betrachtet und im Rahmen des Risikomanagements der Organisation behandelt. Wie bei [21] nachzulesen ist, ist ein Risiko die Wahrscheinlichkeit oder relative Häufigkeit des Eintritts eines Schadensereignisses, und die Höhe des potentiellen Schadens, der dadurch hervorgerufen werden kann.

Eine verantwortungsvolle Unternehmensführung, ein richtig konzipiertes Risikomanagement und eine konsistente Erfüllung der Compliance-Anforderungen werden heutzutage als ein Ganzes betrachtet und sind unter dem Namen Governance-Risiko-Compliance-Management (GRC-Management) bekannt. Dabei stellt die Governance das Führungssystem zur Leitung und Überwachung eines Unternehmens dar [33]. Das Risikomanagement

hat die Aufgabe, alle relevanten Risiken innerhalb der Organisation zu identifizieren und zu bewerten. Dieses Modell erfordert sowohl aufeinander abgestimmte GRC-Strategien, als auch das gemeinsame Management dieser Strategien. Ein integriertes GRC-Management wird z.B im *Deutschen Corporate Governance-Kodex* als Strategie in der Unternehmensführung vorgeschlagen. Der Vorstand des Unternehmens ist für die Umsetzung dieser Strategie verantwortlich [67]:

„4.1.2 Der Vorstand entwickelt die strategische Ausrichtung des Unternehmens, stimmt sie mit dem Aufsichtsrat ab und sorgt für ihre Umsetzung.

4.1.3 Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).

4.1.4 Der Vorstand sorgt für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen.“

Die Arbeiten in dem GRC-Bereich sollen auf einer gemeinsamen Basis effizient organisatorisch zusammengefasst werden, indem z. B. die Governance vorsieht, dass die potentiellen Compliance-Verstöße als Risiken im Rahmen des Risikomanagements des Unternehmens betrachtet werden [79]. Die enge Beziehung zwischen Governance, Risiko und Compliance wird in der Abbildung 2.2 schematisch dargestellt. Der Zusammenhang zwischen Com-

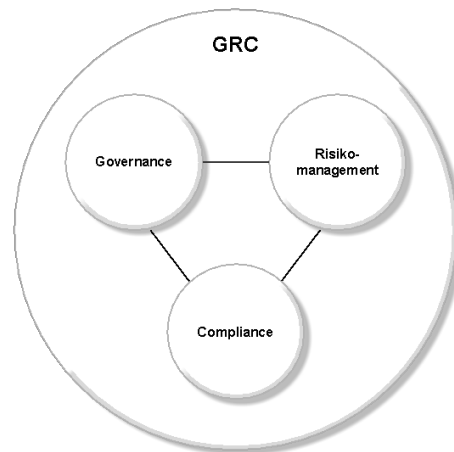


Abbildung 2.2: Die GRC-Trias (vgl. [33]).

pliance, Corporate Governance und Risikomanagement wird auch von den fünf Funktionen der Compliance in einem Unternehmen bestätigt, wie diese aus [54] bekannt sind:

1. Die *Schutzfunktion* dient der Sicherung des Vertrauens und der Reputation und ist Voraussetzung für das Verknüpfen und Pflegen von Geschäftsbeziehungen. Die Einhaltung der Compliance stellt einen Schutz für Geschäftspartner, Mitarbeiter und für die Organisation selbst dar.

2. Die *Beratungs- und Informationsfunktion* ist bei der Einführung und Durchführung von Compliance wichtig, weil Missverständnisse verhindert werden sollen. Daher werden Compliance-Abteilungen eingerichtet, welche die Aufgabe haben, sowohl Zweifelsfragen zu klären, als auch ein Bewusstsein der Mitarbeiter für Compliance zu schaffen. Compliance ist kein Zustand, sondern ein kontinuierliches Prozess, der nur erfolgreich durchgeführt wird, wenn die Mitarbeiter die Einhaltung der Compliance nicht als Behinderung ihrer Arbeit betrachten. Dieser handlungsorientierte Aspekt wird in [60] beschrieben:

„Compliance umfasst die Aufgabe und die Funktion, in einem Unternehmen die Voraussetzungen und das Bewusstsein zu schaffen, dass alle Mitarbeitenden sämtliche für das Unternehmen relevante Bestimmungen selbstständig einhalten und einhalten können. Zudem ist Compliance für die Kontrolle und die Einhaltung der relevanten Bestimmungen besorgt.“

3. Die *Qualitätssicherungs- und Innovationsfunktion* der Compliance schützt eine Organisation und ihre Geschäftspartnern von bewusstem und unbewusstem Missbrauch. Ein Finanzinstitut z. B. muss einerseits seine Kunden über die Art und die Risiken der angebotenen Leistungen informieren, andererseits muss sich das Finanzinstitut selbst über die Kunden informieren, indem dieser Informationen über die Kunden einholt.
4. Die *Monitoring- oder Überwachungsfunktion*: in diesem Fall stehen die Beachtung und die Einhaltung aller Compliance Anforderungen im Mittelpunkt. Monitoring-Systeme überwachen die Durchführung der Compliance in Organisationen und reagieren bei einem Verstoß.
5. Die *Marketing-Funktion* trägt zur Vermeidung der Compliance-Verstöße und zur Behaltung der Reputation der Organisation bei. Auf diese Weise wird das Vertrauen einerseits zwischen der Organisation und den Geschäftspartner und andererseits zwischen der Organisation und den Mitarbeitern aufbewahrt und gestärkt.

Durch die Schaffung eines Bewusstseins für die Compliance und durch die Überwachung der Compliance-Durchführung und -Einhaltung werden Risiken minimiert, der Produktivitätsgrad und die Effizienz steigen und die Wettbewerbsfähigkeit der Organisation erhöht sich.

2.1.3 Die nachweisorientierte Dimension der Compliance

Compliance bedeutet, in jedem Moment die Einhaltung der Compliance Anforderungen nachweisen zu können. Auch wenn das Wort *Compliance* bis vor einigen Jahren noch kein Modewort [33] war, waren sowohl die Einhaltung der oben genannten Anforderungen

(Gesetze, Verträge, externe und interne Vorgaben), als auch die optimale Gestaltung der Unternehmensstruktur für eine effiziente Erfüllung dieser Anforderungen selbstverständlich. Der neue Aspekt, welchen der Begriff *Compliance* mit sich bringt, ist die Pflicht, diese Einhaltung der Vorgaben nachweisen zu können. Eine Organisation handelt compliant mit den gesetzlichen Vorgaben, wenn sie dies auch belegen kann. Die Entscheidungen, Prozesse und Maßnahmen müssen ausreichend in Schriftform dokumentiert werden und auf Nachfrage vorgezeigt werden. Um diesen Herausforderungen nachkommen zu können, werden zunehmend Ressourcen der IT benutzt. Auf diesen Aspekt wird im folgenden Abschnitt näher eingegangen.

2.2 Compliance und IT

Die IT ist heutzutage in den meisten Organisationen ein unverzichtbarer Teil der Geschäftstätigkeit. Einige brauchen nur Internetdienste zu nutzen oder Daten zu speichern, andere setzen die IT in komplexe Produktionsmittel ein. Laut einer Studie¹⁰ zur IT-Nutzung in Unternehmen, durchgeführt von der internationalen Wirtschaftsberatung Deloitte im Jahr 2009, *IT Business Balance Survey 2009*, gewinnt die IT sowohl im Anwendungsbereich, als auch strategisch im Hinblick auf die Unternehmensführung und -entwicklung an Bedeutung [19]. Die Erwartungen der Unternehmen beim Einsatz von IT sind unterschiedlich: bessere Produkte oder Dienstleistungen, Automatisierung und schnellere Ausführung der Geschäftsprozesse, höhere Kundenzufriedenheit, Kosteneinsparung, go-to-market-Vorteile, Umsatzsteigerung, Profitwachstum. Die Abbildung 2.3 zeigt in welchem Maß die IT bei der Erfüllung der oben genannten Ziele bis 2012 beitragen wird, nach Ansicht der IT-Manager bzw. der Geschäftsleiter.

Die Ausdehnung der IT auf viele Unternehmensbereiche und die dadurch entstandene Abhängigkeit der Unternehmen von dieser Technologie haben zu einer „IT-GRC-Trias“ [33] geführt, welche innerhalb der Corporate GRC-Trias integriert werden muss. Nach der Ansicht des IT Governance Institute, besteht die IT-Governance aus „Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die IT die Unternehmensstrategie und -ziele unterstützt“ und liegt in der Verantwortung des Vorstands und des Managements [28].

2.2.1 IT-gestützte Compliance

Die Unternehmensstrategie wird im Einklang mit den im Abschnitt 2.1.1 genannten Compliance Anforderungen erstellt. Durch ihre Rolle, den Geschäftsbetrieb zu unterstützen,

¹⁰Befragt wurden 549 IT-Manager, Unternehmens- bzw. Geschäftsbereichsleitungen aus 28 Ländern. Die Fragen standen im Bezug zu IT-Management, -Entwicklungen und Trends im IT-Management, IT-Outsourcing und Security, Privacy und Fraud Herausforderungen

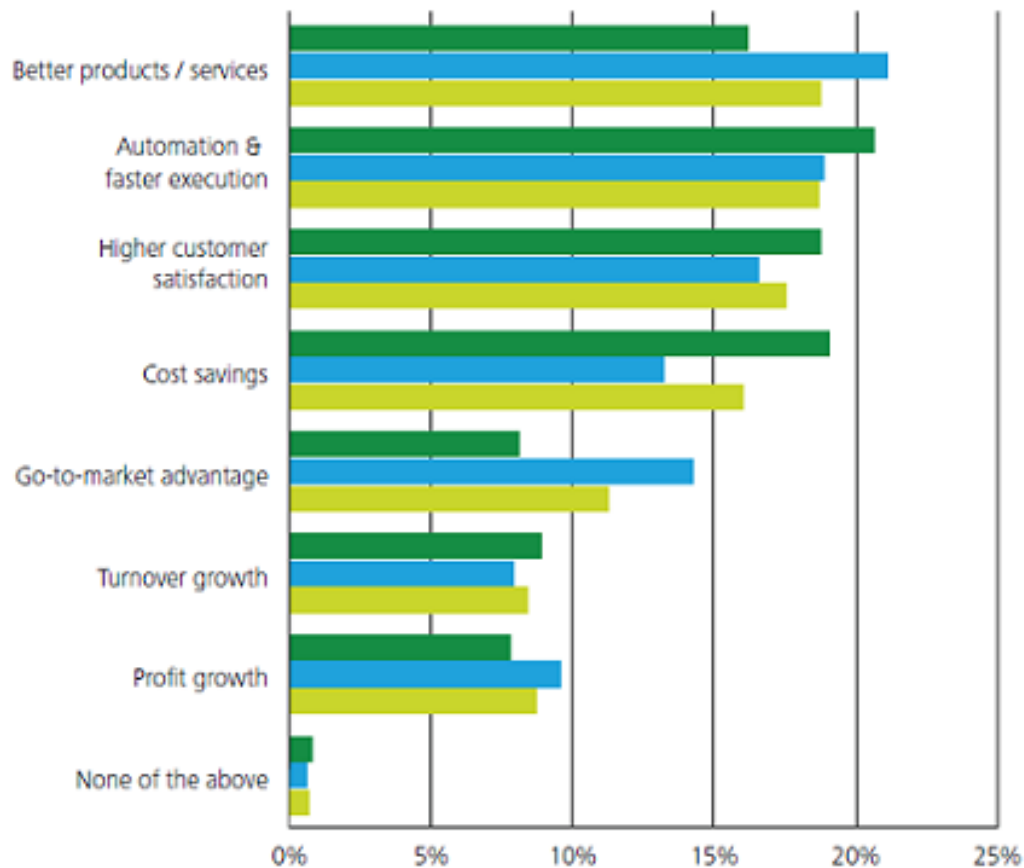


Abbildung 2.3: Rolle der IT in Unternehmen nach einer Deloitte-Studie aus 2009 [19].

wird die IT als Mittel für die Umsetzung von Compliance benutzt. Wegen der großen Anzahl der Compliance Anforderungen ist eine manuelle Verwaltung der Compliance teuer, arbeitsintensiv und fehleranfällig. Eine Automatisierung der Compliance-Aktivitäten reduziert die Kosten der Compliance-Verwaltung. Die Kontrollen können effizienter erreicht werden und eine schnelle Reaktion auf Anfragen zum Nachweis der Compliance ist möglich [33]. Der Einsatz von Soft- und Hardwareprodukten, mit deren Hilfe die Einhaltung von Regelwerken sichergestellt werden kann, kennt die Fachliteratur [33, 79] unter dem Namen *IT-gestützte Compliance*.

Heutzutage werden auf dem Markt unterschiedliche Lösungen für Security, Lifecycle- und Content Management, Archivierung, Verschlüsselung, Nutzer-, Zugangs- oder Lizenzverwaltung angeboten. Diese Lösungen werden gerne von den verschiedenen Organisationen gesehen, weil deren Einsatz das Bemühen um Compliance beweist. Andererseits lassen sich ohne solche Lösungen die Compliance-Risiken nicht kontrollieren. *ARIS Solution for Governance, Risk&Compliance Management, SAP Businessobjects GRC-Lösungen, IBM® Tivoli® Security Compliance Manager* oder *Microsoft Security Compliance Manager* sind nur einige Beispiele für Compliance Management Tools.

2.2.2 IT-Compliance

Als integrierter Teil einer Organisation wird die IT selbst zum Träger der Compliance. Es gibt rechtliche Vorgaben, aus denen sich ein Handlungsbedarf für die IT in verschiedenen Organisationen ergibt. In diesem Fall spricht man von *IT-Compliance*. Die Quellen der IT-Compliance sind unterschiedlich. Einige Gesetze beziehen sich vom Namen her auf die IT: das *Bundesdatenschutzgesetz (BDSG)*, das *Signaturgesetz (SigG)* oder das *Telemediengesetz (TMG)*. Weitere Gesetze regeln den IT-Einsatz in verschiedenen Bereichen, z. B. das *Betriebsverfassungsgesetz (BetrVG)*, das *Strafbuchgesetz (StBG)*, *Basel II* und die *8. EU-Richtlinie* (auch als *Euro-SOX* bekannt). Es gibt auch Regelwerke, die von den zuständigen Behörden zur Interpretation und Ausführung der Rechtsnormen aufgestellt werden und für die IT-Compliance relevant sind. Beispiele hierfür sind die *Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)* oder die *Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)*. Verwaltungen oder privatrechtliche Institutionen (z. B. dem DIN-Deutsches Institut für Normung) geben Regelwerke heraus, die Compliance Anforderungen an die IT stellen. Nicht zuletzt müssen die Verträge mit Geschäftspartnern betrachtet werden: solche Verträge können auch Anforderungen an die IT enthalten, z. B. Anforderungen an den Datenschutz oder bestimmte *Qualities of Service (QoS)*.

2.2.3 Compliance und IT-Security

Die IT-gestützte Compliance und die IT-Compliance befinden sich in einer wechselseitigen Beziehung, so wie in der Abbildung 2.4 dargestellt wird.

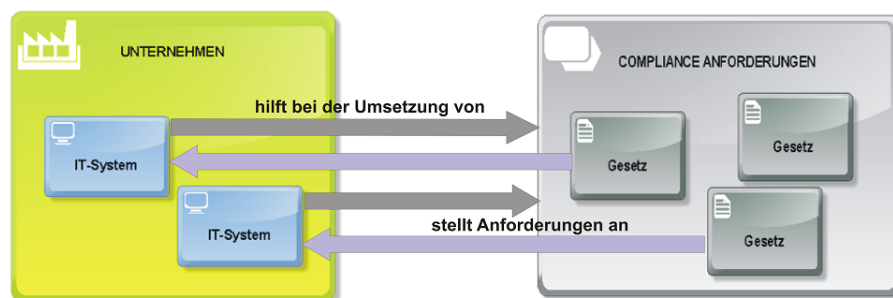


Abbildung 2.4: Wechselbeziehung zwischen IT und Compliance.

Diese beiden Arten von Compliance beeinflussen nach [55] die IT-Strategie, die IT-Organisation und die IT-Ressourcen. Die IT unterstützt die Unternehmensstrategie durch Geschäftsprozessmodellierung: dabei werden Geschäftsprozesse erfasst, gestaltet, ausgeführt, dokumentiert, gemessen, überwacht und gesteuert [26]. Die Automatisierung der Geschäftsprozesse mit Hilfe der IT wirkt bei der Gestaltung des Überwachungs- und Kontrollsystems mit und erlaubt die Nachvollziehbarkeit der Compliance-Aktivitäten durch Datensicherung

und Archivierung.

Der Umgang mit Informationen und Daten führt zur Notwendigkeit einer IT-Infrastruktur, welche den Schutz dieser Daten und Informationen anbieten kann. In der Literatur über (Informations-)Sicherheit ist der Schutz eines IT-Systems unter dem Namen *IT-Sicherheit* oder *IT-Security* bekannt.

IT-Sicherheit oder IT-Security? Das Wort *Sicherheit* ist die deutsche Übersetzung für zwei englische Begriffe: *Safety* und *Security*. Die Nutzung dieser Begriffe im Zusammenhang mit der IT bedarf einer Erklärung, weil in der Literatur keine einheitliche Begriffsbildung verwendet wird. Um sie zu definieren, orientiert sich diese Diplomarbeit an dem Buch *IT-Sicherheit. Konzepte-Verfahren-Protokolle* von C. Eckert [21].

Unter Sicherheit als *Safety* wird die Funktionssicherheit eines Systems verstanden. Ein System ist *safe*, wenn die Ist-Funktionalität und die Soll-Funktionalität übereinstimmen. Eng verwandt mit der Funktionssicherheit sind die Begriffe *Zuverlässigkeit* (engl. *reliability*) und *Verlässlichkeit* (engl. *dependability*). Ein System ist verlässlich, wenn es keine unzulässigen Zustände annimmt. Zuverlässigkeit charakterisiert ein System, das eine spezifizierte Funktion unter den vorgesehenen Bedingungen erbringt.

Safety, also Funktionssicherheit, Verlässlichkeit und Zuverlässigkeit, ist die Grundlage für die Informationssicherheit und die Datensicherheit. Der Begriff *Informationssicherheit*, Übersetzung des englischen *Security*, ist die Eigenschaft eines funktionssicheren Systems, nur solche Zustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen [21].

Die *Datensicherheit* (engl. *protection*) ist die Eigenschaft eines funktionssicheren Systems, nur solche Zustände anzunehmen, die zu keinem unautorisierten Zugriff auf Daten führen. Eng verwandt mit *Datensicherheit* ist der Begriff *Datenschutz* (engl. *privacy*), der im rechtlichen Sinne verwendet wird und den fairen Umgang mit personenbezogenen Daten regelt.

In dieser Diplomarbeit wird der englische Begriff *IT-Security* mit der Bedeutung *Informationssicherheit* verwendet.

Schutzziele der IT-Security Informationen und Daten sind wichtige Güter innerhalb der Organisationen, und daher müssen sie aufbewahrt und geschützt werden. Die Anzahl der so genannten *IT-Security-Schutzziele* unterscheidet sich von Autor zu Autor. Der Bereich dieser Schutzziele überschneidet sich in manchen Fällen und diese unscharfen Grenzen

führen zu der Schwierigkeit, die Begriffe voneinander abzugrenzen.

Gemäß den *BSI-IT-Grundschatz-Katalogen* gibt es drei Schutzziele für die IT-Security: die *Verfügbarkeit*, die *Vertraulichkeit* und die *Integrität* der Information [39]. In der zitierten Arbeit von Eckert [21] oder bei Biskup [8] werden fünf Schutzziele der IT-Security genannt:

- Die *Vertraulichkeit* bedeutet Schutz vor unautorisierter Informationsgewinnung.
- Die *Datenintegrität* bedeutet Schutz der Information gegenüber unautorisierten und unbemerkten Veränderungen.
- Die *Verfügbarkeit* ist erfüllt, wenn Ressourcen und Dienste den legitimen Benutzern zur Verfügung stehen.
- Die *Authentizität* bedeutet die Echtheit und Glaubwürdigkeit eines Teilnehmers, der eindeutig identifiziert und überprüft werden kann.
- Die *Verbindlichkeit* oder die *Nichtabstreitbarkeit* ist die Möglichkeit, den Inhalt und den Absender von Information gegenüber einem an der Kommunikation nicht beteiligten Dritten zu beweisen.

In [44] werden noch zwei IT-Security-Schutzziele genannt:

- Die *Authentifikation* oder *Authentifizierung*: dabei muss ein Kommunikationspartner eindeutig identifiziert werden können.
- Die *Autorisation*: dadurch wird der Zugriff auf ein Datum oder eine Ressource nur auf diejenigen Benutzer beschränkt, die das Recht haben, auf diese Ressource oder dieses Datum zuzugreifen.

Bedrohungen und Gefahren für die IT-Security-Schutzziele Ein IT-System mit den darin gespeicherten Daten und Informationen kann verschiedene Schwachstellen besitzen und ist anfällig für unterschiedliche Bedrohungen und Gefahren. Diese können sowohl von außen als auch von innerhalb der Organisation kommen und entstehen zufällig oder absichtlich, aus Versehen oder mit Vorsatz. Solche Bedrohungen und Gefahren für die IT sind nach den BSI-IT-Grundschatz-Katalogen [39]:

- *Menschliches Versagen*: auch wenn ein IT-System *safe* funktioniert und *secure* konfiguriert ist, wird es nicht geschützt, wenn sich diejenigen, die das System nutzen, fehlerhaft verhalten. Organisatorische Mängel wie unberechtigter Zugriff, Anfertigung von Raubkopien oder ungeschultes Personal sind auch in dieser Kategorie enthalten.

- *Technisches Versagen* findet statt, wenn eine Komponente der IT-Infrastruktur sich in einem Zustand befindet, in dem sie ihren Zweck nicht mehr erfüllen kann. Beispiele dafür sind: Unterbrechung oder Schwankung der Stromversorgung, defekte Datenträger, Ausfall von Netzwerkkomponenten oder einer Datenbank, Ausfall von Sicherungseinrichtungen, usw.
- *Höhere Gewalt*: hier zählen Blitzeinschlag, Feuer, Hochwasser, Überschwemmungen oder Stromausfall, aber auch Personalausfall.
- *Betrug und Diebstahl*: IT-Geräte und Software sind Wertgegenstände einer Organisation und Ziel von Diebstählen; Daten können auch modifiziert oder kopiert werden.
- *Sabotage, Manipulation* bedeuten das absichtliche Verursachen von Schaden durch Zerstörung von Hardware, Einbauen von einem fehlerhaften Code in die erstellte Software, Eingabe von falschen Daten oder Löschen und Verändern der Daten. Solche Handlungen können auch aus Rache durch Mitarbeiter, die bereits das Vertrauen des anzugreifenden Systems genießen, durchgeführt werden.
- *Personen oder Gruppen mit böswilligen Interessen* werden durch Hacker, Cracker, Skript-Kiddies, oder Kriminelle repräsentiert. Hacker sind Angreifer, die sich sehr gut technisch auskennen und mit den Grenzen des Systems experimentieren [75]. Ihr Ziel ist, Schwachstellen und Verwundbarkeiten im System zu entdecken und sich damit an die Öffentlichkeit zu wenden. Sie verfolgen meist keine finanziellen Ziele; es wird heutzutage sogar von einer Hacker-Ethik¹¹ gesprochen. Die Cracker unterscheiden sich von den Hackern dadurch, dass sie Angriffe zum eigenen Vorteil oder zum Vorteil der Anderen durchführen. Die *Script Kiddies* haben kein technisches Wissen wie die ersten zwei Kategorien von Angreifern, verursachen aber Schaden durch die Verwendung (aus Neugier und Spieltrieb) von fertig erstellten und frei verfügbaren Exploits¹². Es gibt auch zunehmend eine so genannte *Internetkriminalität*. Dadurch werden Angriffe auf IT-Systeme von Regierungen oder von verschiedenen Firmen aus dem Finanzsektor durchgeführt und finanzieller Gewinn erzielt. Die Industriespionage besteht aus Lauschangriffen auf Datenleitungen oder Datenverkehrsanalyse mit dem Ziel, Wirtschaftsgeheimnisse zu stehlen oder einen Wettbewerbsvorteil zu gewinnen.

¹¹„An Ethical Hacker is a person employed and trusted by an organization to penetrate the network and computer systems using the same methods as a hacker. Similar to a penetration tester, the goal of the ethical hacker is to assist the organization in taking preemptive measures against malicious attacks by hacking the system“ [57].

¹²Ein Exploit ist eine Angriffsart auf IT-Systeme, in welcher aufgedeckte Verwundbarkeiten und Schwachstellen ausgenutzt werden [21].

IT-Risikomanagement Die IT-Governance setzt die Einrichtung eines IT-Risikomanagements voraus. Innerhalb des Risikomanagements der Organisation werden die beschriebenen Gefährdungen der IT-Security-Schutzziele als IT-Risiken behandelt. Diese IT-Risiken werden systematisch identifiziert, analysiert und bewertet. Abhängig von den Ergebnissen dieser Aktionen werden durch geeignete Maßnahmen die Korrektur, Reduzierung und Vermeidung von Bedrohungen und Schäden an den IT-Systemen gesteuert.

Diese Maßnahmen, welche im Einklang mit der Geschäftsstrategie das Ziel haben, die IT-Systeme und die dazugehörigen Werte zu schützen, werden unter dem Namen *Sicherheitsrichtlinien* oder *IT-Security-Policies* bekannt, und werden im nächsten Abschnitt beschrieben.

2.3 IT-Security-Policies

Definition einer IT-Security-Policy Ins Deutsche wird der englische Begriff *IT-Security Policy* durch *Sicherheitsrichtlinie* oder *Sicherheitspolitik* übersetzt; dabei wird die Übersetzung *Sicherheitspolitik* in [39] als „falsch“ eingestuft. Um Uneindeutigkeiten bezüglich der Übersetzung zu verhindern, wird in dieser Arbeit der englische Begriff bevorzugt.

Auch die Bedeutung des Begriffes *IT-Security-Policy* wird in der Literatur aus zwei Richtungen betrachtet. Die einen sehen darin „eine Menge von technischen und Organisatorischen Regeln, Verhaltensrichtlinien, Verantwortlichkeiten und Rollen und Maßnahmen, um die angestrebten Schutzziele zu erreichen“ [21] oder die Formulierung der „Schutzziele und allgemeine[r] Sicherheitsmaßnahmen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde“ [39]. In der RFC 2828 [77] wird eine Security Policy definiert als „*A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources*“. In diesem Sinne wird auch in der vorliegenden Diplomarbeit der Begriff verwendet. Andere [45] begrenzen den Bereich einer *IT-Security-Policy* nur auf ein „zentrales Werkzeug [...] um die derzeit überwiegend manuell durchgeführten Aufgaben maschinell zu erledigen“.

Entwicklung einer IT-Security-Policy Der Definitionsprozess der IT-Security-Policies fängt mit der Festlegung der allgemeinen Geschäftsstrategie durch die Unternehmensführung an (Governance). Diese beeinflusst/diktiert eine bestimmte IT-Strategie in der Organisation; die IT-Strategie entscheidet, abhängig von den erzielten Ergebnissen, von den zu erfüllenden regulatorischen Vorgaben, von den Verträgen oder Vereinbarungen mit Geschäftspartnern und auch von der Unternehmenskultur, welchen Einsatz, Funktionalität und Nutzung die verschiedenen IT-Ressourcen haben und welchen Wert die Daten und Informationen haben. Mit der Betrachtung aller diesen Faktoren wird eine Corporate IT-

Security-Policy erstellt.

Der nächste Schritt findet abhängig von den Ergebnissen des Risikomanagements statt. Eine Risikoanalyse legt fest, welches Schutzbedarf für die IT-Systeme zu gewährleisten ist. Abhängig vom Schutzziel und vom Schutzbedarf werden organisatorische, administrative und technische Schutzmaßnahmen festgelegt. Komplementär zu diesem *top-down*-Ansatz, der den Schutzbedarf der IT-Systeme betrachtet und zu den IT-Security-Policies führt, wird auch ein *bottom-up*-Definitionsverfahren der IT-Security-Policies durchgeführt: dabei wird berücksichtigt, welche Ressourcen in der Organisation tatsächlich für die Erfüllung der festgelegten Anforderungen zur Verfügung stehen: qualifiziertes Personal, technische Ausstattung oder Budget [82].

Die festgelegten IT-Security-Policies bauen auf der Corporate IT-Security-Policy auf und spezifizieren verbindlich sowohl das Verhalten von IT-Systemen und Nutzern, als auch die Maßnahmen für den Fall, dass die IT-Security der Organisation gefährdet ist. Beispiele solcher IT-Security-Policies werden in der Tabelle 2.2 aufgelistet, allerdings wird keine konkrete Angabe gemacht, wie diese Aktionen durchzuführen sind. Diese IT-Security-Policies haben informellen Charakter und werden in natürlicher Sprache verfasst. In der Literatur sind sie unter den Namen *high-level-Policies* [52, 82] oder *strategische Policies* [18] bekannt. Die Tabelle 2.1 enthält ein Beispiel für eine *high-level*-IT-Security-Policy:

Ein Passwort darf keine Wörterbuch-Einträge enthalten.
Ein Passwort muss mindestens 2 Ziffern und einen Grossbuchstaben enthalten.
Alle Passwörter müssen alle drei Monate geändert werden.

Tabelle 2.1: Beispiel einer *high-level*-IT-Security-Policy für Passwörter.

In einem inkrementellen Verfahren werden die IT-Security-Policies weiter verarbeitet und verfeinert. In dieser Phase wird genau festgelegt, welcher Informationsfluß in der Organisation stattfinden darf, wer auf welche Ressourcen und unter welchen Bedingungen zugreifen darf, und wie die verschiedenen Aktionen aus der Policy durchzuführen sind. Die Anzahl der *zielorientierten Policies* [18] nimmt mit dem Detailgrad zu. Die menschlichen Teilnehmer des IT-Systems müssen diese Policies kennen und anwenden.

Manuell durchgeführte Aufgaben verhindern die Steigerung der Effizienz in immer komplexer werdenden Systemen und sie erhöhen die Fehleranfälligkeit verschiedener Aktivitäten. Heutzutage ist die Automatisierung der Geschäftsprozesse Gegenstand der Forschung [36]. In diesen Bereich gehört auch das automatisierte Management der IT-Security-Policies, von der Definierung bis zur Durchsetzung und Auditierung. In der Literatur wird sogar von einem *policy-based Computing* [45] gesprochen, in welchem die Mensch-Maschine- und die

Security Policy	Inhalt
Corporate Security Policy	Unternehmensweit gültige Sicherheitsleitsätze
Acceptable Use Policy	Korrekte Benutzung von IT Equipment und Services
E-Mail Policy	Sichere Nutzung von E-Mail
Anti-Virus Policy	Vorgaben für alle Computer um Computerviren zu erkennen und vermeiden
Passwort Policy	Sichere Passwortwahl, Aufbewahrung und regelmäßige Änderung
VPN Security Policy	Vorraussetzungen für VPN Verbindungen
Remote Access Policy	Zugriffsarten auf das Intranet von extern
Backup Policy	Beschreibt Vorgaben für die Datensicherung
Wireless Network Policy	Vorgaben für Funknetzwerke und deren Benutzung
Laptop Security Policy	Laptop Sicherheit, Umgang mit Laptops
Server Security Policy	Sicherheitsanforderungen für Server im Unternehmen
Router Security Policy	Minimale Sicherheitsanforderungen für Router und Switches
Acceptable Encryption Policy	Anforderungen an die verwendeten Verschlüsselungsalgorithmen
Public Key Infrastructure Policy	Management von Schlüsseln bei asymmetrischen Verschlüsselungsverfahren

Tabelle 2.2: IT-Security-Policies [51].

Maschine-Maschine-Interaktion geregelt werden. Ein Teil der zielbasierten Policies aus der vorigen Stufe können weiter verfeinert werden, bis sie maschinell verarbeitet werden können. In diesem Fall spricht man von *low-level Policies* [52, 82] oder *operationalen Policies* [18]. Einfache Beispiele für den automatisierten Ablauf auf Basis von IT-Security-Policies ist die Funktionsweise der Netzwerk-Firewalls mit Filterlisten, welche vom System direkt interpretierbare Policies darstellen [52].

Damit die IT-Security-Policies automatisch interpretiert und durchgesetzt werden können, müssen sie in einer speziellen Syntax verfasst werden und ihre Semantik muss sich an einem Policy-Informationsmodell orientieren.

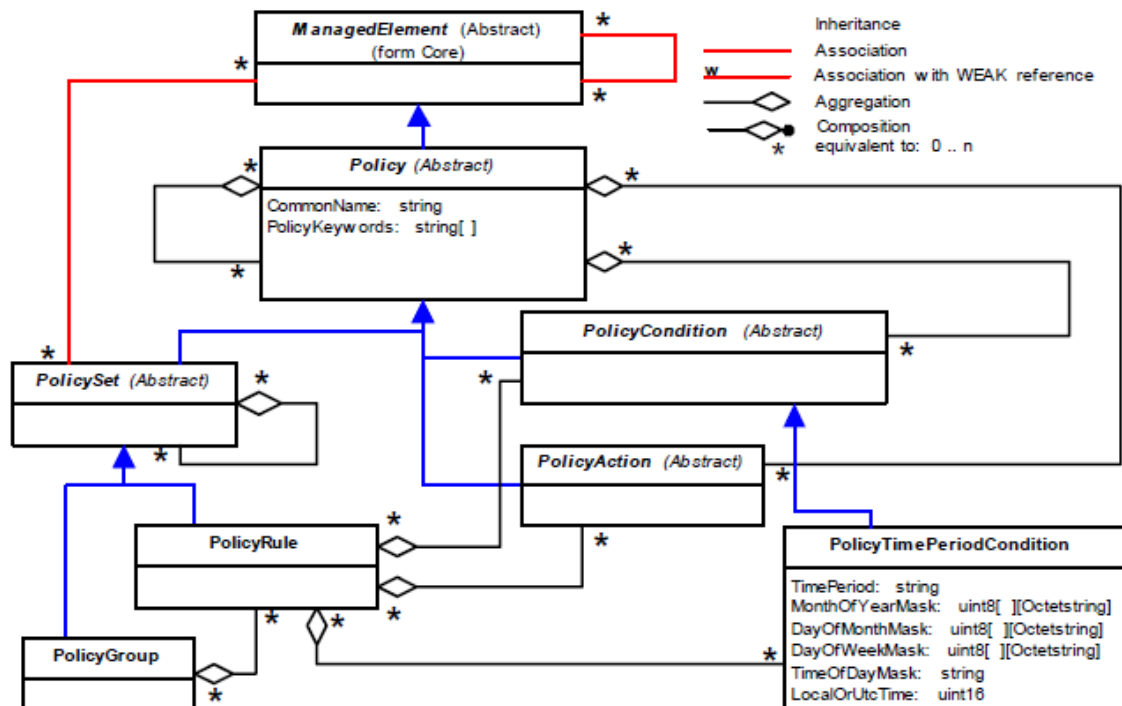


Abbildung 2.5: Klassen des CIM/PCIM von IETF [45].

2.3.1 Informationsmodelle für IT-Security Policies

Das *Common Information Modell (CIM)* von der *Distributed Management Task Force (DMTF)* ist ein allgemeines, objektorientiertes und erweiterbares Informationsmodell zur einheitlichen Spezifizierung von Systemen. Die Spezifizierung der Systemkomponenten und der Beziehungen zwischen den Komponenten wird in Unified Modelling Language (UML) gemacht. Einzelne Elemente dieses Modells wurden durch die *Internet Engineering Task Force (IETF)* spezialisiert und zur Spezifikation des *Policy Core Information Model* in der RFC 3460 [61] verwendet. Das objektorientierte Modell von PCIM bildet die semantische Grundlage für die Definition von Policies. Ein Auszug des IETF/DMTF Policy Modell nach [45] wird in der Abbildung 2.5 dargestellt. Eine Policy wird im Modell *PolicyRule* genannt und kann eine Menge von Bedingungen (*PolicyCondition*) und Aktionen (*PolicyAction*) enthalten. Eine Menge von Policies (*PolicyGroup*) kann mehrere Policies enthalten. Zeitliche Einschränkungen können mit Hilfe der Klasse *PolicyTimePeriodCondition* ausgedrückt werden. Ein Informationsmodell wie das CIM/PCIM kann durch Vererbung erweitert und an verschiedene Szenarien angepasst werden.

2.3.2 Policy-Sprachen

Das semantische Policy-Modell wird von mehreren formalen Policy-Sprachen umgesetzt, die sich in dem Anwendungsbereich, in der Ausdrucksmächtigkeit, in den Operationen auf

Policies (z. B. Kombination, Vergleichbarkeit) oder in formalen Resultaten wie Entscheidbarkeit unterscheiden. Einige Beispiele für Policy-Sprachen sind:

Ponder ist eine deklarative Sprache zur Spezifikation von Autorisierung, Delegation, Filterung und Unterlassung. Mit Hilfe der Autorisierungspolicies werden Rechte an Objekten vergeben. Diese Rechte sind positive Rechte (Erlaubnisse) oder negative Rechte (Verbote). Die Obligationspolicies spezifizieren die Aktionen, die von Subjekten auf Objekte (*targets*) durchgeführt werden müssen. Die Policies können auf einzelne Benutzer, Gruppen oder Rollen angewendet werden [56].

Rei ist eine „ausdrucksvolle und leichtgewichtige“ Policy-Sprache, welche positive und negative Erlaubnisse und Verbote für die Subjekte aus dem Policy-Bereich ausdrücken kann [43]. Besonders wird sie eingesetzt für die Spezifizierung und Durchsetzung von Security-Eigenschaften in dynamischen Systemen (pervasive Umgebungen¹³), in welchen die Security-Anforderungen abhängig von den adressierten Subjekten modifizierbar sind.

Platform for Enterprise Privacy Practices (E-P3P) [5], *Enterprise Privacy Authorisation Language (EPAL)* und *Extended Privacy Definition Tool (ExPDT)* [49] sind IT-Security-Policy-Sprachen, welche die Spezifizierung und Durchsetzung der Datenschutzinformationen innerhalb von Organisationen erlauben und den Zugriff auf Daten steuern.

eXtensible Access Control Markup Language (XACML) [53] ist eine XML-Erweiterung, welche die Zugriffssteuerung und -kontrolle auf zu schützende Objekte ausdrücken kann. *Obligation Specification Language (OSL)* [34] ist eine Policy Sprache, die zur Reglementierung der Benutzung von Ressourcen beiträgt. Benutzungskontrolle in diesem Sinne ist eine Spezialisierung der Zugriffskontrolle und legt fest, nicht nur wer auf Ressourcen zugreifen darf, sondern auch wie und für wie lange.

Die Spezifizierung der zielorientierten IT-Security-Policies mit Hilfe einer formalen Sprache ist der erste Schritt in die Richtung des automatisierten Policy-Managements. Nachdem die definierten Policies auf formale Korrektheit (Konsistenz, Konflikte) überprüft wurden, werden sie zu einer Enforcement-Komponente weiter geleitet, wo sie während der Laufzeit ausgewertet und durchgesetzt werden.

Ein zusätzliches Policy Monitoring, in welchem verfolgt wird, ob die Policies durchgesetzt wurden und ob diese die geplante Wirkung haben, liefert Ergebnisse, die zur Verbesserung der existierenden Policies weiterverwendet werden können. Auch die IT-Security-Policies,

¹³Pervasive Computing ist der industrielle Ansatz zur Durchdringung des Alltags mit smarten Gegenständen [69].

die (noch nicht) automatisiert verwaltet werden können, müssen regelmäßig auf ihre Anwendung und Wirksamkeit überprüft werden. Konkret wird die Wirksamkeit der erstellten und durchgesetzten IT-Security-Policies z. B. durch Penetrationstests¹⁴ oder eine Kontrolle der Umsetzung der nicht automatisierten Security Maßnahmen. Die erkannten Schwachstellen führen zur Änderung oder Anpassung der Policies.

In dem bereits beschriebenen mehrstufigen Verfeinerungsprozess von der Corporate IT-Strategie bis zu den interpretierenden Anweisungen an das System entstehen mehrere IT-Security-Policies. Diese Policies sind wirksam in einem bestimmten Kontext. Damit sie aktuell bleiben, muss das Policy Repository regelmäßig überprüft und weiterentwickelt werden. Dabei müssen die neuen Anforderungen an das System, die sich durch das Bekanntgeben von neuen Schwachstellen und Angriffen ergeben, oder neue Schutzfunktionen, Änderungen in der Organisation oder Änderung der Risiken der zu schützenden IT-Werte betrachtet werden.

2.3.3 Beitrag der IT-Security-Standards zur Erstellung der IT-Security-Policies

Im Rahmen des IT-Security-Prozesses in einer Organisation spielen die IT-Security-Standards, die Normen und Best Practices eine wichtige Rolle. Das Management der IT-Security-Policies, dessen Entstehungsprozess im vorigen Abschnitt beschrieben wurde, kann nach existierenden IT-Security Standards ausgerichtet werden. Manche regulatorischen Vorgaben, wie z. B. die MaRisk VA, verweisen ausdrücklich auf solche Regelwerke.

„Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen.“

Auch wenn keine Pflicht oder Empfehlung in diese Richtung entsteht, ist die Orientierung im IT-Security Prozess nach diesen Standards, Normen und Best Practices ein Signal in Richtung Verstärkung des Vertrauens in eine Organisation, sowohl von der Seite der Geschäftspartner, als auch vom Staat [83]. Die IT-relevanten Prozesse der Organisation werden durch den Einsatz der Standards transparent und leichter zu verwalten. Die Auswahl der relevanten IT-Security Standards ist ein Teil des IT-Security Managements. Die Standards sind hilfreich, weil sie, von allgemeinen Maßnahmen bis zu Implementierungsdetails zeigen, wie der IT-Security Prozess durchzuführen ist. Sie empfehlen Methoden,

¹⁴Ein Penetrationstest ist ein Test, während dessen das Angriffsverhalten eines vorsätzlichen Innen- oder Außentäters simuliert wird. Dabei wird es versucht zu ermitteln, welche Schwachstellen ausgenutzt und welche Schäden verursacht werden können [21].

verschiedene Tools und Produkte, die zur Wirksamkeit dieses Prozesses beitragen. Wie in [9] nachzulesen ist (siehe Abbildung 2.6), werden folgende Ziele beim Einsatz von IT-Security Standards verfolgt:

Kostensenkung	<ul style="list-style-type: none"> ■ Nutzung vorhandener und praxiserprobter Vorgehensmodelle ■ Methodische Vereinheitlichung und Nachvollziehbarkeit ■ Ressourceneinsparung durch Kontinuität und einheitliche Qualifikation ■ Interoperabilität
Einführung eines angemessenen Sicherheitsniveau	<ul style="list-style-type: none"> ■ Orientierung am Stand der Technik und Wissenschaft ■ Gewährleistung der Aktualität ■ Verbesserung des Sicherheitsniveaus durch die Notwendigkeit der zyklischen Bewertung
Wettbewerbsvorteile	<ul style="list-style-type: none"> ■ Zertifizierung des Unternehmens sowie von Produkten ■ Nachweisfähigkeit bei öffentlichen und privatwirtschaftlichen Vergabeverfahren ■ Verbesserung des Unternehmensimage ■ Stärkung der Rechtssicherheit

Abbildung 2.6: Ziele beim Einsatz von Security Standards.

Manche Standards können auch in einer Organisation eingesetzt werden, weil eine Zertifizierung erzielt wird. Dadurch wird bestätigt, dass alle im Standard geforderten Anforderungen zum Zeitpunkt der Zertifizierung erfüllt sind. Alle diese IT-Security Standards haben die Tatsache gemeinsam, dass sie Richtlinien für einzelne Aspekte der IT-Security und des IT-Risikomanagements anbieten. Sie helfen dabei:

- IT-Security-Strategien und -Leitlinien von Organisationen festzulegen,
- IT-Security-Risiken zu bewerten,
- IT-Security-Ziele zu ermitteln und IT-Security-Anforderungen abzuleiten,
- Geeignete Gegenmaßnahmen (unter anderem auch Grundschutzmaßnahmen) auszuwählen und deren dauerhafte Umsetzung sicherzustellen.

Die Auswahl der einzuhaltenden IT-Security Standards ist von mehreren Faktoren abhängig: von der Art der Organisation, vom Bereich, in welchem eine Standardisierung durchgeführt werden soll und auch von den Eigenschaften des Standards. Einige Beispiele von IT-Security Standards, welche bei der Erstellung eines IT-Security Konzeptes hilfreich sein können:

ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements ist ein Standard, der Maßnahmen unabhängig von Typ, Größe und Geschäftsfeld der Organisation vorschlägt. Der technische Detaillierungsgrad ist gering aber die Prozesse innerhalb einer Organisation werden ausführlich beschrieben. Die ermittelten Risiken werden in der Organisation durch festgelegte Kontrollmaßnahmen minimiert. Der Standard richtet sich an das Management und an die Sicherheitsbeauftragten.

ISO/IEC 27002: Code of practice for information security management ist ein Standard, der dort angewendet wird, wo Schutzbedarf für Informationen besteht. Dabei sind alle Bereiche der Organisation einzubeziehen, die an der Erhebung, Verarbeitung, Speicherung und Löschung von Informationen beteiligt sind.

Sektorspezifische Standards sind z. B. *ISO/IEC 27011* und die *Richtlinie VDI/VDE2182 (Informationssicherheit in der industriellen Automatisierung)*. Jene Richtlinie beschreibt durch welche Maßnahmen die Security Aspekte bei dem Einsatz der Automatisierungsgeräte beachtet werden sollen. Der *Payment Card Industry Data Security Standard (PCI DSS)* zielt darauf, durch eine Liste von Anforderungen und Kontrollen die Security der Kreditkarten und des Online-Zahlungsverkehrs zu erhöhen, und richtet sich an Unternehmen, die Kreditkartendaten verarbeiten, speichern oder übermitteln.

Control Objectives for Information and Related Technology (Cobit) sieht die IT als Resource zur Realisierung der Geschäftsprozesse und stellt ein Framework zur Verfügung, das alle Aspekte des IT-Einsatzes von der Planung über den Betrieb bis zur Entsorgung berücksichtigt.

IDW Prüfungsstandard: Abschlussprüfung beim Einsatz von Informationstechnologie (IDW PS 330) ist ein Leitfaden für Wirtschaftsprüfer, zur IT-Prüfung rechnungsrelevanter IT-Systeme.

IT Infrastructure Library (ITIL) ist ein Referenzmodell mit Best Practices im Bereich des IT-Dienstleistungsmanagement. Es gibt Empfehlungen für die Gestaltung der Geschäftsprozesse mit Einbeziehen der Aspekte der IT-Security, mit dem Ziel, Service- und kundenorientierte, zuverlässige, sichere und wirtschaftliche IT-Services aus der Sicht eines Unternehmens zu erbringen [9].

Die *BSI-IT-Grundschatz-Kataloge* vom Bundesamt für Sicherheit in der Informatik (BSI), (vor 2005 als das *IT-Grundschatzhandbuch* bekannt), sind ein Leitfaden zum Aufbau und zur Verbesserung eines funktionierenden IT-Security Management innerhalb von Organisationen, und zur Erstellung von IT-Security-Policies. Dieser Leitfaden enthält Kataloge mit Standard-IT-Security-Maßnahmen aus den folgenden Bereichen: Infrastruktur, Organisation, Personal, Hard- und Software, Kommunikation und Notfallvorsorge. Das Ziel der BSI-IT-Grundschatz-Kataloge ist, abhängig von den identifizierten Gefährdungen in den genannten Bereichen, infrastrukturelle, organisatorische, personelle und technische IT-Security-Maßnahmen für die Erhaltung eines Standard-Sicherheitsniveaus für IT-Systeme zu empfehlen.

2.4 Zusammenfassung

Dieses Kapitel hat die Begriffe erklärt, welche in der restlichen Arbeit eine wichtige Rolle spielen: *Compliance*, *IT-Security* und *IT-Security-Policies*.

Wichtig war ein Überblick über die Quellen, Rollen und Funktionen der Compliance und über die Sanktionen der Nicht-Einhaltung der Compliance Anforderungen. Diese Aspekte erklären, warum die Compliance ein beliebter Untersuchungsgegenstand der aktuellen Forschung ist und bieten eine hohe Motivation, dieses Thema in dieser Diplomarbeit zu behandeln.

Es wurde außerdem gezeigt, dass die „Überregulierung“ durch Compliance Anforderungen ohne die Hilfe der IT nicht beherrschbar ist. Der Einsatz der IT in den Organisationen bringt nicht nur die Vorteile der Automatisierung mit, sondern auch Pflichten, wie z. B. die Bewahrung der IT-Security Ziele. Diese Herausforderung kann nur erfüllt werden, wenn eine funktionierende IT-Security-Organisation existiert. Die IT-Security-Policies stellen ein wichtiges Instrument zur Verfügung, um Security-Maßnahmen einzuführen und durchzusetzen und die Unterstützung durch Security Standards bietet nicht nur Effizienz im Security-Prozess, sondern trägt auch zur Stärkung des Vertrauensdreiecks Staat-Organisation-Geschäftspartner bei.

Beschrieben wurde auch der Prozess der Entstehung der IT-Security-Policies, von den Corporate IT-Policies bis zur formalen Darstellung mit Hilfe spezialisierter, vom System interpretierbarer Sprachen.

Kapitel 3

Die Analyse der regulatorischen Texte

In [50] wird die Aufgabe der Erhebung von Compliance Anforderungen aus den Gesetzestexten als schwierig eingestuft. Eine automatisierte Durchführung dieser Aktion war bisher und wird auch in naher Zukunft nicht möglich sein [33, 38], daher ist eine manuelle Analyse und Interpretation des Gesetzestextes notwendig.

Eine Auseinandersetzung mit dem Gesetzestext führt besonders für diejenigen, die keine rechtlichen oder domänenspezifischen (z.B. aus Wirtschafts-, Versicherungs- oder Bankenbereich) Kenntnisse haben (in der Regel sind die Software-Ingenieure oder die IT-Administratoren für die Erhebung der IT-Security Anforderungen verantwortlich), zu fehlerhaften oder mangelhaften Interpretationen. Die Folge einer solchen Interpretation ist dann die Nichterfüllung der Compliance Anforderungen.

Die Aufgabe dieser Diplomarbeit ist es, zu untersuchen, ob IT-Security Policies direkt von dem regulatorischen Text abgeleitet werden können. Ein Schritt in dieser Untersuchung besteht aus der Analyse der Texte, welche Compliance Anforderungen enthalten. Die Entwicklung einer Methode, welche die semantischen Unterschiede zwischen der Sprache der Gesetze und derjenigen der IT-Security überwindet, setzt die Kenntnis der Eigenschaften des Gesetzestextes voraus. Aus diesem Grund werden in diesem Kapitel einige Eigenschaften des Gesetzestextes beschrieben. Anschließend wird untersucht, worin die Schwierigkeiten bei der Erhebung der Compliance Anforderungen aus den Gesetzen bestehen.

3.1 Eigenschaften der juristischen Sprache

Innerhalb der Institutionen mit Regelungskompetenz wird die juristische Fachsprache (Sprache des Rechts, Rechtssprache) verwendet. In der Literatur [20, 24] wird eine Fachsprache

definiert als spezielle funktionale Sprache mit spezifischen sprachlichen Merkmalen, die auf bestimmte kommunikative Ziele bezogen werden. Das Ziel der juristischen Sprache ist es, Direktiven in einer abstrakten, offiziellen und unpersönlichen Art auszudrücken [63]. Die Besonderheiten der juristischen Fachsprache gegenüber der Standard-Sprache zeigen sich auf morphologischer, syntaktischer, lexikalischer und semantischer Ebene und werden im Folgenden kurz beschrieben.

Morphosyntaktische Merkmale Die morphosyntaktische Ebene der juristischen Fachsprache wird durch die Verwendung von so genannten juristischen „syntaktischen Mustern“ [20] charakterisiert:

- Nominalkonstruktionen, welche durch die Substantivierung der Verben entstehen; dies sind abstrakte Hauptwörter, die eine Tätigkeit oder einen Prozess bezeichnen,
- Viele Kürzungen (Akronyme),
- Verben in der Passivform, welche die oben genannten Nominalkonstruktionen begleiten,
- Verben im Präsens, welche die Gegenwärtigkeit, die Verbindlichkeit und Allgemeingültigkeit des Rechts zum Ausdruck bringen.

Die Häufigkeit solcher Konstrukte ist der Grund dafür, dass die Sprache des Rechts als unpersönliche und passivische Sprache betrachtet wird.

Semantisch-lexikalische Merkmale Die juristische Sprache zeichnet sich besonders durch die Verwendung eines spezifischen Wortschatzes aus:

- Fachjargon: Ausdrücke, die der Form nach den gemeinsprachlichen Begriffen entsprechen, aber mit eingeschränkter oder abweichender Bedeutung verwendet werden [20, 72],
- Fachtermini: eigentliche rechtliche Begriffe,
- Archaismen: veraltete Wörter.

Die juristische Fachsprache hat einen hohen Anspruch auf Eindeutigkeit, daher steht sie der Synonymbildung entgegen und vermeidet auch die Nutzung von mehrdeutigen Wörtern (Polyseme) [20].

Gesetzliche Konzepte Die Gesetze beschreiben Aktionen, durch welche eine spezifische Handlungsqualität und ein spezifischer Zweck vorgeschrieben werden [35]. Nach G. Sartor ist eine Aktion die kleinste Einheit des Gesetzestextes auf interpretativer Ebene. Eine Aktion bekommt Normenstatus, indem sie mit Hilfe von deontischen Möglichkeiten

verfeinert wird [73]. Der Begriff *deontisch* ist besonders durch die Arbeiten im Bereich der deontischen Logik bekannt geworden. Als besondere Form der Modallogik, untersucht die deontische Logik Konzepte, die sich auf Handlungen beziehen, die Menschen bindend erfüllen müssen oder dürfen. Eine zentrale Rolle in der deontischen Logik spielen Begriffe wie: *Gebot*, *Verbot*, *Erlaubnis*, *Recht* oder *Pflicht*.

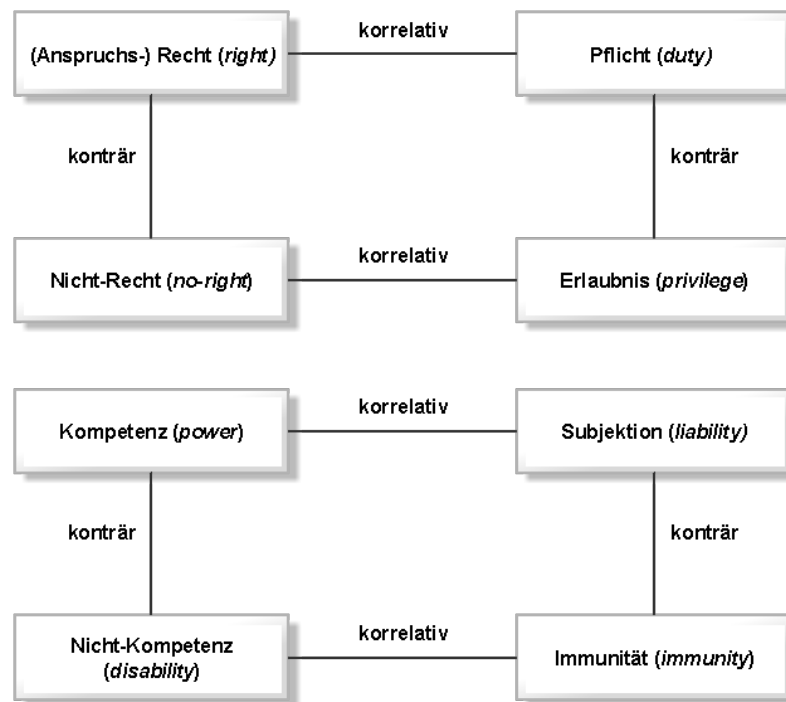


Abbildung 3.1: Die gesetzliche Taxonomie von Hohfeld.

Die deontische Natur des Rechtes wurde z. B. von W.N.Hohfeld in seiner Arbeit *Fundamental Legal Conceptions as Applied in Judicial Reasoning* (1920) [37] hervorgehoben. Hohfeld unterscheidet zwischen acht grundlegenden rechtlichen Konzepten, die in zwei Gruppen unterteilt werden: die so genannten korrelativen Relationen (*jural correlatives*) und die konträren Relationen (*jural opposites*). Eine korrelative Relation besteht nach Hohfeld zwischen gesetzlichen Konzepten, die sich wechselseitig ergänzen; eine konträre Relation besteht zwischen Konzepten, die sich gegenseitig ausschließen. Die Abbildung 3.1 stellt die gesetzliche Taxonomie von Hohfeld dar (die Übersetzung der Konzepte ins Deutsche ist in der Literatur nicht einheitlich; hier werden die Begriffe aus [76] übernommen).

Die gesetzlichen Konzepte von Hohfeld werden in mehreren Arbeiten (siehe z. B. [4, 10, 62, 64, 40]) als Grundlage für die Analyse von gesetzlichen Anforderungen innerhalb des Requirements Engineering benutzt.

3.2 Probleme bei der Analyse der juristischen Texte

Der Gesetzestext interagiert mit zwei generischen Akteuren: dem Gesetzgeber, der das Gesetz verfasst, und demjenigen, an den sich das Gesetz wendet [87]. Daher ist es wichtig, dass die Konzepte, die in dem Rechtstext enthalten sind, die gleiche Bedeutung für alle Teilnehmer des Rechtsaktes haben. Als Fachsprache strebt die Sprache des Rechts ein höchstmögliches Maß an Eindeutigkeit, Bestimmtheit und Genauigkeit an [20]. Der Abstraktionsgrad und die Sachlichkeit, welche durch die im vorigen Abschnitt beschriebenen morphosyntaktischen und lexikalisch-semanticen Mittel erzielt werden, sollten die Eindeutigkeit der rechtlichen Aussagen und somit eine einheitliche Interpretation des Gesetzestextes sicherstellen. Zu diesem Zweck dienen auch die verschiedenen Definitionen und Erklärungen von Rechtsbegriffen oder von Anforderungen, die im Gesetz enthalten sein können.

3.2.1 Ambiguität und Vagheit

Eine Eigenschaft der natürlichen Sprache ist, dass sie durch ihre Arbitrarität und Konventionalität interpretationsfähig ist. Diese Eigenschaft charakterisiert auch die juristische Sprache, und einerseits wird sie oft im Recht absichtlich zur Eröffnung eines Interpretationsspielraums ausgenutzt. Diese Möglichkeit erlaubt die flexible Anpassung an unterschiedliche Kontexte für verschiedene Interessen. Andererseits bereitet der Mangel an Deutlichkeit und Verständlichkeit Probleme besonders für Fachfremde, wie z. B. Software- oder Security-Ingenieure, welche als Aufgabe die Erhebung von relevanten Compliance Anforderungen aus regulatorischen Texten haben.

Lexikosemantische Ambiguität Die Schwierigkeiten in der Analyse des Gesetzestextes, die oft in der Literatur über *Requirements Engineering* (z. B. [4, 10, 50]) Erwähnung finden, werden durch die Verwendung von mehrdeutigen Wörtern, vagen Ausdrücken und ambigen Sätzen verursacht. Die Vagheit besteht dann, wenn eine Referenzundeutlichkeit oder Referenzunschärfe in der Bedeutung vorhanden ist und diese Unbestimmtheit der Bedeutung nicht durch den Kontext aufgehoben werden kann. Die Ambiguität ist eine Art semantische Unbestimmtheit eines Wortes, für das mehrere konkurrierende Interpretationen gibt.

Morphosyntaktische Ambiguität Probleme in der Interpretation des Rechtes gibt es sogar auf der morphosyntaktischen Ebene der juristischen Sprache. Die Häufigkeit der Nominalkonstrukte und der passivischen Sätze erlauben das Zurücktreten oder sogar die Abwesenheit eines handelnden Subjektes [72]. Bei der Umsetzung der Compliance Anforderungen kann dies die Unbestimmtheit der Verantwortlichen für verschiedene Aktivitäten zur Folge haben. Auch die Ordnung der einzelnen Wörter in der Phrase oder die einfache

Verwendung der Konjunktionen (*und*, *oder*) können zu unterschiedlichen Interpretationen der gesetzlichen Anforderungen führen. Eine ausführliche Analyse der Quellen der syntaktischen Ambiguität in der juristischen Sprache wird in [17] gemacht.

Konzeptuelle Ambiguität G. Sartor beschreibt in [73] eine Art von Ambiguität, welche durch die Unvollständigkeit von manchen gesetzlichen Konzepten verursacht wird. *Pflicht* und *Verbot* z. B. sind vollständig, denn wenn es gesagt wird, dass eine Aktion A verpflichtend ist, dann ist die Aktion NON-A verboten; wenn die Aktion A verboten ist, dann ist die Aktion NON-A verpflichtend. Im Fall des Konzeptes *Erlaubnis* gibt es keine Vollständigkeit: impliziert eine Erlaubnis der Aktion A die Erlaubnis der Aktion NON-A? Die Antworten auf solche Fragen hängen stark von der Interpretation derjenigen ab, die sich mit der Analyse und Interpretation des Gesetzestextes beschäftigen.

3.2.2 Die Intertextualität des Gesetzestextes

Es kann im Fall der juristischen Texte von einer Intertextualität im Sinne von G. Genette gesprochen werden [27], weil solche Texte als vollständig betrachtet werden können, wenn alle Gesetze, die darin erwähnt werden, auch beachtet und analysiert werden. Solche Fälle vom „Text im Text“ sind in der Form von Querverweise sichtbar und werden schematisch in der Abbildung 3.2 dargestellt.

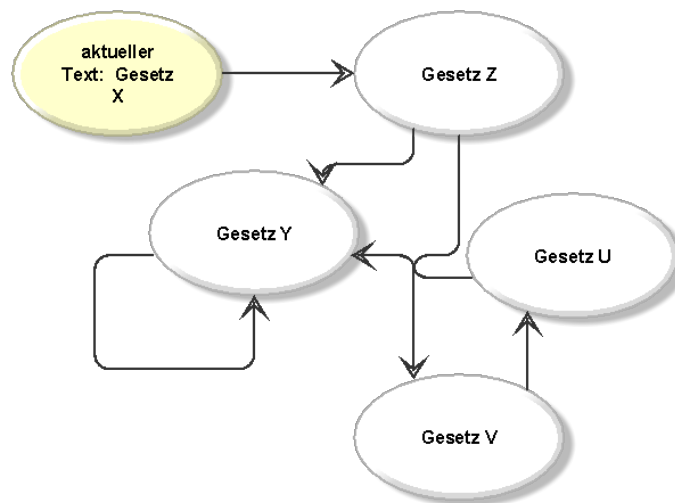


Abbildung 3.2: Querverweise im Gesetzestext.

Die Missachtung der Querverweise hat die Formulierung unvollständiger und fehlerhafter Compliance Anforderungen zur Folge.

Wenn mehrere Regularien zum selben Zeitpunkt beachtet werden müssen (und im vorigen Kapitel wurde gezeigt, dass dies der normale Fall ist), besteht für die Analysten der Rechtstexte die Gefahr, dass die Compliance Anforderungen inkonsistent oder redundant

interpretiert werden [90, 92]. Inkonsistenzen treten auf, wenn sich die Anforderungen aus unterschiedlichen Quellen widersprechen. Wenn Anforderungen mit der gleichen Semantik in verschiedenen regulatorischen Texten syntaktisch unterschiedlich ausgedrückt werden, dann können Redundanzen bei der Formulierung der zu befolgenden Regeln entstehen.

Die morphosyntaktische Ambiguität der juristischen Sprache kann nach [17] durch Formulierung der Aussagen nach logischen Regeln vermieden werden; die semantisch-lexikalische Ambiguität sowie die Ambiguität auf Konzeptebene bleiben trotzdem der Sprache inhärent. Damit die Missverständnisse, Inkonsistenzen und Fehler in der Erhebung der Compliance Anforderungen aus den Gesetzestexten vermieden werden, müssen nach [50], zusätzlich zu den sprachlichen Analysemethoden, noch systematische (im Kontext des ganzen Gesetzes) oder historische (mit dem Betrachten der Umstände, unter welchen das Gesetz erlassen wurde) Methoden angewendet werden.

3.3 Zusammenfassung

In diesem Kapitel wurden einige der spezifischen Merkmale, welche Schwierigkeiten bei der Analyse des juristischen Textes bereiten und ein Grund für fehlerhafte Interpretationen der Compliance Anforderungen sein können, beschrieben. Die Beseitigung solcher Probleme und die Erhebung der Compliance Anforderungen aus den Rechtstexten, sowie deren Formalisierung, ist einer der Schwerpunkte der Forschung im Bereich des *Requirements Engineering* oder der Rechtsinformatik. Das nächste Kapitel stellt einige relevante Arbeiten aus diesem Bereich der Analyse der regulatorischen Vorgaben vor.

Kapitel 4

Compliance Management: Stand der Forschung

In Kapitel 2 dieser Arbeit wurde gezeigt, dass die Compliance mit den regulatorischen Vorgaben ein Prozess ist, der sich über mehrere Phasen, von der Identifizierung der einzuhaltenden Anforderungen bis zum Nachweis der Einhaltung dieser Anforderungen streckt. Die Wichtigkeit dieses Prozesses zeigt sich seit Jahren auch am Interesse der Forschung, zur Gestaltung eines effizienten Compliance Managements beizutragen.

Die Untersuchung des Forschungsstandes im Bereich der Compliance, die im Rahmen dieser Diplomarbeit durchgeführt wurde, hat das Ziel, Antworten auf die folgenden Fragen bereitzustellen:

- Welche Ansätze gibt es für die Analyse der regulatorischen Texte, damit die Durchsetzung der Compliance Anforderungen vereinfacht und automatisiert abläuft?
- Wie werden die Compliance Anforderungen an die IT-Security adressiert und formalisiert?
- Gibt es bereits Lösungen für die Abbildung der regulatorischen Compliance auf IT-Security-Policies?

Der Schwerpunkt der untersuchten Arbeiten liegt auf folgenden Aspekten des Compliance-Lebenszyklus:

- Darstellung des Wissens, welches in den Gesetzestexten enthalten ist, oder eines der juristischen Konzepte (z. B.. eines Teiles der in Kapitel 3 vorgestellten Hohfeldschen Taxonomie) mit Hilfe unterschiedlicher Logiken.
- Strukturierte Darstellung der Gesetze mit Hilfe von Markup-Sprachen mit dem Zweck, das Information Retrieval und die Navigation in den gesetzlichen Texten oder den

Austausch von Informationen über diese Texte zwischen Organisationen zu vereinfachen.

- Modellierung der Compliance Anforderungen mit Hilfe von Logiken und Überprüfung der Einhaltung dieser Anforderungen (z. B.. durch *Model Checking*) in den verschiedenen Phasen der Geschäftsprozesse: *design-time-Compliance*, *run-time-Compliance*, Überprüfung der Einhaltung der Compliance anhand der Audit-Daten (mehr dazu in [70, 81, 85]).

Die für diese Diplomarbeit wichtige Frage, wie die regulatorische Compliance auf Security Policies abgebildet werden kann, wird in der untersuchten Literatur nicht behandelt.

Im diesem Kapitel wird ein Überblick über die unterschiedlichen Ansätze zur Modellierung der Gesetzestexte, zur Identifizierung und Formalisierung der juristischen Konzepte (so wie sie z. B.. durch die Taxonomie von Hohfeld dargestellt werden), und zur Entwicklung der Compliance-Checking-Systeme gegeben.

4.1 Systematische Darstellung des juristischen Wissens

Die im vorigen Kapitel beschriebene Ambiguität einerseits und die interne Logik der juristischen Sprache andererseits haben dazu geführt, den gesetzlichen Text als Computerprogramm zu modellieren, um legale Konzepte wie z. B.. diejenigen aus der Taxonomie von Hohfeld zu formalisieren und Schlussfolgerungen aus den gesetzlichen Anforderungen automatisch zu berechnen. Auf diese Weise werden besonders die syntaktischen Ambiguitäten im Text entfernt.

ESPLEX [7] ist ein Projekt zur Modellierung von Gesetzen in PROLOG und wurde auf einige italienische Gesetze angewendet. Die logischen Relationen zwischen den gesetzlichen Anforderungen werden mit Hilfe der Prädikatenlogik erster Stufe ausgedrückt (deklarative Funktion von PROLOG). Dieses explizite Wissen wird durch die manuelle Analyse des Textes erworben und durch die Modellierung der Beziehungen zwischen den Konzepten als semantisches Netz vervollständigt. Für Anfragen der Wissensbasis steht ein in PROLOG implementiertes Management-System zur Verfügung (prozedurale Funktion von PROLOG).

Language for Legal Discourse (LLD) [58] ist eine formale Sprache, die für die Darstellung der konzeptuellen Modelle aus dem juristischen Bereich geeignet ist. Sie basiert auf der Prädikatenlogik erster Stufe und wird um Möglichkeiten erweitert, die die *common sense*-Kategorien (Raum, Zeit, Aktion, Erlaubnis, Verpflichtung, Kausalität, Zweck, Absicht, Wissen, Grauben) ausdrücken.

Formal Contract Language (FCL) [29, 59, 71] ist ein Ansatz, der auf der Theorie der normativen Systeme basiert und Elemente der deontischen Logik mit Elementen der Logik der Verstöße (*logic of violations*) kombiniert. Die Compliance Anforderungen (in diesem Fall *control objectives* genannt) werden als deontische Einschränkungen (*deontic constraints*) in FCL spezifiziert; zusätzlich zu den Verpflichtungen, Erlaubnissen und Verboten aus der deontischen Logik, können auch Verstöße ausgedrückt werden. Die FCL-Spezifikationen werden geparkt, und die Parsing-Ergebnisse, die so genannten *control tags* (*flow, data, resource* und *time tags*), werden zur Annotation des Geschäftsprozessmodells benutzt. Der Vorteil, dass die Compliance Anforderungen innerhalb der Geschäftsprozessmodelle visualisiert werden können und ihre Konsistenz automatisch überprüfbar ist, macht das Verfahren zur modellgetriebenen Entwicklung complianter Systeme gut geeignet und bietet eine integrierte Sicht auf das Compliance- und Geschäftsprozess-Management.

Semantic Web Technologien werden immer öfter zur Darstellung des juristischen Wissens benutzt. Die juristischen Ontologien (*legal ontologies*) fassen die juristischen Konzepte und die Zusammenhänge zwischen ihnen in einem semantischen Modell zusammen. Der Zweck der semantischen Darstellung der Gesetze ist sowohl die theoretische Untersuchung, der Erwerb und die Wiederverwendung des juristischen Wissens als auch die Indexierung der Gesetze, um das Suchen und Finden von Informationen nach bestimmten semantischen Kriterien organisationsübergreifend zu gewährleisten. Die Ontologien werden mit Hilfe von W3C-Standardsprachen formalisiert, wie *Resource Description Framework (RDF)* oder *Web Ontology Language (OWL)*, und hauptsächlich mit dem Ontologien-Editierungstool Protegé¹ modelliert [16].

Interessant ist es, wenn sowohl der Rechtstext, als auch die Struktur der Organisation, die mit dem Rechtstext compliant sein muss, mit Hilfe von Ontologien dargestellt werden, damit überprüft werden kann, ob die Organisation die Compliance Anforderungen erfüllt. Ein solcher Ansatz wird z. B. in [88, 90, 91] vorgestellt. Hier werden die gesetzlichen Anforderungen mit Hilfe der *Semantic Web Rule Language (SWRL)* modelliert und mittels Model Cheking auf Einhaltung innerhalb des mit Ontologien modellierten Systems überprüft. Das Verfahren unterstützt auch die Anwendung von Regeln oder die Auswertung von Daten, die unvollständig definiert sind (*robust and adaptive compliance system*).

Semantic parameterization [11, 12, 13, 14] ist eine Methode für die automatisierte Abbildung der natürlichen Sprache auf semantische Modelle. Der Zweck des Verfahrens ist einerseits die Lösung der Ambiguitäten der juristischen Sprache und andererseits die automatisierte Analyse der juristischen Schlussfolgerungen. Im ersten Schritt des Verfahrens

¹<http://protege.stanford.edu/>

wird der juristische Text durch die *Goal-Based Requirements Analysis Method (GBRAM)* analysiert. Diese Methode erlaubt die informelle Darstellung der Compliance Anforderungen als Ziele (engl. *goals*) in *unrestricted natural language statements (UNLS)*. Im nächsten Schritt wird eine semantische Analyse der UNLS durchgeführt. Das Ziel dieser Analyse ist die Identifizierung von einzelnen Aktivitäten, welche Verpflichtungen oder Rechte der Stakeholder darstellen.

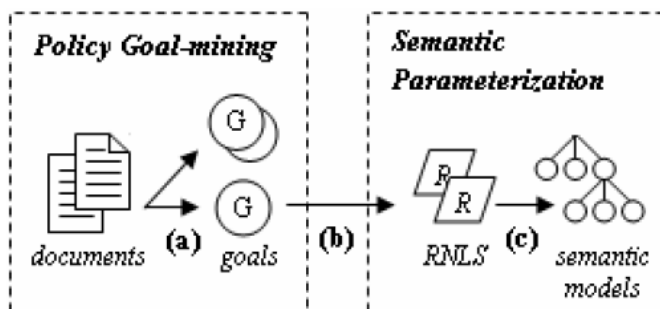


Abbildung 4.1: *Semantic parameterization* (vgl. [13]).

Das UNLS wird dann in mehrere *restricted natural language statements (RNLS)* umformuliert (siehe Tabelle 4.1). Ein RNLS stellt eine einzige Aktion dar und hat ein oder mehrere Subjekte und Objekte (Pflichtkomponenten), sowie andere optionale Komponenten (z. B. Zweck, Instrument). Abhängig von ihrer Semantik werden die RNLS durch logische Konnektoren in Constraints zusammengefasst, welche semantisch Verpflichtungen oder Rechte darstellen.

Aus den erstellten semantischen Modellen können die Subjekte, Objekte, Aktionen, Zwecke oder Instrumente, welche Rechte, Erlaubnisse und Verpflichtungen beschreiben, automatisch extrahiert werden. Die Informationen können z. B. zur automatischen Generierung von Policies bereit gestellt werden.

Die oben beschriebenen Ansätze zur logischen Beschreibung des juristischen Textes oder zur Spezifikation der einzelnen juristischen Konzepte (außer der Modellierung mit Hilfe der Ontologien) haben die Tatsache gemeinsam, dass die Analyse des Textes manuell durchgeführt wird. Diese Analyse ist sehr aufwendig: z. B. die Extrahierung der Rechte und Verpflichtungen mit Hilfe der *semantic-parameterisation*-Methode aus vier Abschnitten des Health Insurance Portability and Accountability Act (HIPAA) hat 42 Mannstunden gekostet. Zusätzlich kann die manuelle Analyse fehleranfällig sein. Die durch diese Ansätze erstellten Expertensysteme, können durch die Requirements Engineers befragt werden, wenn Ambiguitäten im regulatorischen Text zur Unsicherheit führen. Die vorgestellten Ver-

Goal (UNLS1)	A covered entity that agrees to a restriction may not use or disclose protected health information, except if the individual who requested the restriction is in need of emergency treatment.
RNLS1	The covered entity who (RNLS2) may not disclose protected health information, except if (RNLS3).
RNLS2	The covered entity agrees to a restriction.
RNLS3	The individual who (RNLS4) needs emergency treatment.
RNLS4	The individual requests the restriction.
Constraint C1:	The covered entity agrees to a restriction. 164.522 (a)(1)(iii)
Constraint C2	The individual needs emergency medical treatment. 164.522 (a)(1)(iii)
Constraint C3	The individual requests a restriction. 164.522 (a)(1)(iii)
Obligation O1	The covered entity may not disclose protected health information. 164.522 (a)(1)(iii) $[C1 \wedge \neg C2 \wedge C3]$

Tabelle 4.1: Anwendung der *semantic-parameterization*-Methode (vgl. [13]).

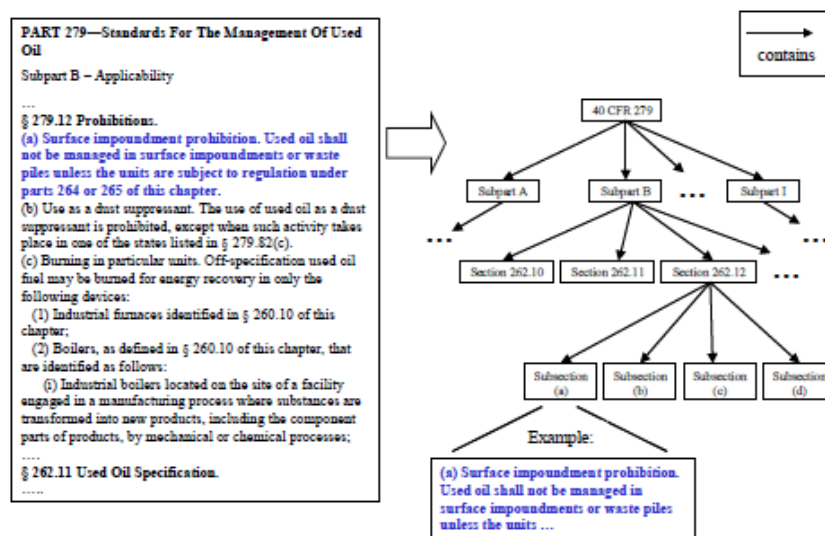
fahren sind begrenzt, weil sie nur in bestimmten Bereichen des Rechtes angewendet und getestet wurden (eigentlich in denjenigen Bereichen, für welche die Verfahren entwickelt wurden).

4.2 Systematische Darstellung des juristischen Textes

Die hierarchische Struktur der juristischen Texte eignet sich gut zur Darstellung mit Hilfe der Markup-Sprachen. Der Vorteil einer solchen Darstellung besteht darin, dass die Informationen über die im Text enthaltenen Definitionen, Abkürzungen und Querverweise als Metadaten zur Verfügung stehen. Die Darstellung dieser Informationen kann mit Techniken des Information Retrieval und mit logischen Methoden kombiniert werden; in diesem Fall können einzelne Abschnitte im Text gefunden und analysiert werden [64].

REGNET [46] ist ein Framework für die Unterstützung der Compliance mit den regu-

latorischen Anforderungen und basiert auf der XML-Darstellung der Informationen über gesetzliche Texte, in Kombination mit einem Kalkül in der Prädikatenlogik erster Stufe. XML-Tags tragen zur Darstellung des XML-Baums bei. Der XML-Baum spiegelt die hierarchische Struktur des Textes wider, der aus verschiedenen Abschnitten und Unterabschnitten besteht (siehe Abbildung 4.2). Der Text wird weiter mit *regulation metadata* annotiert. Diese Metadaten bestehen aus *concept tags*, *reference tags* und *definition tags*. Die *concept tags* erlauben die Navigation zu verwandten Dokumenten aus dem *Document Repository*, die *reference tags* bestimmen die Querverweise aus dem Text, und die *definition tags* werden für die Markierung standardisierter Definitionen von Fachbegriffen oder Abkürzungen benutzt. Sowohl die Compliance Regeln aus dem Gesetz als auch die möglichen



Decomposition of regulation into a tree structure

```
<regulation id="40.cfr.279" name="Standards For The Management Of Used Oil" type="federal">
  <regElement id="40.cfr.279.A" title="Subpart A">
    <regElement id="40.cfr.279.12" title="Prohibitions">
      <regElement id="40.cfr.279.12.a" title="Surface Impoundment prohibition">
        <regText>
          <paragraph>Used oil shall not be managed in surface impoundments or waste
            piles...</paragraph>
        </regText>
      </regElement>
    </regElement>
  </regElement>
  <regulation id="40.cfr.279.12.b" title="Use as a dust suppressant">
  </regulation>
</regulation>
```

Abbreviated XML representation of regulation tree structure

Abbildung 4.2: XML-Baum eines Gesetzes nach REGNET-Konzept [46].

Fragen der Benutzer zur Compliance werden im REGNET mit Hilfe der Logik-Metadaten

modelliert. Die Benutzer können Informationen über einzelne Gesetze aus dem *Document Repository* über ein Web Interface abfragen. Der Beitrag von REGNET ist, dass es die Benutzer durch die regulatorischen Texte führt und ihr Verständnis für die Compliance erleichtert. Die Grenzen des Verfahrens sind, wie bei den bereits vorgestellten Ansätzen, die Einschränkung der Analyse auf einzelne regulatorische Texte.

Extensible Information Security Specification Format (XISSF) [89, 92] ist ein auf XML basiertes Markup-Format zur Spezifizierung von IT-Security Anforderungen. Der Vorteil dieses Ansatzes besteht darin, dass die wichtigsten Anforderungen aus unterschiedlichen IT-Security Standards mit der selben Semantik in einem XISSF-Dokument zusammengefasst werden und durch Ontologien-Mapping aufeinander abgebildet werden. Dieses Format trägt sowohl zur Vermeidung der Redundanzen bei der Umsetzung der Anforderungen als auch zur Austauschbarkeit der IT-Security Informationen zwischen verschiedenen Organisationen bei.

4.3 Regulatorische Compliance und Requirements Engineering

Einige Ansätze benutzen Methoden des Requirements Engineering² für die Analyse der regulatorischen Compliance. Das Ziel in diesem Fall ist, die Compliance Anforderungen bereits in der Design-Phase des Systems zu berücksichtigen.

*Secure Tropos*³ ist eine Methodologie zur Erhebung und Spezifizierung der Agenten, Akteure, Rollen, Standpunkte, Security-Ziele, Security-Aufgaben, Security-Ressourcen und Abhängigkeiten zwischen den Akteuren. Die Security Anforderungen des zu entwickelnden Systems, die möglichen Bedrohungen und Schwachstellen, sowie die möglichen Gegenmaßnahmen dafür, welche auf Basis dieser Security Anforderungen festgelegt werden, bilden die Security Referenz für das System. In [41, 40] wird die Secure Tropos Methodologie Bestandteil eines Frameworks für die Modellierung der Compliance Anforderungen an die IT-Security und ihre Spezifizierung beim Systementwurf. Die vier Komponenten dieses Security-Compliance Frameworks werden in der Abbildung 4.3 dargestellt:

1. Die *Modelling-Regulation*-Komponente unterstützt die Interpretation der Gesetzestexte und die Ableitung der gesetzlichen Rechte durch die Identifizierung und Analyse der Konzepte der bereits beschriebenen Taxonomie von Hohfeld. Für die Textanalyse werden verschiedene Heuristiken, Natural Language Processing-Techniken

²Teil des Software- und Systementwicklungsprozesses.

³<http://www.securetropos.org/>

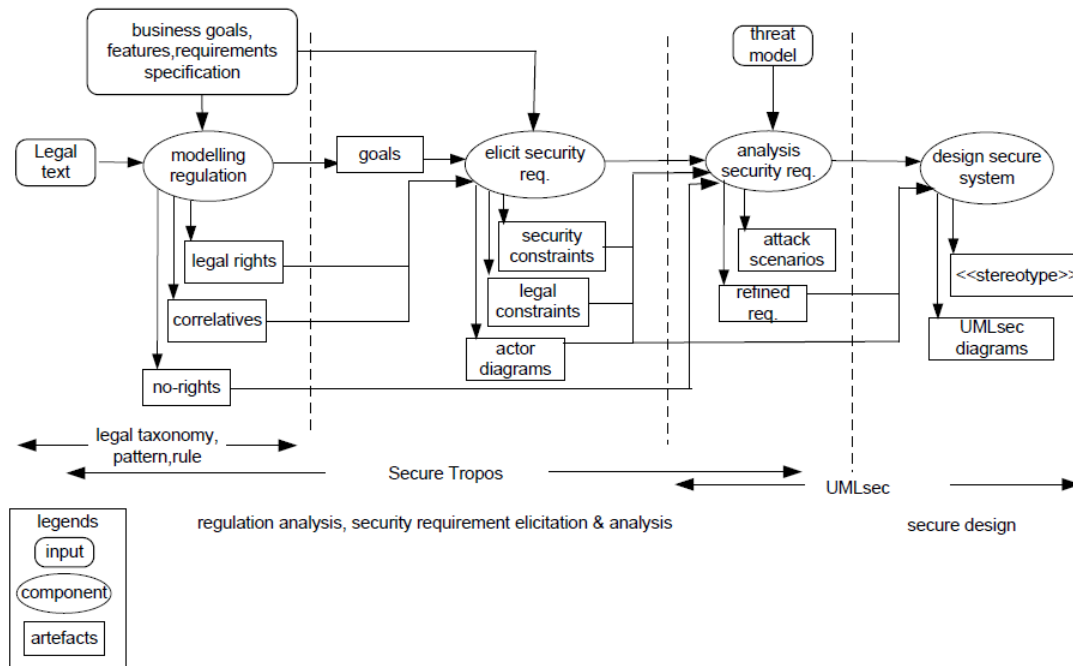


Abbildung 4.3: Modellierung der Compliance Anforderungen mit Secure Tropos [40].

(NLP-Techniken) und ein Pattern-basierter Ansatz benutzt, welcher der semantic-parameterization-Methode ähnlich ist.

2. Innerhalb der *Elicit-Security-Requirements*-Komponente, die auf den Analysetechniken von Secure Tropos basiert, werden die gesetzlichen Anforderungen auf IT-Security Ziele abgebildet. Die identifizierten IT-Security Ziele werden verfeinert und mit Secure Tropos modelliert.
3. Die *Security-Requirements-Analysis*-Komponente basiert auf der Analyse von Gefährdungen und Nicht-Einhaltung der Compliance. Die möglichen Security-Attacken an das System werden identifiziert und analysiert. Diese Szenario-basierte Methode erlaubt die Spezifizierung der IT-Security Anforderungen im Einklang mit den regulatorischen Vorgaben.
4. Die *Secure-System-Design*-Komponente unterstützt die Berücksichtigung der Compliance Anforderungen an die IT-Security bereits beim Design des Systems. Die Modellierung des sicheren Systems wird mit UMLsec durchgeführt. UMLsec ist eine Erweiterung von UML, welche IT-Security-Eigenschaften mit Hilfe von Stereotypen und Tags ausdrücken kann [42] (ein Überblick über die IT-Security-Aspekte, welche durch UMLsec modelliert werden können, kann der Abbildung 4.4 entnommen werden).

Der Vorteil des Frameworks besteht aus seiner Flexibilität in der Analyse und Modellierung der Compliance Anforderungen mit Schwerpunkt auf der IT-Security. Darüber hinaus

Diagram & stereotype	Tags	Constraints	Tech. security measures
Use case <<privacy>>	{state = {dataflow}, {data storage}, {data access}, {data process}}	right = (access, disclose, process, transmit) obligation = (unauthorized access & disclose, unlawful process, accidental loss or destruction) purpose = (financial, social security, health) policy = (privacy, access control, data classification, data transmission, etc)	Security of data communication (cryptographic algorithm, key length), strengthens of password (length, minimum number of combination, life time)
Deployment <<secure links>>	{authenticity = actor, data} {confidentiality} {adversary = {type={read}, {logical condition}}	right = (access, process) obligation = (unauthorized disclosure & access, unlawful process) policy = (data transmission, cryptographic control, etc)	data classification (sensitivity, confidential, public) location of critical data, storage (plain text, encrypted), access control mechanism (mandatory, role based, optional)
Deployment <<secure storage>>	{authenticity = actor, data} {authorization = actor, right} {data storage = format} {adversary = {type = {access, process}, {logical condition}}	right = (access, disclose, process) obligation = (unauthorized access, unlawful process, accidental loss, or destruction) policy = (access control, user responsibility, password, data storage, data classification, data backup, etc)	secure channel, authorization mechanism, etc.
Interaction <<data security>>	{authenticity = actor, data} {authorization = actor, right} {confidentiality = data} {integrity = {actor, data}} {adversary = {type = {access, process}, {logical condition}}	right = (access, disclose, process, transmit) obligation = (unauthorized access, disclosure, unlawful alternation, controller consent) policy = (data classification, user responsibility, acceptable use of asset, access control, data transmission, cryptographic control, etc)	

Abbildung 4.4: Unterstützung der IT-Security-Ziele durch UMLsec.

wurde das UMLsec-Tool bereits in mehreren Anwendungen getestet und wird weiter entwickelt.

4.4 Zusammenfassung

Dieses Kapitel hat einige aktuelle Forschungsrichtungen der Analyse, Spezifizierung, Formalisierung und Modellierung der regulatorischen Compliance vorgestellt. Die logikbasierten Ansätze haben den Vorteil, dass sie eine exakte Darstellung des Gesetzes erlauben, Ambiguitäten lösen und automatisierte logische Schlussfolgerungen über das Gesetz zulassen. Markup-Sprachen favorisieren die gezielte Navigation in den regulatorischen Texten und erleichtern das Verständnis des Gesetzes mit Hilfe der Metadaten. Methoden des Requirements Engineering erlauben die Berücksichtigung der Compliance Anforderungen bei Systementwurf und -Modellierung.

Bei der Untersuchung der beschriebenen Verfahren wurde beobachtet, dass die Analyse des regulatorischen Textes, besonders zur Klärung von Ambiguitäten, welche in der natürlichen Sprache charakteristisch sind, nicht vermieden werden kann. Die IT-Security-Anforderungen werden nur im Fall des Secure Tropos-UMLsec Frameworks adressiert. Die anderen Ansätze behandeln diese Anforderungen ohne sie von den anderen Anforderungen zu unterscheiden. Hierbei ist das Ziel nicht eine Lösung zu den Security Anforderungen anzubieten, sondern sie mit Hilfe von verschiedenen Logiken formalisiert wiederzugeben.

Die Beobachtungen aus der Untersuchung des Forschungsstandes in der Analyse der Rechtstexte und Formalisierung der gesetzlichen Anforderungen werden im nächsten Kapitel berücksichtigt. Dort wird ein Konzept für die Ableitung von IT-Security-Policies von der *MaRisk VA* vorgestellt.

Kapitel 5

Von der MaRisk VA zu IT-Security Policies

Die Einbeziehung der IT-Security-Aspekte bei der Planung und Ausführung der Geschäftsprozesse innerhalb von Organisationen ist die Voraussetzung für die Erfüllung der IT-Security-Ziele, und die Grundlage der Ausführung der Geschäftsprozesse im Einklang mit den Compliance Anforderungen aus den gesetzlichen Texten. In diesem Kapitel wird untersucht, inwiefern IT-Security Policies aus einem regulatorischen Text direkt ableitbar sind. Die Untersuchung wird auf die *MaRisk VA* angewendet, welche durch alle Versicherungsunternehmen aus Deutschland erfüllt werden muss. Dafür wird zuerst die Rolle der IT für die effiziente Ausführung der Geschäftsprozesse eines Versicherungsunternehmens vorgestellt, die *MaRisk VA* und ihr Bezug zu der IT-Security wird beschrieben, und anschließend wird das im Rahmen dieser Diplomarbeit erarbeitete Konzept zur Abbildung der regulatorischen Compliance auf IT-Security Policies vorgestellt.

5.1 Vorüberlegungen

5.1.1 Die Rolle der IT in Versicherungsunternehmen

Nach [15] gibt es in einem Versicherungsunternehmen folgende Geschäftsprozesse:

Strategische Management- und Führungsprozesse

- Die *Strategiedefinition* besteht aus der Festlegung der Strategie des Versicherungsunternehmens. Innerhalb dieses Geschäftsprozesses werden die lang- und mittelfristigen Ziele der Organisation abgeleitet und definiert. Auf dieser Basis wird die so genannte *Corporate Identity* entwickelt, an welcher sich alle nachfolgenden Führungsprozesse sowie alle weiteren strategischen und operativen Aktivitäten im Unternehmen orientieren.

- *Controlling* ist der Prozess, der die Ergebnisse der strategischen Planung aufnimmt, verarbeitet und umgesetzt; er enthält die Teilprozesse Planung, Durchführung und Steuerung.
- *Risikomanagement* besteht aus der Identifizierung und Steuerung der Risiken; dieser Geschäftsprozess liegt in der Verantwortung der Geschäftsleitung und ist nicht delegierbar.
- *Qualitätsmanagement* enthält alle Teilprozesse, die zur Verbesserung der Produkte, der Prozesse oder der zu erbringenden Dienstleistungen dienen. Die Unternehmensführung ist für diese Kategorie von Prozessen ebenso verantwortlich.

Operative Kernprozesse

- Das *Marketing* und der *Vertrieb* haben als Objekt die Planung, die Durchführung und die Kontrolle aller auf die Absatzmärkte gerichteten Unternehmensprozesse.
- Die *Produktentwicklung* hat als Ziel das Bereitstellen von markt- und kundengerechten sowie für das Versicherungsunternehmen profitable Versicherungsprodukte.
- Die *Bestandsführung und -verwaltung*: Das elementare Ergebnis jedes erfolgreichen Absatzprozesses ist der Antrag auf Abschluss eines Versicherungsvertrags. Das ist gleichzeitig ein auslösendes Ereignis und Input für einen zentralen Teilprozess der Bestandsverwaltung: die Antrags- oder Neugeschäftsbearbeitung.

Unterstützende Prozesse sind diejenigen Prozesse, die strategische oder operative Kernprozesse unterstützen. Obwohl sie keinen unmittelbaren wertschöpfenden Charakter besitzen, sind sie für den Gesamterfolg des Versicherungsunternehmens wichtig. Unterstützungsprozesse bilden oftmals erst die Voraussetzung für die Ausführung eines Kernprozesses.

- *Beschaffungsprozesse* stellen sicher, dass alle im Unternehmen benötigten Produktionsfaktoren in genau dem Umfang zur Verfügung stehen, wie sie für die Erstellung und Abwicklung der Kernprozesse (und der sonstigen, unterstützenden Prozesse) benötigt werden. Wesentliche Beschaffungsmärkte sind die Märkte für Arbeitskräfte, Dienstleistungen, Investitionsgüter, Software, Betriebsmittel und Finanzprodukte.
- Die *Verwaltungsprozesse* sind Prozesse, welche z. B. die Verwaltung des Personals, die Verwaltung der im Unternehmen vorhandenen Sachmittel und die Bereitstellung versicherungsfremder interner Dienstleistungen betreffen.
- Das *Rechnungswesen* enthält Teilprozesse mit einer wichtigen Rolle in der Erstellung der Jahresabschlüsse. Alle für den Jahresabschluss relevanten Ergebnisse aus den im

Unternehmen durchgeführten Prozessen werden hier buchungstechnisch abgebildet. Die Buchführung bildet zudem die Datenbasis für periodische Auswertungen oder Ad hoc- Auswertungen, außerdem für das Controlling sowie für Hochrechnungen und Bewertungsprozesse.

- Das *Dokumentenmanagement* Die Dokumente, welche innerhalb eines Versicherungsunternehmens verarbeitet werden, enthalten wichtige Informationen über einzelne Vorgänge innerhalb der Organisation, von den abgeschlossenen Verträgen mit Kunden bis zur Beschaffung von Sachmitteln, welche die verschiedenen Abläufe unterstützen. Das Dokumentenmanagement nimmt als integrierte Komponente im Zusammenspiel mit der elektronischer Archivierung eine zentrale Rolle in Versicherungsunternehmen ein.

Die Rolle der IT in der Ausführung der Geschäftsprozesse Die Effizienz aller Geschäftsprozesse im Bereich der Bestandsverwaltung hängt stark von der Unterstützung durch die IT ab. Die Antragsdaten aus dem Absatzprozess werden standardmäßig elektronisch in die Antrags- und Vertragssysteme der Bestandsführung überführt. Andere Folgeprozesse inklusive Policierung, Provisionsgutschrift und Inkasso laufen oft vollautomatisiert.

Die einzelnen Teilprozesse sowie deren Zuweisung zu den Sachbearbeitern werden durch Workflow-Systeme gesteuert, die häufig über Mechanismen zur dynamischen Lastverteilung und zur Einordnung in unterschiedliche Servicelevel verfügen. Solche prozesssteuernden Komponenten werden in fast allen Bereichen der Bestandsverwaltung und des Schadenmanagements verwendet. Typischerweise ist hieran ein Dokumentenmanagement inklusive optischer Archivierung gekoppelt, so dass im Zuge des Prozessablaufs extern neu hinzukommende Dokumente sowie durch den Prozess erstellte oder generierte Ergebnisdokumente zugeordnet und verknüpft werden können. Gleichzeitig wird ein elektronischer Zugriff auf relevante Dokumente gewährleistet. In allen Prozessen der Bestandsverwaltung ist das Dokumentenmanagement daher ein wichtiger Prozessbestandteil [15].

5.1.2 Struktur und Inhalt von MaRisk VA

Die *MaRisk VA* ist eine Verwaltungsvorschrift (siehe Diskussion über die Rechtsnatur von *MaRisk VA* in [48]) von nur 44 Seiten¹, welche die Grundlage der Umsetzung der *Solvency II* auf nationaler Ebene in Deutschland enthält. Sie gehört zur Kategorie der Verwaltungsrechts und beschreibt die Mindestanforderungen an das Risikomanagement in den Versicherungsunternehmen aus Deutschland. Die *MaRisk VA* präsentiert sich in tabella-

¹http://www.bafin.de/SharedDocs/Downloads/DE/Service/Rundschreiben/2009/rs_0903_mariskva,templateId=raw,property=publicationFile.pdf/rs_0903_mariskva.pdf (abgerufen am 14.04.2011)

rischer Form, wobei auf der linken Seite der verbindliche Teil des Gesetzes, und auf der rechten Seite ein Erläuterungsteil steht. Der Erläuterungsteil ist unverbindlich und enthält Empfehlungen, Definitionen und Erklärungen des linken Teils von *MaRisk VA*, sowie Beispiele zum Umgang mit den Anforderungen in der Praxis. Das Dokument enthält 10 Abschnitte, welche im Folgenden kurz vorgestellt werden.

Die Abschnitte 1-3 erklären das Ziel, den Anwendungsbereich und das Verhältnis des Rundschreibens zu den sonstigen Regelungen. Das Ziel von *MaRisk VA* ist die Verbindlichkeit von § 64a und § 104a VAG (siehe Abschnitt 2.1.1) für Versicherungsunternehmen festzulegen und basiert auf den Ansatz, dass die Geschäftsleiter eines Versicherungsunternehmens ein Risikobewusstsein entwickeln müssen, das stetig gelebt wird. Im Sinne der *MaRisk VA* umfasst das Risikomanagement:

- Die Festlegung einer angemessenen Risikostrategie,
- Die Schaffung adäquater aufbau- und ablauforganisatorischer Regelungen,
- Die Einrichtung eines angemessenen internen Steuerungs- und Kontrollsystems,
- Die Etablierung einer internen Revision und interner Kontrollen,
- Die adäquate und regelmäßige Information des gesellschaftsrechtlichen Aufsichtsorgans über die Risikosituation.

Abschnitt 4: Grundsatz der Proportionalität bedeutet, dass die Mindestanforderungen an das Risikomanagement immer unter der Berücksichtigung der unternehmensinternen Risiken, der Art und des Umfangs des Geschäftsbetriebes sowie der Komplexität des gewählten Geschäftsmodells zu erfüllen sind.

Abschnitt 5: Risiken beschreibt die Risiken, auf die sich das Schreiben bezieht. Der Begriff *Risiko* wird definiert und es werden die wesentlichen Risiken genannt, deren Management den Mindestanforderungen des Gesetzes genügen müssen. Die Beurteilung der Wesentlichkeit der Risiken wird durch die Geschäftsleitung vorgenommen. Diese Beurteilung findet innerhalb der Prozesse Risikoidentifikation, Risikoanalyse und -bewertung statt. Für die restlichen Risiken, die so genannten nicht wesentlichen Risiken, müssen angemessene Vorkehrungen getroffen werden. Die Risikokategorien, die berücksichtigt werden sollen, sind: versicherungstechnisches Risiko, Marktrisiko, Kreditrisiko, operationelles Risiko, Liquiditätsrisiko, Konzentrationsrisiko, strategisches Risiko, Reputationsrisiko.

Abschnitt 6: Gesamtverantwortung der Geschäftsleitung besagt, dass die Aufgabe der Einrichtung einer ordnungsgemäßen Geschäftsorganisation und der Einführung und Umsetzung eines funktionierenden Risikomanagements sowie dessen Weiterentwicklung, der Ge-

schäftsleitung obliegt. Risikomanagemententscheidungen liegen ebenfalls in der Verantwortung der Geschäftsleitung und sind nicht delegierbar.

Abschnitt 7: Elemente eines angemessenen Risikomanagements sind die Entwicklung einer Risikostrategie, welche auf die Unternehmensstrategie abgestimmt ist, die Beschaffung von organisatorischen Rahmenbedingungen, welche aus geeigneten aufbau- und ablauforganisatorischen Regelungen bestehen, ein geeignetes internes Steuerungs- und Kontrollsystem und eine funktionsfähige Interne Revision.

Abschnitt 8: Funktionsausgliederungen und Dienstleistungen regelt die Sicherstellung einer angemessenen Anbindung ausgelagerter Geschäftsaktivitäten und -prozesse in das Risikomanagement des Versicherungsunternehmens; auch in diesem Fall ist dafür die Geschäftsleitung verantwortlich.

Abschnitt 9: Notfallplanung besteht aus der Festlegung von Verfahren für die Fortführung der Geschäftstätigkeit in Störfällen, Notfällen und Krisen und Planung für den Schutz der Personen, Sachen und Vermögen. Sie ist regelmäßig zu überprüfen und muss allen Geschäftsbereichen zur Kenntnis gebracht werden.

Abschnitt 10: Information und Dokumentation beschreibt die Voraussetzung der Information der Entscheidungsträger, damit das Risikomanagement wirksam ist. Durch die MaRisk erfolgt eine grundlegende Neuregelung der qualitativen Finanzaufsicht.

Die MaRisk stellt die Versicherungswirtschaft vor eine Vielzahl von Herausforderungen, die nicht nur als Belastung sondern vielmehr als Maßnahme zum Vertrauensgewinn betrachtet werden sollen. Die frühzeitige Auseinandersetzung mit dem Risikomanagementsystem kann zudem für jeden Versicherer bereits heute, vor dem Hintergrund von *Solvency II*, entscheidende Wettbewerbsvorteile generieren.

5.2 Abbildung von MaRisk VA auf IT-Security-Policies

Das direkte Objekt von *MaRisk VA* ist ein einziger Geschäftsprozess aus dem Versicherungsunternehmen: das Risikomanagement. Die Abbildung dieses Gesetzes, dessen Schwerpunkt nicht die IT-Security ist, auf IT-Security-Policies, setzt eine detaillierte Analyse und Interpretation des Textes voraus, damit die direkten und die indirekten Hinweise auf die IT-Security-Ziele diesem entnommen werden können, um sie dann weiter zu IT-Security-Policies verarbeiten zu können.

Die Notwendigkeit eines neuen Konzeptes Die im Kapitel 4 beschriebenen Ansätze zur Analyse des juristischen Textes sind für das Ziel der aktuellen Arbeit wenig geeignet. Eine Formalisierung von *MaRisk VA* durch prädikatenlogische Formeln, durch Ontologien, oder die Darstellung des Textes mit Hilfe von Markup-Sprachen wie XML könnte zur Festlegung der logischen Beziehungen oder zur strukturierten Darstellung des Textes beitragen, mit dem Zweck, die Navigation und das Information Retrieval innerhalb dessen zu vereinfachen. Die *semantic-parameterization*-Methode eignet sich zur systematischen Identifizierung und automatischen Extrahierung der Pflichten und Rechte aus dem Text; im Fall dieser Diplomarbeit hilft das Verfahren nicht weiter zur Erstellung der IT-Security-Policies. Die Grenze aller dieser Methoden zur Analyse des juristischen Textes besteht darin, dass kein Schwerpunkt auf die Aspekte der IT-Security gesetzt wird. Um IT-Security-Policies auf Basis eines juristischen Textes wie die *MaRisk VA* zu erstellen, bedarf es einer Analyse, Interpretation und Untersuchung der Möglichkeit einer Abbildung zwischen zwei Domänen, welche sich voneinander unterscheiden: Recht und IT-Security. Die Modellierungs- und die Erhebungskomponente aus [40] sind für die Analyse der regulatorischen Texte geeignet, allerdings eignen sie sich zur Anwendung auf juristische Texte, dessen Objekt die Compliance mit den Anforderungen an die IT-Security ist und viele Hinweise auf die IT-Security-Ziele enthalten. Die Anwendung des Frameworks aus [40] auf einen Text wie *MaRisk VA*, welches das Risikomanagement, und nicht die IT-Security in Versicherungsunternehmen regelt, würde relevante Aspekte der IT-Security vernachlässigen.

Daher wurde im Rahmen dieser Diplomarbeit ein Verfahren entwickelt, das sich auf alle Arten von regulatorischen Texten anwenden lässt, mit dem Ziel, IT-Security-Policies aus solchen Texten abzuleiten. Das in dieser Diplomarbeit erzielte Ergebnis wird in der Abbildung 5.1 schematisch dargestellt: der Spezialist, dessen Aufgabe es ist, IT-Security-Policies aus der *MaRisk VA* abzuleiten, hat den regulatorischen Text *MaRisk VA* in der Hand; die Versicherungsunternehmen müssen mit der *MaRisk VA* compliant sein; innerhalb eines Versicherungsunternehmens finden mehrere Geschäftsprozesse statt, darunter auch das Risikomanagement; die *MaRisk VA* regelt nur einen Geschäftsprozess aus dem Versicherungsunternehmen (durch blauen Pfeil dargestellt), und zwar das Risikomanagement; das Risikomanagement steuert Risiken aus allen anderen Geschäftsprozessen des Versicherungsunternehmens (durch schwarze Pfeile dargestellt); der IT-Security-Spezialist soll IT-Security-Policies direkt von der *MaRisk VA* ableiten, welche an die Geschäftsprozesse aus dem Versicherungsunternehmen adressiert sind (durch rote Pfeile dargestellt). Die Erstellung von IT-Security-Policies auf Basis von *MaRisk VA* setzt das Beantworten von zwei Fragen voraus:

1. Welche Compliance-Anforderungen aus der Menge aller Compliance-Anforderungen aus der *MaRisk VA* können auf IT-Security-Policies abgebildet werden?

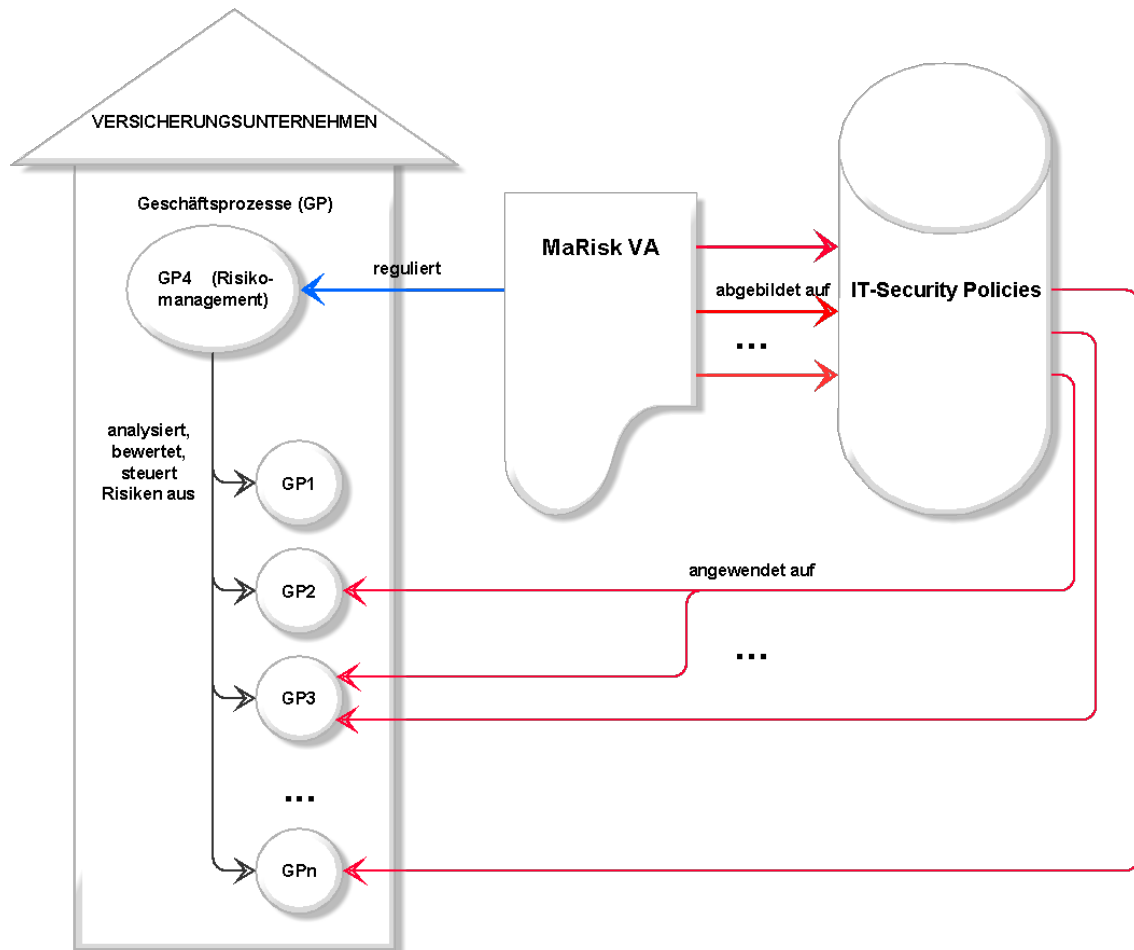


Abbildung 5.1: Vorgehen in der Diplomarbeit (rote Pfeile)

2. Wie kann die Abbildung der Compliance-Anforderungen aus dem Punkt 1. auf IT-Security-Policies durchgeführt werden?

Für die Beantwortung dieser Fragen wurde im Rahmen dieser Diplomarbeit das Konzept eines Frameworks zur Abbildung der regulatorischen Compliance auf IT-Security Policies entwickelt. Dieses Framework enthält zwei Komponenten, welche im Folgenden vorgestellt werden: die Analysekomponente und die Abbildungskomponente.

5.2.1 Die Analysekomponente

Die Compliance-Anforderungen aus den regulatorischen Texten werden nach ihrem Bezug auf IT-Security wie folgt klassifiziert:

1. Compliance-Anforderungen, welche keine expliziten Anforderungen an die IT-Security enthalten, aber deren IT-gestützte Erfüllung Anforderungen an die IT-Security mit sich bringt (siehe IT-gestützte Compliance im Abschnitt 2.2.1).

2. IT-Security-Anforderungen: dies sind explizite Anforderungen an die Einhaltung der IT-Security Ziele (siehe IT-Compliance im Abschnitt 2.2.2).
3. Andere Compliance Anforderungen.

Die Analyse-Komponente des Frameworks identifiziert die ersten zwei Kategorien von Compliance Anforderungen. Nur für diese Anforderungen wird mit der Abbildungskomponente untersucht, wie diese im Bezug zu den IT-Security-Zielen erfüllt werden können.

Die Analyse der *MaRisk VA* erfolgt in zwei Schritten: im ersten Schritt werden die Compliance Anforderungen aus dem Text identifiziert; innerhalb des zweiten Schrittes wird untersucht, ob die im ersten Schritt identifizierten Compliance-Anforderungen direkte Anforderungen an die IT-Security sind, oder ob ihre automatisierte Umsetzung mit Mitteln der IT Anforderungen an die IT-Security mit sich bringt.

I. Identifizierung der Compliance Anforderungen Die Elemente der Analysekomponente werden schematisch, mit Hilfe der UML-Notation, in der Abbildung 5.2 dargestellt. Der linke Teil der Abbildung zeigt, welche morphosyntaktischen Mittel der natürlich-juristischen Sprache in der *MaRisk VA* benutzt werden, um die Compliance Anforderungen auszudrücken. Diese Compliance Anforderungen werden identifiziert, indem die Aktivitätsverben aus dem Text gesucht und analysiert werden. Die Aktivitätsverben beschreiben nach [78] Verhalten oder Aktionen; dies wird in der Abbildung durch die Vererbungshierarchie Aktivität – Aktionsverb und Aktivität– Verhaltensverb dargestellt. Diese Vorgehensweise basiert auf der Theorie aus [84], welche besagt, dass das Verb, auf morphosyntaktischer Ebene, die Haupteinheit der Phrase ist, und alle anderen Konstrukte sich um das Verb gruppieren : der/die Akteure (welche die durch das Verb ausgedrückte Aktivität ausführen), das/die Objekte der Aktivität, das Instrument, mit welchem die Aktivität durchgeführt wird, der Zweck der Aktivität, die Ausnahmen bei der Durchführung der Aktivität und Bedingungen für die Durchführung der Aktivität. Die Abhängigkeit solcher Konstrukte vom Verb wird im linken Teil der Abbildung 5.2 durch Aggregationskanten dargestellt.

Aus semantischer Sicht ist eine Compliance Anforderung die Konkretisierung eines gesetzlichen Konzeptes aus der im Kapitel 5.2.1 vorgestellten Taxonomie von Hohfeld. Die gesetzliche Natur der Compliance Anforderungen aus der *MaRisk VA* wird in dem rechten Teil der Abbildung dargestellt. Die durchgeführte Untersuchung von MaRisk im Rahmen dieser Diplomarbeit hat drei der acht gesetzlichen Konzepte nach Hohfeld identifiziert: Pflichten, Verbote und Erlaubnisse. Diese Semantik der Compliance Anforderungen wird in der Abbildung durch die Vererbung Typ – Pflicht, Typ – Verbot und Typ – Erlaubnis dargestellt. Die Pflichten, die Verbote und die Erlaubnisse beziehen sich auf die Aktivitäten aus dem linken Teil der Abbildung (siehe die rote gestrichelte Linie A). Modale Konstrukte

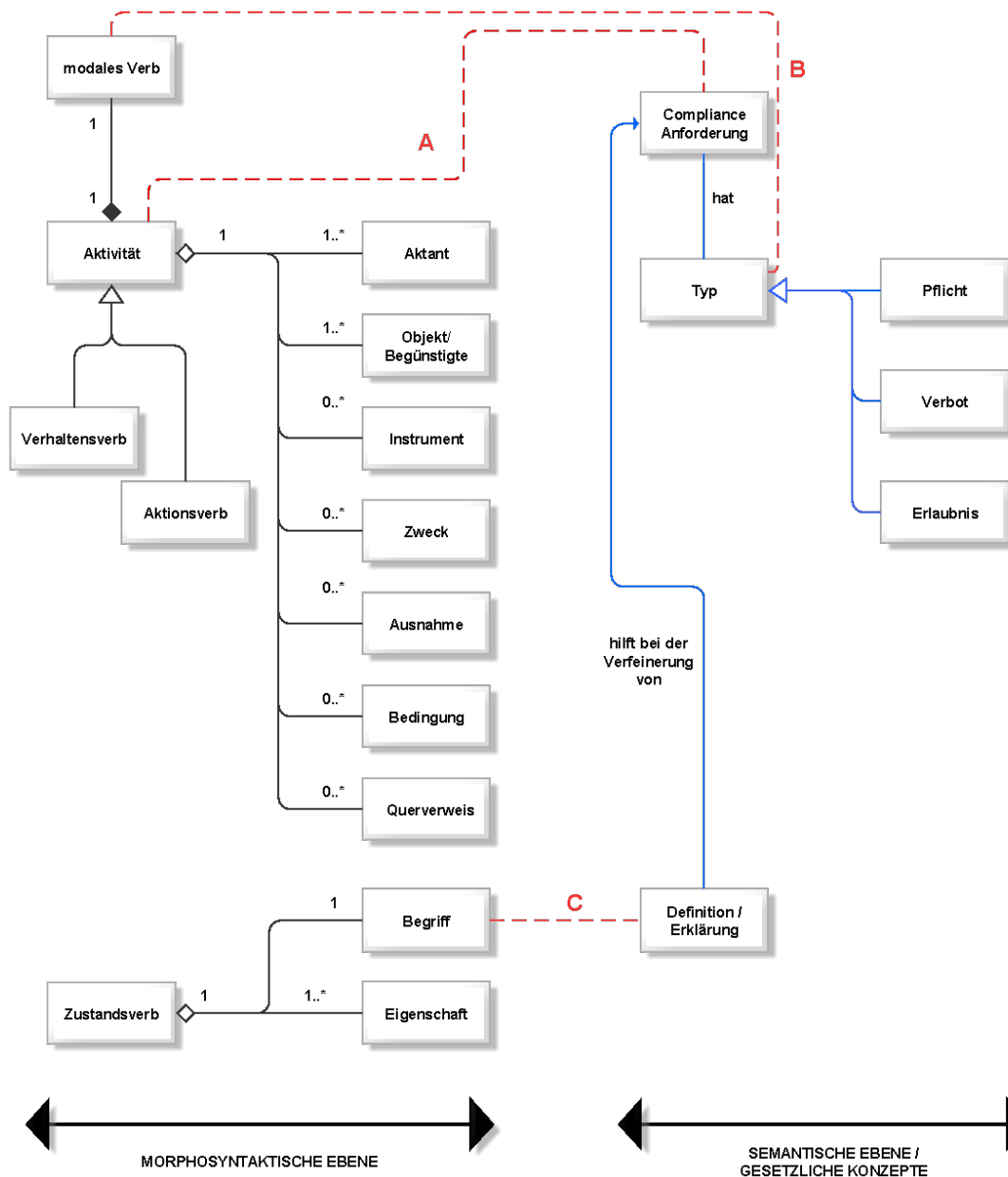


Abbildung 5.2: Elemente bei der Analyse der Compliance Anforderungen.

entscheiden, ob die genannte Aktivität eine Pflicht, ein Verbot oder eine Erlaubnis ist (siehe gestrichelte rote Linie B). In der MaRisk werden folgende modale Konstrukte benutzt:

1. Um Pflichten auszudrücken, werden verbale Konstrukte wie: *hat/haben zu* + Aktivitätsverb; *ist/sind zu* + Aktivitätsverb, *muss/müssen* + Aktivitätsverb benutzt. Beispiele:

„Es *muss* sichergestellt sein, dass auch auf Gruppen- bzw. Konglomeratsebene im Rahmen einer ordnungsgemäßen Geschäftsorganisation ein angemessenes Risikoma-

nagement vorhanden ist.“ (2. Anwendungsbereich, Seite 5/44)

„Die Anforderungen des §64a und des §104s VAG sowie die Mindestanforderungen dieses Rundschreibens *sind* unter Berücksichtigung des Grundsatzes der Proportionalität *zu* erfüllen.“ (4. Grundsatz der Proportionalität, Seite 7/44)

„Die Geschäftsleitung *hat* sowohl die Geschäftsstrategie als auch die Risikostrategie mindestens einmal im Geschäftsjahr *zu* überprüfen und ggf. anzupassen.“ (7.1 Risikostrategie, Seite 10/44)

2. Verbote werden durch die Negierung des Verbes *dürfen* + Aktivitätsverb ausgedrückt. Beispiel:

„Anreizsysteme *dürfen nicht* manipulierbar sein.“ (7.2.2 Betriebliche Anreizsysteme und Ressourcen, Seite 20/44)

3. Erlaubnisse werden mit Hilfe der Verbes *dürfen* und *können* + Aktivitätsverb ausgedrückt. Beispiel:

„Die teilweise oder vollständige Ausgliederung von Funktionen oder Dienstleistungen *darf* nur unter Maßgabe der in § 64a Abs. 4 VAG niedergelegten Grundsätze erfolgen.“ (8. Funktionsausgliederungen und Dienstleistungen im Sinne des § 64a Abs. 4 VAG, Seite 41/44)

Zusätzlich zu den Aktivitäten gibt es in der MaRisk noch Definitionen oder Erklärungen von Begriffen, sowie Erklärungen der tatsächlichen Compliance Anforderungen. Diese werden mit Hilfe von Zustandsverben (*sein, bestehen aus, bedeuten* usw.) ausgedrückt und tragen zum Verständnis und zur Verfeinerung der Compliance Anforderungen bei (siehe rote gestrichelte Linie C). Erklärungen gibt es besonders im rechten, unverbindlichen Teil des Textes. Als Beispiel dafür wird hier der folgende Abschnitt, der im rechten Teil von 7.2.2.2 Betriebliche Anreizsysteme und Ressourcen vorkommt, genannt:

„Als zur Verfügung gestellte Mittel kommen u.a. Budgets, qualifiziertes Personal und die technische Ausstattung in Betracht. Der jeweilige Verantwortliche ist z. B. der Leiter der Organisationseinheit. Beispiel: Wenn in den innerbetrieblichen Leitlinien eine wöchentliche Berichterstattung aller Geschäftsbereiche verankert wird, aber das IT-System nur eine monatliche Berichterstattung technisch zulässt, sollte dies der Geschäftsleitung berichtet werden.“

Gesetzliche Akteure Die Geschäftsleitung ist für die Umsetzung und Erfüllung aller Compliance Anforderungen aus der *MaRisk VA* insgesamt verantwortlich. Zuständig

für einzelne Compliance-Aktivitäten sind gemäß der *MaRisk VA* die folgenden Personen/Bereiche aus dem Versicherungsunternehmen:

- Der Geschäftsleiter / die Geschäftsleitung,
- Die unabhängige Risikocontrollingfunktion,
- Die operativen Geschäftsbereiche,
- Die interne Revision,
- Fachlich und technisch für IT-Systeme zuständige Mitarbeiter.

Diese Zuständigkeiten sind bei der Formulierung der IT-Security-Policies in der Abbildungskomponente zu beachten.

Querverweise In Kapitel 3 wurde gezeigt, dass die Querverweise häufig im Gesetzestext vorkommen. Dieser Aspekt wird in der Abbildung 5.2 durch die Aggregationskante von *Querverweis* zu *Aktivität* dargestellt. Diese Aggregation besagt, dass, wenn eine Compliance-Aktivität beschrieben wird und ein Querverweis angegeben wird, die Aktivität nur dann vollständig und korrekt verstanden werden kann, wenn der Querverweis verfolgt und mit Hilfe des hier vorgestellten Frameworks analysiert wird. In der *MaRisk VA* gibt es direkte Hinweise auf die *VAG*, auf die *Richtlinie 2002/87/EG*, das *IT-Grundschriftbuch des Bundesamtes für Sicherheit in der Informationstechnik*, auf den internationalen Security-Standard *ISO/IEC 27002* sowie auf das *HGB*.

Ambiguitäten in der MaRisk VA Im Kapitel 3 wurde erwähnt, dass die Ambiguitäten eine Schwierigkeit bei dem Verständnis und der Analyse des juristischen Textes darstellen. Auch die *MaRisk VA* enthält Ambiguitäten, deren Interpretation entscheidend bei der Festlegung der Compliance Anforderungen ist. Einige Beispiele von Ambiguitäten aus der *MaRisk VA* sind:

- Der Begriff *Wesentlichkeit*, welcher in der *MaRisk VA* eine wichtige Rolle spielt, beschreibt Aspekte, die für das Institut bedeutend (wesentlich) sind: *wesentliche Risiken*, *wesentliche risikostrategische Vorgaben*, *wesentliche Mängel*, *wesentliche Fehler*, *wesentliche finanzielle Schäden*, *wesentliche Funktionen*, *wesentliche Aktivitäten*, *wesentliche Anpassungen* oder *wesentliche Veränderungen*. Da die Grenze zwischen Wesentlichem und Unwesentlichem nicht vorgegeben wird, sollte die Beurteilung der Wesentlichkeit vorsichtig durchgeführt werden.
- Die *Angemessenheit* und die *Eignung* sind auch Begriffe, die einer kontextabhängigen Interpretation bedürfen: *angemessenes Risikomanagement*, *angemessene Maßnahmen*, *angemessene Information und Dokumentation*, *angemessene Zeit*; *geeignete Anordnungen*, *geeignete Risikokennzahlen*.

- *Soll/ sollte*-Anforderungen: neben den gesetzlichen Konzepten von Pflicht, Verbot und Erlaubnis, welche „Muss-Vorschriften“ sind, beinhaltet die *MaRisk VA* auch einige „Sollte-Anforderungen“, welche im Sinne von Empfehlungen oder Zielvorgaben zu interpretieren sind. Beispiele hierfür sind: Die *Risikostrategie soll die sich aus der Geschäftsstrategie ergebenden Risiken darstellen [...] oder die Risikostrategie sollte an jedes Mitglied des Aufsichtsorgans berichtet werden.*
- *Grundsätzlich* ist ein Begriff, der oft in der *MaRisk VA* vorkommt und bedeutet, dass bestimmte Aussagen oder Anforderungen nur im Prinzip gelten und Ausnahmen zugelassen werden. Welche Ausnahmen von den Regeln zugelassen sind, wird im Text nicht konkretisiert. Beispiele dafür sind: *Grundsätzlich sollte die Risikostrategie an jedes Mitglied des Aufsichtsorgans berichtet werden, Grundsätzlich hat eine klare Funktionstrennung bis einschließlich der Ebene der Geschäftsleitung zwischen unvereinbaren Funktionen zu erfolgen.*
- Keine konkreten Zeitvorgaben, sondern Begriffe wie *unverzüglich* und *zeitnah*: *unverzüglich zu berichten, unverzüglich bekannt zu geben, unverzügliche Berichterstattung; zeitnah zu überprüfen und anzupassen, zeitnah mitzuteilen, zeitnah zu beseitigen* usw.

Solche Ambiguitäten in der *MaRisk VA* lassen Spielraum für Interpretationen und erschweren die Festlegung von konkreten Compliance Anforderungen, ohne den Kontext, durch ein konkretes Versicherungsunternehmen dargestellt, zu kennen.

II. Analyse der Anforderungen an die IT-Security Für jede im vorigen Schritt identifizierte Compliance Anforderung wird jetzt untersucht:

1. Ob es sich um eine direkte Anforderung an die IT-Security handelt: in diesem Fall wird nach Begriffen gesucht, welche im Zusammenhang mit der IT-Security stehen (lexikosemantische Analyse).
2. Ob bei der Erfüllung der untersuchten Compliance Anforderung oder bei deren automatisierter Umsetzung IT-Security Aspekte beachtet werden müssen (kontextuelle Analyse).

Lexikosemantische Analyse Diese Analyse identifiziert die Compliance Anforderungen an die IT-Security durch die Suche nach lexikosemantischen Hinweisen auf die IT-Security-Ziele im Text. Die im Rahmen dieser Diplomarbeit durchgeführte Untersuchung von *MaRisk VA* hat ergeben, dass es wenige direkte Anforderungen an die IT-Security in diesem Gesetz gibt. Das liegt daran, dass der Schwerpunkt von *MaRisk VA* nicht die IT-Security ist, sondern das Risikomanagement in Versicherungsunternehmen. Solche direkten, lexikosemantischen Hinweise auf die IT-Security-Ziele in der *MaRisk VA* – aus der

Sicht der aktuellen Interpretation, welche durch die lexikosemantische Analyse von *MaRisk VA* identifiziert werden können – sind z. B. in den folgenden Teilen von *MaRisk VA* enthalten:

7.2 Organisatorische Rahmenbedingungen Hier werden die Aufbau- und Ablauforganisation des Versicherungsunternehmens erklärt.

- Oft in diesem Abschnitt angedeutet ist die „klare Funktionstrennung [...] zwischen unvereinbaren Funktionen“, welche durch Mittel der IT umgesetzt werden können, z. B. durch rollenbasierte Zugriffskontrolle² (RBAC).
- „Vollständiges und uneingeschränktes Informationsrecht“ für die Risikokontrollfunktion weist auf die IT-Security-Ziele Verfügbarkeit der Information und Autorisierung hin.
- Die *MaRisk VA* enthält die Compliance Anforderung, dass die in dem Versicherungsunternehmen eingesetzten IT-Systeme und die zugehörigen IT-Prozesse die IT-Security-Ziele sicherstellen müssen. Im unverbindlichen rechten Teil von *MaRisk VA*, unter 7.2.2.2 Punkt 3 wird für die Behandlung der IT-Risiken als Leitfaden das *BSI-Grundschriftbuch* oder der Standard *ISO/IEC 27002* für die Umsetzung der IT-Security-Maßnahmen empfohlen.
- Gefordert wird auch, dass die IT-Systeme vor ihrem ersten Einsatz und nach Veränderungen getestet werden müssen.

7.3.5 Qualitätssicherung internes Steuerungs- und Kontrollsystem bezieht sich auf die Dokumentation der verwendeten Daten, Methoden und Verfahren des internen Steuerungs- und Kontrollsystems. Der Geschäftsprozess Dokumentation setzt den Umgang mit Information voraus, und wenn die Information mit Hilfe der IT verarbeitet und verwaltet wird, müssen die IT-Security Ziele berücksichtigt werden. Lexikosemantische Hinweise auf die IT-Security sind:

- „Die verwendeten Daten, Methoden und Verfahren [...] ggf. notwendige Modifizierungen sind [...] verständlich und nachvollziehbar zu validieren und zu dokumentieren“: Nachvollziehbarkeit und Dokumentation verlangen ein Konzept für die Auditierung verschiedener Vorfälle im Versicherungsunternehmen.
- „Der Validierungsprozess [...] hat insbesondere die kontinuierliche Zweckmäßigkeit, Angemessenheit, Qualität, Vollständigkeit und Wirksamkeit von Daten, Methoden und Verfahren nachzuweisen“: hier sind sowohl die Begriffe *Vollständigkeit*, als auch in

²Bei RBAC werden die Berechtigungen zur Nutzung geschützter Komponenten direkt an Rollen vergeben und es wird festgelegt, welche Subjekte welche Aufgaben durchführen [21].

diesem Kontext, *nachzuweisen* IT-Security relevant und verweisen auf die Notwendigkeit eines Konzeptes für die Auditierung und auf die Einhaltung der IT-Security-Ziele Verfügbarkeit und Integrität.

7.4 *Interne Revision* enthält Compliance Anforderungen, welche die Funktionstrennung und das Informationsrecht der Verantwortlichen für die interne Revision regeln.

- „Zur Wahrnehmung ihrer Aufgaben ist der internen Revision jederzeit ein vollständiges und uneingeschränktes Informations- und Prüfungsrecht einzuräumen“: der Begriff *Informationsrecht* weist auf die Verfügbarkeit und Integrität der Information hin.

Der Abschnitt *10 Information und Dokumentation* wird im nächsten Kapitel ausführlich behandelt.

Kontextuelle Analyse Dieser Schritt der Analysekomponente hat das Ziel, diejenigen Anforderungen an die IT-Security festzulegen, welche durch die Ausführung der Geschäftsprozesse aus dem Versicherungsunternehmen mit Hilfe der IT impliziert werden. Das Einbeziehen solcher IT-Security Aspekte, welche im Text nicht direkt ausgedrückt, aber durch die automatisierte Ausführung der Geschäftsprozesse impliziert werden, stellt eine präventive Maßnahme bei der Planung und Gestaltung der Geschäftsprozesse dar.

Jede in der Phase *Identifizierung der Compliance Anforderungen* der Analysekomponente festgelegte Compliance Anforderung wird wie folgt untersucht:

- An welchen Geschäftsprozess oder welche Aktivität aus dem Versicherungsunternehmen richtet sich die Compliance Anforderung?
- Wenn der Geschäftsprozess oder die Aktivität automatisiert durchgeführt wird, kann auch die zugehörige Compliance Anforderung automatisiert durchgeführt werden?
- Wenn eine Automatisierung der Geschäftsprozesse oder der Aktivitäten mit Hilfe der IT durchgeführt wird, welche sind die IT-Security Aspekte, die in diesem Fall zusätzlich beachtet werden müssen?

Diese Art von Untersuchung lässt sich nicht nur mit Hilfe des Textes der *MaRisk VA* durchführen. Die Kenntnis des Kontextes, der durch ein konkretes Versicherungsunternehmen und durch konkrete zur Verfügung stehende Mittel der IT dargestellt wird, wird darüber hinaus benötigt. Für die kontextuelle Analyse eignen sich folgende Abschnitte aus der *MaRisk VA*:

8 *Funktionsausgliederungen und Dienstleistungen im Sinne des §64a Abs.4 VAG*: im Fall des Outsourcings müssen z. B. Datenschutzmaßnahmen in Betracht gezogen werden, auch

wenn solche Maßnahmen im Text nicht explizit genannt werden.

9 *Notfallplanung* enthält keine direkten Anforderungen an die IT-Security; die Notfallplanung wird für die Fälle, in denen die Kontinuität der wichtigsten Unternehmensprozesse nicht mehr gewährleistet ist, und für alle Güter des Versicherungsunternehmens durchgeführt. Die IT-Systeme stellen einen Teil dieser Güter dar. Die Notfallplanung für die IT-Systeme kann z. B. nach den Empfehlungen aus den *BSI-Grundschutz-Katalogen* gemacht werden. Der Baustein *B 1.3 Notfallmanagement* aus diesem Leitfaden beschreibt Notfälle, welche die Kontinuität von Geschäftsprozessen beeinträchtigen und schlägt ausführliche Maßnahmen für die Prävention und für die Beseitigung vor (siehe [39], Seite 68-70).

Die Überwachung von Risiken und Einhaltung von Limiten, welche in der *MaRisk VA* oft als Anforderung vorkommt, z. B. in *7.2.1 Aufbauorganisation* (Seite 16/44), *7.3.1 Risikotragfähigkeitskonzept und Limitierung* (Seite 23/44), wenn sie mit Hilfe der IT-Mittel automatisiert durchgeführt wird, setzt die Einhaltung der IT-Security Ziele voraus.

Wenn neue Geschäftsfelder in das Versicherungsunternehmen aufgenommen werden, wie in *7.2.2.1 Neue Geschäftsfelder sowie Kapitalmarkt-, Versicherungs- und Rückversicherungsprodukte* (Seite 20/44) erwähnt, muss untersucht werden, welche Auswirkungen und welche neuen Anforderungen an die IT-Systeme dadurch impliziert werden.

Das Ergebnis der Anwendung der Analysekomponente auf die *MaRisk VA* ist eine Menge von Anforderungen an die IT-Security, welche direkt dem Text durch lexikosemantische Analyse entnommen werden, zusammen mit Anforderungen an die IT-Security, welche durch die automatisierte Ausführung der Geschäftsprozesse mit Hilfe der IT-Mittel impliziert werden. Diese Anforderungen an die IT-Security werden weiter mit der Abbildungskomponente bearbeitet.

5.2.2 Die Abbildungskomponente

Mit der Abbildungskomponente des Frameworks werden IT-Security-Policies von denjenigen Anforderungen an die IT-Security, welche mit der Analysekomponente identifiziert wurden, erstellt.

Die Abbildungskomponente enthält folgende Schritte:

1. Wenn die IT-Security Anforderungen durch die lexikosemantische Analyse identifiziert wurden, so werden die Geschäftsprozesse und Aktivitäten, an welche sich diese Anforderungen richten, weiter berücksichtigt.

2. Wenn die automatisierte Ausführung von Aktivitäten und Geschäftsprozessen Anforderungen an die IT-Security mit sich bringt, was durch die kontextuelle Analyse festgelegt wird, so werden diese Geschäftsprozesse und Aktivitäten weiter berücksichtigt.
3. Für jede IT-Security Anforderung aus 1. wird untersucht, welches IT-Security-Ziel erfüllt werden muss.
4. Für jede Aktivität aus 2. wird untersucht, welches IT-Security-Ziel im Fall der automatisierten Durchführung erfüllt werden muss.
5. Für die Visualisierung der durch 1. und 2. festgelegten Aktivitäten und Geschäftsprozesse des Versicherungsunternehmens kann ein Modellierungstool (z. B. ARIS³ oder ADONIS⁴) benutzt werden.
6. Für jedes IT-Security-Ziel aus 2. und 3. werden, abhängig von der durchgeführten Aktivität, die Gefährdungen/die IT-Security Risiken an dieses IT-Security Ziel identifiziert. Für die Visualisierung dieser Gefährdungen kann z. B. das Tool ARIS verwendet werden. Dieses Tool bietet die Möglichkeit, ereignisgesteuerte Prozessketten (EPK) mit Berücksichtigung der Risiken zu modellieren.
7. Gegen jede in 6. identifizierte Gefährdung werden IT-Security-Maßnahmen formuliert. Diese IT-Security Maßnahmen sind die IT-Security-Policies, welche auf Basis von *MaRisk VA* erstellt werden. In dem Abschnitt 2.3 wurde beschrieben, dass die Erstellung der IT-Security-Policies ein inkrementelles Verfahren ist, welches mit dem Verfassen von informellen IT-Security-Policies beginnt. Die Formulierung von IT-Security-Policies auf Basis eines Textes mit einem sehr hohen Abstraktionsgrad wie die *MaRisk VA* erfolgt auf einer informellen Ebene. Erst bei der Anwendung der Policies in konkreten Versicherungsunternehmen werden diese, abhängig von der technischen Ausstattung und auch von der Geschäftsstrategie, verfeinert und, wenn möglich, automatisiert durchgesetzt.

Für die Identifizierung der Gefährdungen in 6. und für die Formulierung der Maßnahmen in 7. werden in dieser Diplomarbeit die *BSI-Grundschutz-Kataloge*, benutzt, welche im Abschnitt 2.3.3 beschrieben wurden. Dieser IT-Security Leitfaden bietet den Vorteil, dass seine Strukturierung für das hier dargestellte Vorgehen in der Abbildung der regulatorischen Compliance aus IT-Security-Policies gut geeignet ist: in den *BSI-Grundschutz-Katalogen* werden sowohl die Gefährdungen an die IT-Security innerhalb einer Organisation als auch die Maßnahmen gegen solche Gefährdungen ausführlich mit Beispielen dargestellt. Auch die

³http://www.softwareag.com/ch/products/aris_platform/default.asp (abgerufen am 26.04.2011)

⁴http://www.adonis-community.com/geschaeftsprozessmanagement_tool.html (abgerufen am 26.04.2011)

Tatsache, dass die *BSI-Grundschutz-Kataloge* aus dem deutschsprachigen Raum stammen und kostenlos zur Verfügung stehen, oder die Möglichkeit der *ISO-27001*-Zertifizierung der Organisationen auf der Basis von IT-Grundschutz können als Vorteile betrachtet werden.

Gesetzliche Akteure und IT-Security Verantwortliche Für die Umsetzung und Einhaltung der Compliance Anforderungen aus der *MaRisk VA* sind, wie bereits bei der Vorstellung der Analysekomponente diskutiert, die Geschäftsleitung, die unabhängige Risikocontrollingfunktion, die operativen Geschäftsbereiche, die interne Revision und die fachlich und technisch für IT-Systeme zuständigen Mitarbeiter verantwortlich. Die Erstellung, Durchsetzung und Überwachung der IT-Security-Policies fällt in den Aufgabebereich der letzteren. Bei der Konkretisierung der Funktionen im IT-Bereich helfen die *BSI-Grundschutz-Kataloge*: im Kapitel 3, *Rollen*, werden unter Anderem sowohl die IT-Verantwortlichen, als auch ihr Aufgabengebiet vorgestellt.

5.3 Zusammenfassung

In diesem Kapitel wurde das Konzept eines Frameworks für die Abbildung der regulatorischen Compliance auf IT-Security-Policies vorgestellt. Dieser Framework enthält zwei Komponenten: die Analysekomponente und die Abbildungskomponente. Diese Komponenten haben die Rolle, die Abstraktion der juristischen Sprache zu überwinden und dem Text die direkten und indirekten Anforderungen an die IT-Security zu entnehmen. Diese IT-Security-Anforderungen werden mit den Geschäftsprozessen in Verbindung gebracht, auf welche sie anzuwenden sind. Mit Hilfe der *BSI-Grundschutz-Kataloge* werden die Gefährdungen der IT-Security Ziele identifiziert, welche durch die IT-Security Anforderungen adressiert werden. Die Maßnahmen-Kataloge aus demselben IT-Security Leitfadens werden benutzt, um IT-Security-Policies zu formulieren. Im nächsten Kapitel wird der vorgestellte Framework auf einen Abschnitt aus der *MaRisk VA* angewendet.

Kapitel 6

Anwendung des Frameworks

In diesem Kapitel wird das im Rahmen dieser Diplomarbeit entwickelte Konzept zur Abbildung der regulatorischen Compliance auf IT-Security-Policies auf den Abschnitt *10 Information und Dokumentation* (siehe Tabelle 6.1 auf der Seite 64) aus der *MaRisk VA* angewendet. Die linke Seite des Abschnittes enthält den verbindlichen Teil von *MaRisk VA*. In diesem Fall geht es um die Anforderungen an die Information und Dokumentation innerhalb des Versicherungsunternehmens. Der rechte Teil stellt den unverbindlichen Teil dar, in welchem die Anforderungen aus dem linken Teil erklärt werden.

6.1 Anwendung der Analysekomponente

6.1.1 Identifizierung der Compliance Anforderungen

Die Identifizierung der Compliance Anforderungen beginnt mit der Suche nach Verben, welche Aktivitäten ausdrücken. In Abschnitt 10 von *MaRisk VA*, in dem verbindlichen Teil des Textes, gibt es folgende Aktivitäten:

- Um das Verhalten auszudrücken: *zur Verfügung stehen, nachvollziehbar sein, überprüfbar sein,*
- Um Aktionen auszudrücken: *steuern, festlegen, aufzeichnen, kommunizieren.*

Weiter werden die modalen Konstrukte analysiert, welche über die juristische Natur der Aktivitäten entscheiden.

- Das Verb *müssen* begleitet die Aktivitäten *zur Verfügung stehen* und die verbalen Formen *nachvollziehbar sein* und *überprüfbar sein*.
- Die modalen Formen *ist zu/ sind zu* begleiten die Aktivitäten *festlegen, aufzeichnen* und *kommunizieren*.

10 Information und Dokumentation	
<p>Alle für die Funktionsfähigkeit des Risikomanagements wesentlichen Informationen müssen den Entscheidungsträgern exakt und vollständig zur Verfügung stehen. Wie gesteuert werden soll, ist in Abstimmung mit der Strategie des Unternehmens festzulegen. Hinsichtlich der Dokumentation gelten die Anforderungen des § 64a Abs. 3 VAG. Die Dokumentation umfasst alle wesentlichen Formeln, Parameter, Methoden, Verfahren, Handlungen, Festlegungen, Entscheidungen und ggf. Begründungen sowie festgestellten Mängel und daraus gezogene Schlussfolgerungen. Wesentliche unterjährige Änderungen sind aufzuzeichnen und zeitnah innerhalb des Unternehmens zu kommunizieren. Die Dokumentation muss für sachverständige Dritte nachvollziehbar und überprüfbar sein.</p>	<p>Für das Risikomanagement in der Versicherungswirtschaft kommen eine Vielzahl von Daten und Informationen aus den verschiedensten betrieblichen Teilfunktionen und wissenschaftlichen Disziplinen infrage, z. B.</p> <ul style="list-style-type: none"> - Vertrieb - Interne und externe Rechnungslegung - Unternehmensplanung, -entwicklung und -bewertung - Datenarchivierung und -sicherung - Asset Management, inklusive Kapitalmarktinformationen - Tarifierung, Produktentwicklung, Aktuariat - Schadensmanagement - Versicherungstechnische Bestandsführung - Mathematisch-statistische Verfahren <p>Die Dokumentation soll einen systematischen Überblick über Risiken, Prozesse und Kontrollen geben. Die hier geschilderte Dokumentationspflicht stellt aus Sicht der Aufsicht keine abschließende Liste für den gem. § 55c VAG zu erstellenden Risikobericht dar, sondern benennt die Felder, die als Minimum dokumentiert werden müssen.</p>

Tabelle 6.1: 10 Information und Dokumentation aus der *MaRisk VA*.

Die Semantik dieser modalen Konstrukte weist auf die Pflichten aus der Taxonomie von Hohfeld. So enthält der Abschnitt 10 aus der *MaRisk VA* die folgenden Pflichten als Compliance Anforderungen:

1. Die wesentlichen Informationen für die Funktionsfähigkeit des Risikomanagements *müssen* den Entscheidungsträgern exakt und vollständig *zur Verfügung stehen*.
2. Die Strategie des Unternehmens *[muss]* Einzelheiten darüber enthalten, wie die wesentlichen Informationen zur Verfügung gestellt werden.
3. Wesentliche unterjährige Änderungen *sind* aufzuzeichnen.

4. Wesentliche unterjährige Änderungen *sind* zeitnah innerhalb des Unternehmens zu kommunizieren.
5. Die Dokumentation *muss* für sachverständige Dritte nachvollziehbar sein.
6. Die Dokumentation *muss* für sachverständige Dritte überprüfbar sein.

Weitere Erklärungen in Abschnitt 10 aus der *MaRisk VA* zeigen, aus welchen Informationen die Dokumentation innerhalb des Versicherungsunternehmens besteht (wesentliche Formeln, Parameter, Methoden, Verfahren, Handlungen, Festlegungen, Entscheidungen, Begründungen usw.) und für welche Bereiche diese Informationen zur Verfügung gestellt werden müssen (Vertrieb, interne und externe Rechnungslegung, Unternehmensplanung, -entwicklung, -bewertung, Datenarchivierung und -sicherung, usw.)

Querverweise Der verbindliche Teil von *10 Information und Dokumentation* enthält einen Querverweis auf § 64a Abs.3 VAG. Das Schema für diesen Querverweis wird in der Abbildung 6.1 auf Seite 66 dargestellt. Um vollständige Anforderungen an die IT-Security aus dem Abschnitt 10 der *MaRisk VA* gewinnen zu können, müssen auch die Compliance Anforderungen aus dem VAG, HGB, Wertpapierhandelsgesetz (*WpHG*), Wertpapiererwerbs- und Übernahmegesetz (*WpÜG*), Investmentgesetz, und aus der Richtlinie 2004/39/EG mit der Analysekomponente untersucht werden. Der unverbindliche rechte Teil des untersuchten Abschnittes enthält den Querverweis § 55c VAG, dessen Objekt der verpflichtende Risikobericht des Versicherungsunternehmens ist.

Ambiguitäten Die Verwendung des modalen Verbes *sollen* in der rechten Spalte von *10 Information und Dokumentation*: „Die Dokumentation *soll* einen systematischen Überblick über Risiken, Prozesse und Kontrollen geben“ ist ambig, denn, obwohl in dem unverbindlichen Teil des Abschnittes 10 von *MaRisk VA*, kann diese Empfehlung als Compliance Anforderung an die Dokumentation interpretiert werden. In der aktuellen Analyse wird diese Empfehlung als Pflicht betrachtet.

6.1.2 Analyse der Anforderungen an die IT-Security

Lexikosemantische Analyse Für jede Compliance Anforderung aus dem vorigen Schritt wird untersucht, ob diese direkte Anforderungen an die IT-Security enthält. Die direkten Anforderungen werden durch Begriffe mit Bezug auf die IT-Security dargestellt.

„Die wesentlichen Informationen für die Funktionsfähigkeit des Risikomanagements müssen den Entscheidungsträgern exakt und vollständig zur Verfügung stehen.“ Diese Compliance Anforderung enthält drei Begriffe, welche mit der IT-Security in Zusammenhang stehen:

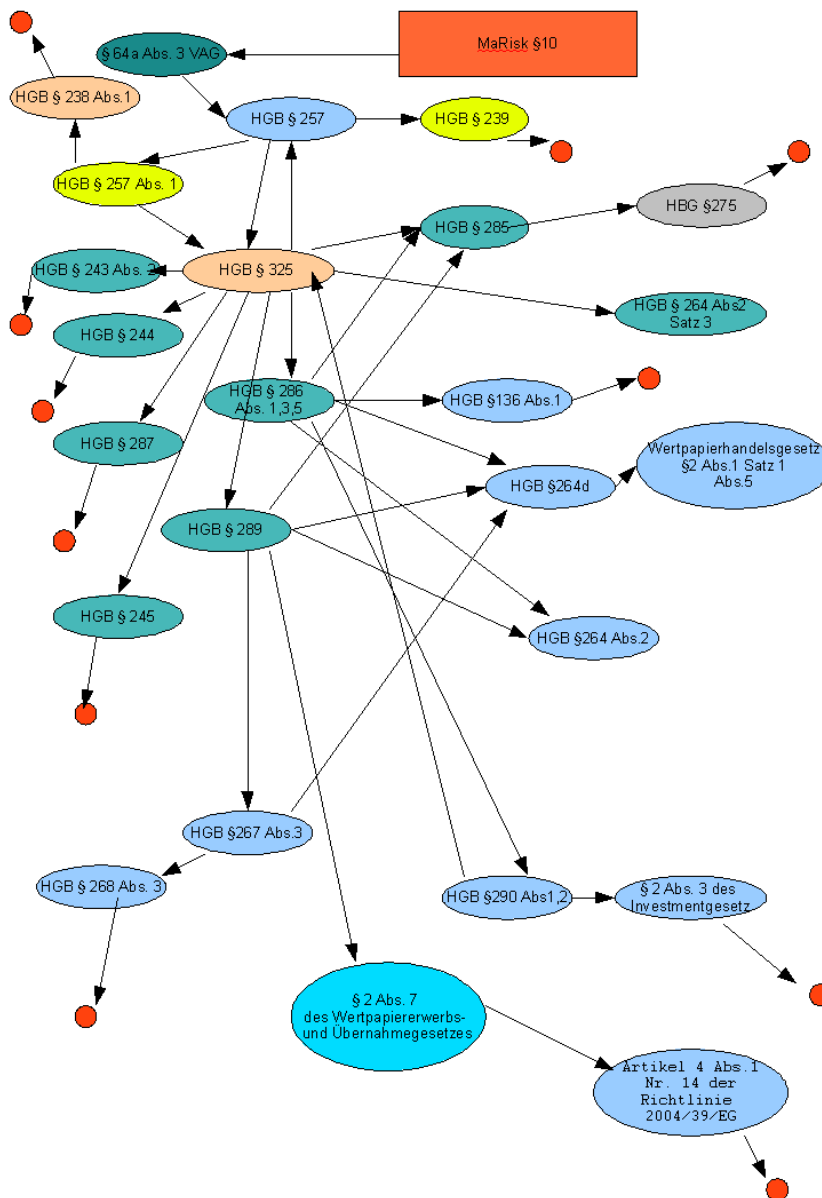


Abbildung 6.1: Querverweis § 64a Abs.3 VAG aus 10 Information und Dokumentation von MaRisk VA.

Informationen, *exakt zur Verfügung stehen* und *vollständig zur Verfügung stehen*. Innerhalb eines Unternehmens ist die Erstellung und Verwaltung der Dokumentation ein Teil der Informationspolitik. *Exakte* Information bedeutet, dass das IT-Security-Ziel Integrität erfüllt werden muss, und *vollständige* Information bedeutet, dass alle relevanten Abläufe innerhalb eines Unternehmens aufgezeichnet werden müssen.

„Wesentliche unterjährige Änderungen sind aufzuzeichnen.“ Die relevanten Begriffe mit

Bezug auf die IT-Security im Fall dieser Compliance Anforderung sind *Änderungen* und *aufzeichnen*. Die Aufzeichnung der Änderungen der wesentlichen Informationen für das Risikomanagement ist nur dann möglich, wenn im Fall der elektronischen Dokumentenverfassung ein Audit-System zur Verfügung steht. Dieses Audit-System protokolliert, wer wann auf welche Information und auf welche Art (lesend, schreibend, ausführend) zugegriffen hat.

„Wesentliche unterjährige Änderungen sind zeitnah innerhalb des Unternehmens zu kommunizieren.“ Der Begriff *kommunizieren* ist in diesem Fall ambig, weil die Art der Kommunikation innerhalb des Versicherungsunternehmens nicht spezifiziert wird. Angenommen, die Kommunikation solcher Änderungen und die Kommunikation im Allgemeinen findet per E-Mail statt, so muss eine geeignete Infrastruktur zur Verfügung gestellt werden.

„Die Dokumentation muss für sachverständige Dritte nachvollziehbar sein.“ Aus der Sicht des IT-Security Spezialisten könnte *nachvollziehbar* bedeuten, dass jedes verfasste Dokument einem Mitarbeiter in dem jeweiligen Versicherungsunternehmen zugeordnet werden kann. Das bedeutet, dass das IT-Security Ziel Zurechenbarkeit in diesem Fall erfüllt sein muss. Die Dokumentation nachzuvollziehen kann nur unter der Voraussetzung stattfinden, dass diese Dokumentation verfügbar ist, dass sie nicht gefälscht wurde und dass sie vollständig ist. Dabei spielt die Auditierung der Zugriffe auf die Dokumente eine wichtige Rolle.

„Die Dokumentation muss für sachverständige Dritte überprüfbar sein.“ Wieder aus der Sicht des IT-Security Spezialisten kann *überprüfbar* bedeuten, dass jedes erstellte Dokument derjenigen Person, die es verfasst hat, zurechenbar ist, und jede Änderung der Dokumente protokolliert wird. Die Überprüfung der Dokumentation kann nur dann stattfinden, wenn eine Dokumentation über Dokumentation existiert, d.h., der Lebenszyklus eines Dokumentes verfolgt und aufgezeichnet wird und es bekannt ist, wann das Dokument erstellt, geändert oder vernichtet wurde und wer diese Aktionen durchgeführt hat.

„Die Dokumentation soll einen systematischen Überblick über Risiken, Prozesse und Kontrollen geben.“ In diesem Fall, gemäß der aktuellen Interpretation, enthält diese Compliance Anforderung keine Hinweise an die IT-Security.

Das Ergebnis der Analyse der Anforderungen an die IT-Security aus den Querverweisen hat als Ergebnis die folgenden IT-Security Aspekte:

§64a Abs.3 VAG besagt, dass die Dokumentation sechs Jahre aufzubewahren ist. Dies bedeutet für den Zeitraum dieser sechs Jahre, dass im Fall der elektronischen Dokumente Mechanismen zur Verfügung gestellt werden müssen, welche die Ziele der IT-Security er-

füllen; auch Konzepte für Datensicherung und Archivierung müssen erstellt werden.

HGB §238 Abs.1 besagt, dass „die Geschäftsvorfälle sich in ihrer Entstehung und Abwicklung verfolgen lassen müssen“. Um diese Anforderung zu erfüllen, wird ein Konzept für die Auditierung verschiedener Vorfälle im Unternehmen benötigt. *HGB §239* stellt Anforderungen sowohl an die Integrität eines Dokumentes: „eine Eintragung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, daß der ursprüngliche Inhalt nicht mehr feststellbar ist“, als auch an die Authentizität des Dokumentes: „solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiß läßt, ob sie ursprünglich oder erst später gemacht worden sind“.

HGB §239 gibt Vorschriften für die Aufbewahrung der Dokumente auf Datenträgern: „[...] muß insbesondere sichergestellt sein, daß die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können“. Das selbe Gesetz besagt außerdem, dass elektronische Dokumente ausgedruckt und im Papierform aufbewahrt werden können.

Kontextuelle Analyse In diesem zweiten Schritt der Analysekomponente wird untersucht, welche Aspekte der IT-Security berücksichtigt werden müssen, im Fall der IT-gestützten Umsetzung der oben genannten Compliance Anforderungen.

Die untersuchten Compliance Anforderungen wenden sich an den Geschäftsprozess *Dokumentieren*. Die Dokumentation ist integrierter Teil vieler Geschäftsprozesse aus den Versicherungsunternehmen, weil alle Geschäftsvorfälle nachvollziehbar und nachweisbar ausgeführt werden müssen.¹ Die Automatisierung mit Hilfe der IT spielt dabei eine wichtige Rolle (siehe Abschnitt 5.1.1). Aus diesem Grund müssen für die Dokumentation Mechanismen zur Verfügung gestellt werden, welche zur Erfüllung der IT-Security Ziele Verfügbarkeit, Integrität, Datensicherheit, Authentizität, Verbindlichkeit und Autorisation beitragen.

Die Ergebnisse der Analysekomponente werden in der Tabelle 6.2 auf der Seite 69 zusammengefasst. Die erste Spalte der Tabelle enthält die Namen der juristischen Texte, welche Anforderungen an die IT-Security stellen. Diese Anforderungen an die IT-Security befinden sich in der dritten Spalte.

¹Modelle für Geschäftsprozesse, welche den Teilprozess *Dokumentieren* enthalten, können in [23] nachgesehen werden

GESETZ	AKTIVITÄT/ GESCHÄFTS- PROZESS	IT-SECURITY ANFORDERUNG	IT- SECURITY- ZIEL
<i>MaRisk</i> VA §10	Information	vollständig	Verfügbarkeit
<i>MaRisk</i> VA §10	Information	exakt	Integrität
<i>MaRisk</i> VA §10	Dokument ändern	Änderung aufzeichnen	Autorisation Verbindlichkeit Authentifikation
<i>MaRisk</i> VA §10	Dokumentation	nachvollziehbar	Verbindlichkeit Authentizität Integrität
<i>MaRisk</i> VA §10	Dokumentation	überprüfen	Integrität Authentizität Verfügbarkeit
VAG §64a Abs.3	Dokumentation	6 Jahre aufbewahren	Verfügbarkeit Integrität Datensicherheit
VAG §64a Abs.3	Dokumentation	Datensicherung Datenarchivierung	Verfügbarkeit Integrität Datensicherheit
HGB §238 Abs.1	Geschäftsvorfälle	Entstehen und Abwicklung verfolgbar	Verfügbarkeit
HGB §239	Dokument ändern	Änderung aufzeichnen, ursprünglicher Inhalt verfolgbar	Verfügbarkeit
HGB §239	Datenträger verwalten	Daten verfügbar	Verfügbarkeit
HGB §239	Datenträger verwalten	Daten lesbar	Verfügbarkeit
HGB §239	ausgedruckte Dokumente verwalten	Dokumente verfügbar	Verfügbarkeit

Tabelle 6.2: IT-Security Anforderungen in der *MaRisk* VA §10 und in den darin enthaltenen Querverweisen.

6.2 Anwendung der Abbildungskomponente

Die Anwendung der Analysekomponente hat gezeigt, dass die Compliance Anforderungen an die IT-Security aus *10 Information und Dokumentation* an den Geschäftsprozess Dokumentieren gerichtet sind. Die Ergebnisse der Anwendung der Schritte 1–4 (siehe Abschnitt 5.2.2) der Abbildungskomponente sind in der zweiten und in der vierten Spalte der Tabelle 6.2 enthalten. Die zweite Spalte der Tabelle enthält die einzelnen Aktivitäten, welche diejenigen Anforderungen an die IT-Security erfüllen müssen, die durch die lexikosemantische und kontextuelle Analyse festgelegt wurden. Die letzte Spalte der Tabelle enthält die Ziele an die IT-Security, welche durch die Compliance Anforderungen an die IT-Security adressiert werden.

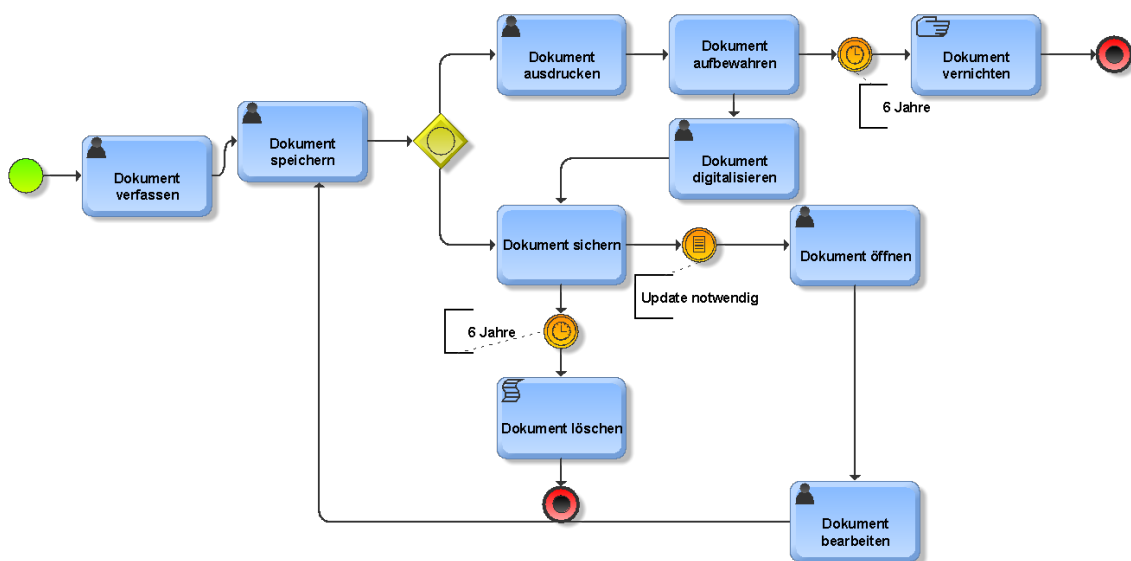


Abbildung 6.2: Lebenszyklus eines Dokumentes.

Laut Schritt 5 der Abbildungskomponente kann der Geschäftsprozess *Dokumentieren* mit Hilfe eines gängigen Modellierungstools visuell dargestellt werden. Die Abbildung 6.2 zeigt eine Version dieses Geschäftsprozesses. *Dokumentieren* beginnt mit dem Verfassen des Dokumentes, welches dann gespeichert wird. Aufbewahrt wird das Dokument entweder in elektronischer Form oder auf Papier. In letztem Fall muss es ausgedruckt werden. Das Dokument in elektronischer Form könnte bearbeitet (geändert, gelöscht) werden. Nach sechs Jahren Aufbewahrung werden alle Dokumente gelöscht oder vernichtet.

Für jede Aktivität aus dem Geschäftsprozess *Dokumentieren* werden mit Hilfe der *Gefährdungskataloge* aus [39] mögliche Gefährdungen identifiziert, welche die Ziele der IT-Security verletzen könnten (Schritt 6 der Abbildungskomponente). Eine Version des Geschäftsprozesses *Dokumentieren* mit Aktivitäten, welche mit Gefährdungen annotiert sind, wird in

der Abbildung 6.3 dargestellt.

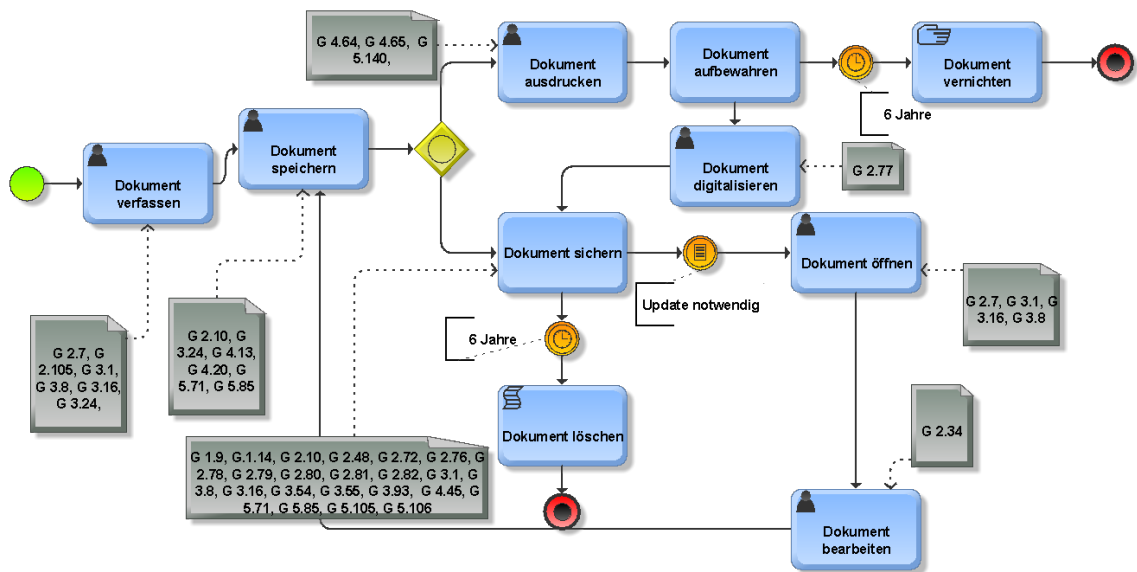


Abbildung 6.3: Gefährdungen im Lebenszyklus eines Dokuments.

Die Abbildung 6.4 stellt detailliert die Gefährdungen für die Aktivität *Dokument verfassen* aus dem Lebenszyklus eines Dokumentes dar. Der Anhang A enthält die restlichen Aktivitäten des Geschäftsprozesses *Dokumentieren*, welche mit Gefährdungen annotiert sind.

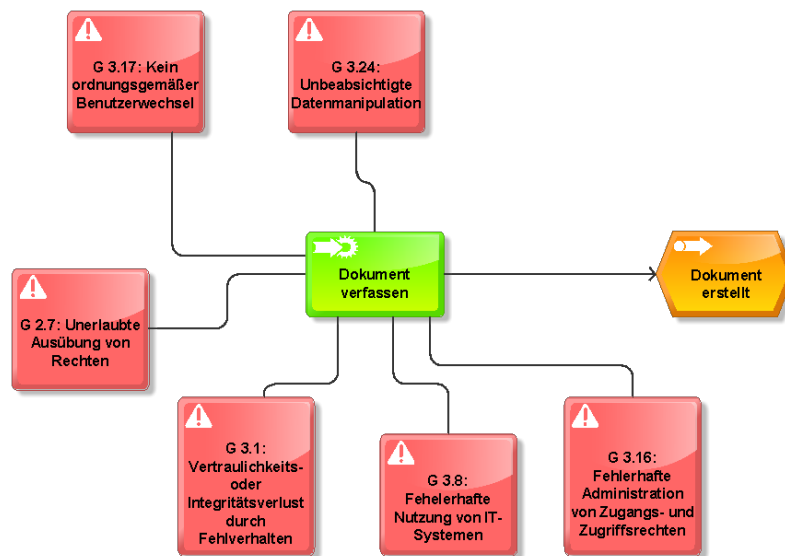


Abbildung 6.4: Gefährdungen für die Aktivität *Dokument verfassen*.

In letzten Schritt der Abbildungskomponente werden IT-Security-Policies erstellt. Diese haben die Rolle, die im Schritt 6. identifizierten Gefährdungen zu vermeiden und die

Aktivitäten des Geschäftsprozesses Dokumentieren im Bezug auf die IT-Security Ziele auszuführen. Die Basis für die IT-Security-Policies wird durch Maßnahmen aus den Maßnahmenkatalogen aus [39] dargestellt.

Von Gefährdungen zu informellen IT-Security-Policies Im Folgenden wird ausführlich gezeigt, wie die in der Abbildung 6.4 dargestellten Gefährdungen für die Aktivität *Dokument verfassen* untersucht werden und dann mit Hilfe der Maßnahmenkataloge aus den *BSI IT-Grundschutz Katalogen* IT-Security-Policies erstellt werden.

- *G 2.7: Unerlaubte Ausübung von Rechten*
Wenn Rechte wie Zugangs- oder Zugriffsberechtigungen zu großzügig, und dadurch an die falschen Personen vergeben werden, besteht das Risiko, dass ein Dokument nicht durch die berechtigte Person verfasst wird. Solche Rechte können durch berechtigte Personen, aber unautorisiert ausgeübt werden.
- *G 3.1: Vertraulichkeits- oder Integritätsverlust durch Fehlverhalten*
Diese Gefahr besteht, wenn z. B. Dokumente durch unberechtigte Personen gelesen oder verfasst werden oder wenn Daten aus Versehen fehlerhaft eingetragen, geändert oder gelöscht werden.
- *G 3.8: Fehlerhafte Nutzung von IT-Systemen*
Eine fehlerhafte oder nicht ordnungsgemäße Nutzung von IT-Systemen besteht z. B. in nicht gesperrten Terminals oder versehentlicher Löschung oder Veränderung von vertraulichen Daten.
- *G 3.16: Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
Wenn das Least Privilege-Prinzip² nicht respektiert wird und Zugriffsrechte auf gespeicherten Daten und IT-Anwendungen nicht ausreichend oder zu großzügig für die Wahrnehmung der Aufgaben vergeben werden, dann kommt es zu Betriebsstörungen, falls erforderliche Rechte nicht zugewiesen wurden, bzw. zu Sicherheitslücken, falls über die notwendigen Rechte hinaus weitere vergeben werden. Ein Beispiel dafür ist die fehlerhafte Administration der Zugriffsrechte eines Sachbearbeiters, wodurch er die Möglichkeit hat, auf die Protokolldaten zuzugreifen. Durch gezieltes Löschen einzelner Einträge ist es ihm möglich, seine Manipulationsversuche am Rechner zu verschleiern, da sie in der Protokolldatei nicht mehr erscheinen.
- *G 3.17: Kein ordnungsmäßiger Benutzerwechsel*
Wenn mehrere Benutzer an einem Rechner arbeiten, so kann es vorkommen, dass sich bei einem Benutzerwechsel der vorhergehende Benutzer nicht abmeldet und der neue sich nicht ordnungsgemäß abmeldet. Dieses Fehlverhalten führt dazu, dass die Protokollierung von An- und Abmeldevorgängen und damit ein Teil der Beweissicherung

²So wenige Rechte wie möglich, so viel wie nötig

unwirksam wird. Die Protokolle können nicht mehr zuverlässig beweisen, wer den Rechner zu einem bestimmten Zeitpunkt genutzt hat.

- *G 3.24: Unbeabsichtigte Datenmanipulation*

Diese Gefährdung besteht aus den zu umfangreich vergebenen Zugriffsberechtigungen auf IT-Anwendungen, welche das Risiko einer unbeabsichtigten Datenmanipulation mitbringt. Die grundsätzlichen Ursachen für unbeabsichtigte Datenmanipulationen können z. B. sein: mangelhafte oder fehlende Fachkenntnisse, mangelhafte oder fehlende Kenntnisse der Anwendung, zu umfangreiche Zugriffsberechtigungen und Fahrlässigkeit (z. B. das Verlassen des Arbeitsplatzes ohne korrekte Beendigung der Anwendung).

Gegen diese Gefährdungen werden in den *BSI-IT-Grundschutz-Katalogen* Maßnahmen vorgeschlagen.

Die Vergabe von Zugriffsrechten wird in der gleichnamigen Maßnahme *M 2.8: Vergabe von Zugriffsrechten* geregelt. Dadurch wird festgelegt, welche Person im Rahmen ihrer Funktion bevollmächtigt wird, IT-Anwendungen oder Daten zu nutzen. Die Zugriffsrechte (z. B. Lesen, Schreiben, Ausführen) auf IT-Anwendungen, Teilanwendungen oder Daten sind von der Funktion abhängig, welche von einer Person wahrgenommen wird, z. B. Anwenderbetreuung, Arbeitsvorbereitung, Systemprogrammierung, Anwendungsentwicklung, Systemadministration, Revision, Datenerfassung, Sachbearbeitung. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. Diese Maßnahme verhindert auch, dass Dokumente ohne Berechtigung verfasst, geändert oder gelöscht werden.

Die Festlegung und Überprüfung von Rollen wird durch die folgenden Maßnahmen geregelt:

- *M 2.5: Aufgabenverteilung und Funktionstrennung* sorgt dafür, dass diejenigen Funktionen bestimmt werden, welche miteinander nicht vereinbar sind, wie z. B. in dem Fall operativer und kontrollierender Funktionen. Nachdem die einzuhaltende Funktionstrennung festgelegt wurde, kann die Zuordnung der Funktionen zu Personen erfolgen. Vertreterregelungen sind ebenfalls zu berücksichtigen und zu dokumentieren.
- *M 2.30: Regelung für die Einrichtung von Benutzern/Benutzergruppen* Regelungen für die Einrichtung von Benutzern/Benutzergruppen bilden die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten und für die Sicherstellung eines geordneten und überwachbaren Betriebsablaufs.

- *M 2.65: Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System* Die Wirksamkeit von M 2.5 und M 2.30 ist mittels Protokollauswertung oder durch Stichproben in regelmäßigen Zeitabständen zu überprüfen. Wenn mehrere Benutzer unter einer Kennung arbeiten, sind diese auf die Verpflichtung zum Abmelden nach Aufgabenerfüllung hinzuweisen.
- *M 2.217: Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen* Die geschäftsrelevanten Daten, welche in einer Organisation die Grundlage für die Aufgabenerfüllung bilden, müssen besonders geschützt werden. Neben den allgemeinen Sorgfaltspflichten können auch hier für diese Daten bei der Speicherung, Verarbeitung, Weitergabe und Vernichtung besondere Vorschriften und Regelungen gelten. Geschäftskritische Informationen müssen vor Verlust, Manipulation und Verfälschung geschützt werden. Längerfristig gespeicherte oder archivierte Daten müssen regelmäßig auf ihre Lesbarkeit getestet werden. Nicht mehr benötigte Informationen müssen zuverlässig gelöscht werden.
- *M 2.220: Richtlinien für die Zugriffs- bzw. Zugangskontrolle* empfiehlt, Standard-Rechteprofile für nutzungsberechtigte Personen aufgrund ihrer Funktionen und Aufgaben festzulegen. Die Benutzerrechte für Zugriffe auf Dateien und Programme müssen abhängig von der jeweiligen Rolle, dem Need-to-Know und der Sensitivität der Daten definiert sein. Falls Rechte vergeben werden, die über den Standard hinausgehen, sollte dies begründet werden. Für jedes einzelne IT-System und jede IT-Anwendung sollten schriftliche Zugriffsregelungen und die Dokumentation der Einrichtung von Benutzern und der Rechtevergabe vorhanden sein.
- *M 3.3: Vertretungsregelungen* Vertretungsregelungen ermöglichen die Fortführung der Aufgabenwahrnehmung im Fall der vorhersehbaren und unvorhersehbaren Situationen (Urlaub, Krankheit usw.). Daher muss vor Eintritt eines solchen Falles geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist besonders im Bereich der Informationsverarbeitung von Bedeutung, da dafür meist Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Mitarbeiter für den Vertretungsfall nicht möglich ist.

Die Überprüfung der Zugangsberechtigung wird in der Maßnahme *M 2.7: Vergabe von Zugangsberechtigungen* geregelt. Zugangsberechtigungen erlauben der betroffenen Person oder einem autorisierten Vertreter, bestimmte IT-Systeme bzw. System-Komponenten, Netze und Anwendungen zu nutzen. Zugangsberechtigungen sind für jede nutzungsberechtigte Person aufgrund ihrer Funktion unter Beachtung der Funktionstrennung im Einzelnen festzulegen.

NAME	BASIS	IT-SECURITY-POLICY	ZIEL
P1	M 2.8	Eine aktuelle Dokumentation der vergebenen Zugriffsrechte muss vorliegen.	Zugriffskontrolle
P2	M 2.8	Zugriffsrechte werden minimal vergeben, damit diese für die jeweiligen Aufgaben ausreichend sind.	Zugriffskontrolle
P3	M 2.220 M 2.217	Beantragte Zugriffsrechte oder Änderungen verteilter Zugriffsrechte werden von den Verantwortlichen bestätigt und geprüft.	Zugriffskontrolle
P4	M 2.217	Ein geregeltes Verfahren für den Entzug von Zugriffsrechten muss existieren.	Zugriffskontrolle
P5	M 2.7	Eine umfassende Aufzählung der relevanten Funktionen muss erstellt werden.	Rollenüberprüfung
P6	M 2.7	Die Funktionstrennungen müssen vollständig definiert werden.	Rollenüberprüfung
P7	M 2.220 M 2.217	Richtlinien für die Zugriffs- bzw. Zugangskontrolle müssen erstellt werden.	Rollenüberprüfung
P8	M 2.220	Standard-Rechteprofile für verschiedene Funktionen bzw. Aufgaben müssen erstellt werden.	Rollenüberprüfung
P9	M 2.30	Organisatorische Regelungen zur Einrichtung von Benutzern bzw. Benutzergruppen müssen existieren.	Rollenüberprüfung
P10	M 2.65	Der ordnungsgemäße Benutzerwechsel muss regelmäßig geprüft werden.	Rollenüberprüfung
P11	M 2.5 M 3.3	In allen Bereichen müssen Vertretungsregelungen existieren.	Rollenüberprüfung
P12	M 2.7 M 3.3	In allen Vertretungsfällen müssen ausreichend kompetente Vertreter zur Verfügung stehen.	Rollenüberprüfung
P13	M 4.99	Sicherheitsmaßnahmen müssen ergriffen werden, damit Dateien nicht unbemerkt verändert werden können.	Signieren von erstellten Dateien

Tabelle 6.3: IT-Security-Policies für den Teilprozess *Dokument erstellen*.

Bewahrung der Integrität der Dokumente wird in der Maßnahme *M 4.99: Schutz gegen nachträgliche Veränderungen von Informationen* geregelt. Um unbemerkte Änderungen an Dateien zu verhindern, werden hier die Verwendung von digitalen Signaturen, das Hinzufügen von Copyright-Vermerken zu Informationen, oder die Verwendung von Dateiformaten empfohlen, die nachträgliche Änderungen bzw. auszugsweise Weiterverarbeitung erschweren. Auf der Basis dieser Maßnahmen werden IT-Security-Policies erstellt. Die Tabelle 6.3 ist ein Beispiel für informelle IT-Security-Policies, welche mit Hilfe der *BSI-*

IT-Grundschutz-Kataloge erstellt wurden. Die Abbildung 6.5 stellt schematisch dar, wie der Geschäftsprozess *Dokument verfassen* ausgeführt werden soll, damit die IT-Security Anforderungen aus der *MaRisk VA* erfüllt werden können. Der Prozess wird als ereignisgesteuerte Prozesskette (EPK) modelliert³. Die Gefährdungen werden als Risiken dargestellt, die Maßnahmen/IT-Security-Policies als Ereignisse und die Aktivitäten als Funktionen.

6.3 Zusammenfassung

In diesem Kapitel wurde das Framework zur Abbildung der regulatorischen Compliance auf IT-Security-Policies auf *10 Information und Dokumentation* der *MaRisk VA* angewendet. Mit der Analysekomponente wurden die Anforderungen an die IT-Security identifiziert. Die Abbildungskomponente hat mögliche Gefährdungen für die IT-Security Ziele und für die Aktivitäten, an welche diese IT-Security Anforderungen gerichtet werden, identifiziert. Die Analyse der Gefährdungen und der Maßnahmen gegen diese Gefährdungen benutzt die *BSI-IT-Grundschutz-Kataloge* als Leitfaden.

Die auf Basis der Maßnahmenkataloge erstellten IT-Security-Policies haben einen informellen Charakter und sie sind in allgemein lesbarer Form verfasst. Diese High-Level Policies stehen für die weitere Verarbeitung in einem inkrementellen Verfeinerungsprozess und abhängig von der IT-Ausstattung und von den konkreten Abläufen des Versicherungsunternehmens zu Low-Level Policies bereit. Die zwei Parameter, IT-Ausstattung und konkrete Abläufe des Versicherungsunternehmens, sind für den Automatisierungsgrad des Transformations- und des Durchsetzungsprozesses der IT-Security-Policies entscheidend.

³modelliert mit Aris 2.3 Express: <http://www.ariscommunity.com/aris-express>

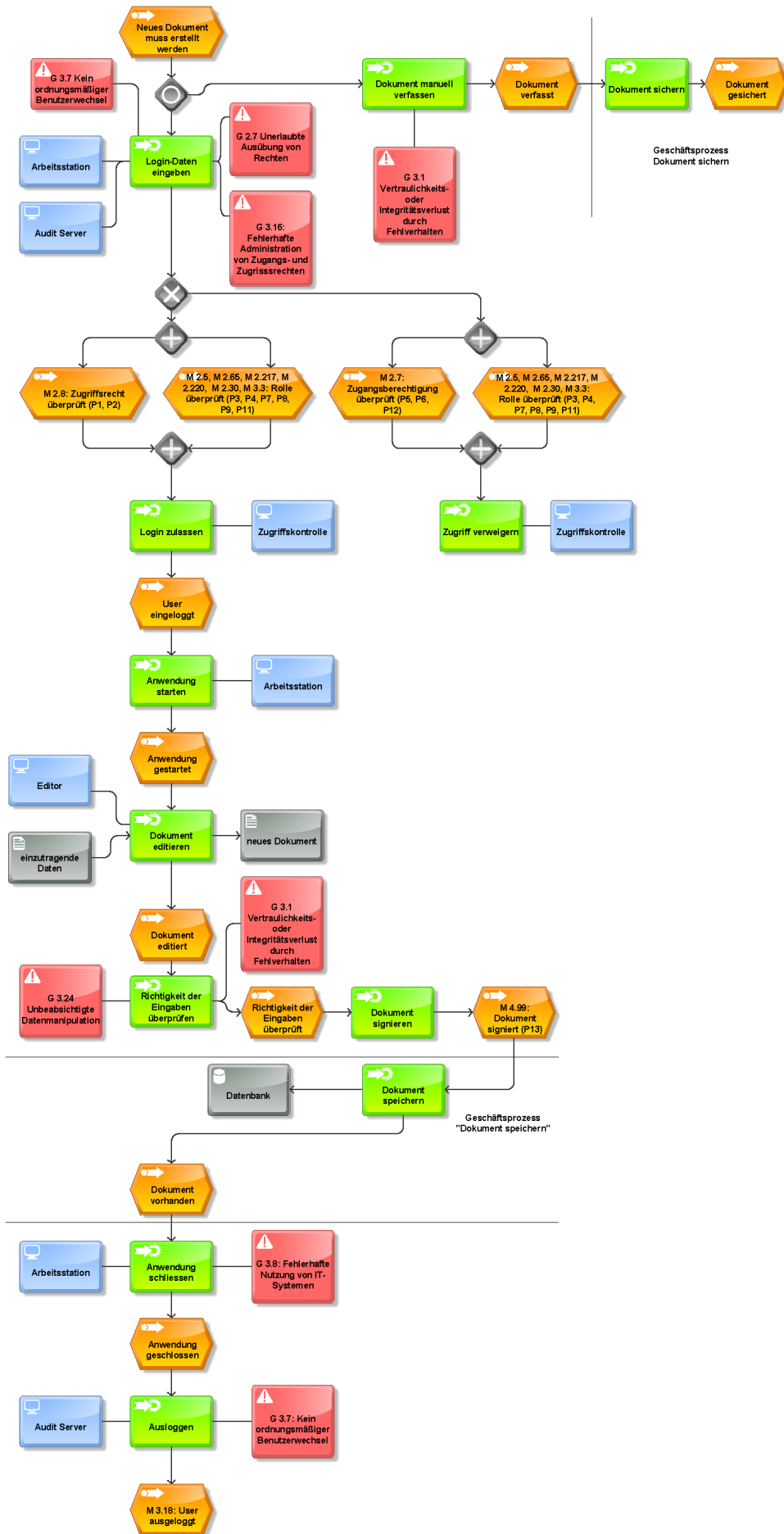


Abbildung 6.5: Der Geschäftsprozess *Dokument editieren* mit Berücksichtigung der Anforderungen an die IT-Security.

Kapitel 7

Erfahrungen und Diskussion

In diesem Kapitel wird diskutiert, welche regulatorischen Texte sich für die Anwendung des in den Kapiteln 6 und 7 vorgestellten Frameworks zur Abbildung der regulatorischen Compliance auf IT-Security Policies eignen, welches Wissen von der Seite des Benutzers benötigt wird, um das Framework anzuwenden, und anschließend, ob es möglich ist, bestimmte Schritte des Frameworks automatisiert durchzuführen.

7.1 Anwendungsbereich des Frameworks

Das im Rahmen dieser Diplomarbeit vorgeschlagene Framework zur Abbildung der regulatorischen Compliance auf IT-Security Policies wurde speziell entwickelt, damit die Anforderungen an die IT-Security aus der *MaRisk VA* identifiziert, analysiert und auf IT-Security Policies abgebildet werden können. Diese „Spezialisierung“ auf die *MaRisk VA* grenzt den Anwendungsbereich des Verfahrens nicht ein:

- Die verfeinerten Analysemethoden der Analysekomponente identifizieren gesetzliche Konzepte und Anforderungen an die IT-Security in jedem regulatorischen Text.
- Die Abbildungskomponente unterstützt den Anwender des Verfahrens bei der Abbildung der Anforderungen an die IT-Security, welche mit der Analysekomponente identifiziert werden, auf IT-Security-Policies. In dieser Diplomarbeit wurden die *BSI-IT-Grundschutz-Kataloge* als Leitfaden für die Erstellung der IT-Security-Policies vorgeschlagen; mit dem gleichen Zweck können auch die internationalen IT-Security-Standards *ISO 27001* und *ISO 27002* (siehe Abschnitt 2.3.3) benutzt werden.

7.2 Wirkungsbereich des Frameworks

Das Framework zur Abbildung der regulatorischen Compliance auf IT-Security-Policies adressiert nur eine Teilmenge aller Compliance Anforderungen, welche in einem regulatorischen Text enthalten sind:

- Compliance Anforderungen an die IT-Security (IT-Compliance),
- Compliance Anforderungen, welche sich mit Hilfe der IT umsetzen lassen (IT-gestützte Compliance).

Auch die IT-Security-Aspekte, welche durch die vom Text abgeleiteten IT-Security Policies adressiert werden, stellen nur einen Teil der gesamten Aspekte der IT-Security dar, welche durch eine Organisation betrachtet werden müssen. Daher empfiehlt sich die Anwendung dieses Verfahrens komplementär zu anderen Methoden für die Umsetzung der Compliance Anforderungen und der IT-Security-Maßnahmen, die für eine Organisation notwendig sind. In der Regel existiert bereits ein IT-Security-Konzept in jeder Organisation; in diesem Fall kann das in dieser Diplomarbeit vorgeschlagene Verfahren zur Abbildung der regulatorischen Compliance auf IT-Security Policies als Prüfmethode dienen. So kann überprüft werden, ob die IT-Security Aspekte, welche durch die regulatorischen Vorgaben verlangt werden, in dem existierenden IT-Security Konzept der Organisation bereits existieren, oder ob diese noch berücksichtigt werden müssen.

7.3 Anforderungen an das Benutzerprofil

Damit das Framework zur Abbildung der regulatorischen Compliance auf IT-Security-Policies die gewünschten Ergebnisse bringt, muss der Benutzer, der es anwendet, einige Fachkenntnisse besitzen:

- Die Anwendung der ersten Phase der Analysekomponente, innerhalb derer die Compliance Anforderungen identifiziert werden, stellt den ersten Kontakt des Benutzers mit dem juristischen Text dar. Daher sollen die Besonderheiten der juristischen Fachsprache, so wie sie im Kapitel 3 beschrieben wurden, dem Benutzer bekannt sein. Des Weiteren soll der Benutzer in der Lage sein, sowohl die Aktivitätsverben, als auch die modalen Konstrukte zu erkennen.
- Die zweite Phase der Analysekomponente identifiziert die direkten und die indirekten Anforderungen an die IT-Security im regulatorischen Text. Die direkten Anforderungen werden durch lexikosemantische Hinweise dargestellt. Die lexikosemantische Analyse des Textes setzt Kenntnisse im Bereich der IT-Security voraus: der Benutzer soll in diesem Fall erkennen können, ob ein Begriff einen Hinweis auf einen Aspekt der IT-Security darstellt. Die indirekten Anforderungen an die IT-Security, welche durch die kontextuelle Analyse identifiziert werden, setzen sowohl die Kenntnis der Geschäftsabläufe aus dem Anwendungsbereich des analysierten Gesetzes, als auch die Kenntnis über die technischen Möglichkeiten der Organisation voraus, welche die Compliance Anforderungen umsetzen muss. Im Fall von *MaRisk VA* sollten die Geschäftsprozesse aus dem Versicherungsunternehmen dem Anwender des in dieser Diplomarbeit vorgeschlagenen Verfahrens bekannt sein.

- Die Anwendung der Abbildungskomponente setzt sehr gute Kenntnisse über die IT-Security Mechanismen und der IT-Security Standards voraus. Im Fall des vorgestellten Verfahrens sollte der Benutzer mit dem Inhalt der *BSI-IT-Grundschutz-Kataloge* vertraut sein.

Diese Anforderungen an das Profil des Benutzers werden in der Tabelle 7.1 zusammengefasst:

KOMPONENTE	PHASE	KENNTNISSE
Analysekomponente	Identifikation der Compliance Anforderungen	- Kenntnis der Besonderheiten der juristischen Sprache - Linguistische Kenntnisse
Analysekomponente	Lexikosemantische Analyse	- Kenntnisse über IT-Security
Analysekomponente	Kontextuelle Analyse	- Kenntnisse über Geschäftsprozesse aus dem Versicherungsunternehmen
Abbildungskomponente		- Kenntnisse über IT-Security - Kenntnis der gängigen IT-Security Standards

Tabelle 7.1: Anforderungen an die Ausbildung des Benutzers.

7.4 Unterstützung der Benutzer durch (Teil-)Automatisierung

Ähnlich wie die in Kapitel 4 beschriebenen Ansätze zur Analyse des regulatorischen Textes wird das in dieser Diplomarbeit vorgeschlagene Verfahren zur Abbildung der regulatorischen Compliance auf IT-Security-Policies manuell angewendet. Das manuelle Vorgehen hat den Vorteil, dass es sicherstellt, dass die Ambiguitäten gelöst, die Querverweise verfolgt, und alle im Text erwähnten IT-Security-Aspekte betrachtet werden. Der Nachteil des manuellen Vorgehens ist einerseits der Aufwand bei der Anwendung der Komponenten und andererseits die Tatsache, dass der Benutzer Kenntnisse aus mehreren Bereichen für eine erfolgreiche Anwendung des Verfahrens mitbringen soll (siehe Tabelle 7.1).

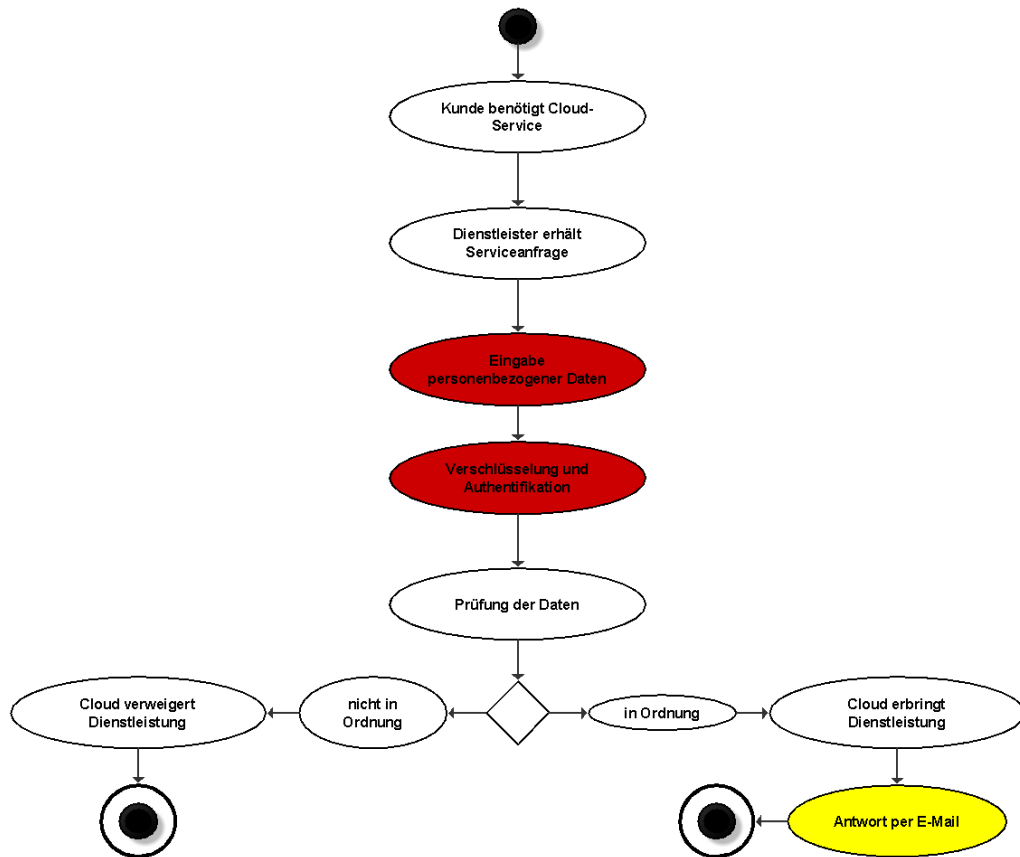
Um sowohl den Aufwand bei der Anwendung des Verfahrens zu verringern als auch diejenigen Benutzer, welche die notwendigen Kenntnisse im Bereich der IT-Security oder Versicherungen nicht haben, zu unterstützen, könnte versucht werden, das Verfahren zu automatisieren. Eine völlige Automatisierung ist mit den heutigen Mitteln der semantischen

Technologien nicht möglich: es würde ein automatisiertes Textverständnis voraussetzen, und dieses steht noch nicht zur Verfügung. Einige Möglichkeiten für die Teilautomatisierung des Verfahrens werden im Folgenden vorgestellt.

Heuristischer Editor für Compliance Anforderungen Die Compliance Anforderungen, welche in der ersten Phase der Analysekomponente (siehe Abschnitt 5.2.1) festgelegt werden, können auf IT-Security Anforderungen (lexikosemantische Analyse) toolbasiert untersucht werden. Zu diesem Zweck kann z. B. der Editor HeRA (Heuristic Requirements Assistant) [38] zum Editieren der Compliance Anforderungen benutzt werden. HeRA ist ein spezieller Editor für funktionale und Service Anforderungen. Dieser Editor benutzt heuristische Regeln zur Darstellung des Wissens und der Erfahrung der IT-Security-Experten aus anderen Projekten. Der Benutzer von HeRA bekommt Warnungen oder Tipps, wenn die editierten Anforderungen relevante Begriffe und Muster aus dem Bereich der IT-Security enthalten. Ein solcher Editor kann auch diejenigen Benutzer, die keine IT-Security-Experten sind, bei der Identifizierung der expliziten Anforderungen an die IT-Security unterstützen.

Automatisierte Suche in den BSI-IT-Grundschutzkatalogen Die Schritte 5 und 6 der Abbildungskomponente (Abschnitt 5.2.2) schlagen eine Visualisierung der Abläufe aus dem Versicherungsunternehmen mit den dazugehörigen IT-Security Anforderungen durch Geschäftsprozessmodelle vor. Wenn diese Abläufe mit Hilfe von UML-Aktivitätsdiagrammen modelliert werden, kann das UMLsec-Werkzeug mit dem Riskfinder-Plugin [65] benutzt werden. Das UMLsec-Werkzeug überprüft die in UMLsec (siehe Abschnitt 4.4) modellierten IT-Security-Eigenschaften. Zusammen mit dem Riskfinder-Plugin unterstützt das UMLsec das Risikomanagement und die Überprüfung von Geschäftsprozessen auf IT-Security Eigenschaften. Das Riskfinder-Plugin nutzt für die IT-Security Analyse der Aktivitätsdiagramme ein Repository mit Begriffen aus dem Bereich der IT-Security. Dieses Repository basiert auf den *BSI-IT-Grundschutzkatalogen*. Wenn in dem mit UMLsec-Werkzeug überprüften Aktivitätsdiagramm IT-Security relevante Aktivitäten identifiziert werden (siehe in der Abbildung 7.1 die rot- und die gelb-gefärbten Aktivitäten im Beispiel-Aktivitätsdiagramm), werden dem Anwender die relevanten Stellen aus den *BSI-IT-Grundschutzkatalogen* gezeigt, welche weiter für die Erstellung der IT-Security-Policies benutzt werden sollen (siehe die textuelle Ausgabe des Werkzeugs Risikoverdacht bei [*Eingabe personenbezogenes Daten*], Risikoverdacht bei [*Antwort per E-Mail*] und Risikoverdacht bei [*Verschlüsselung und Authentifikation*]).

7.4. UNTERSTÜTZUNG DER BENUTZER DURCH (TEIL-)AUTOMATISIERUNG 83



Risikoverdacht bei [Eingabe personenbezogener Daten]:	
1	B_1.5_Datenschutz
2	B_1.7_Kryptokonzept
3	B_1.11_Outourcing
4	B_1.15_Löschen_und_Vernichten_von_Daten
5	B_2.10_Mobiler_Arbeitsplatz
6	B_3.201_Allgemeiner_Client
7	B_3.301_Sicherheitsgateway_Firewall
8	B_3.302_Router_und_Switches
9	B_4.6_WLAN
10	B_4.4_VPN
11	B_5.3_E-Mail

Risikoverdacht bei [Antwort per E-Mail]:	
1	B_5.3_E-Mail

Risikoverdacht bei [Verschlüsselung und Authentifikation]:	
1	B_1.7_Kryptokonzept
2	B_1.7_Kryptokonzept
3	B_1.11_Outourcing
4	B_1.11_Outourcing
5	B_1.15_Löschen_und_Vernichten_von_Daten
6	B_1.15_Löschen_und_Vernichten_von_Daten
7	B_2.10_Mobiler_Arbeitsplatz
8	B_2.10_Mobiler_Arbeitsplatz
9	B_3.201_Allgemeiner_Client
10	B_3.201_Allgemeiner_Client
11	B_3.301_Sicherheitsgateway_Firewall
12	B_3.301_Sicherheitsgateway_Firewall
13	B_3.302_Router_und_Switches
14	B_3.302_Router_und_Switches
15	B_4.6_WLAN
16	B_4.6_WLAN
17	B_4.4_VPN
18	B_4.4_VPN
19	B_5.3_E-Mail
20	B_5.3_E-Mail

Abbildung 7.1: Relevante Stellen aus den *BSI-IT-Grundschutzkatalogen* für die IT-Security-kritischen Aktivitäten (vgl. [65]).

7.5 Zusammenfassung

Damit das Framework zur Abbildung der regulatorischen Compliance auf IT-Security-Policies erfolgreich und effizient angewendet werden kann, muss der Benutzer ein bestimmtes Wissen mitbringen. Dieses notwendige Wissen wurde am Anfang des Kapitels vorgestellt. Es wurden dann zwei Möglichkeiten diskutiert, Teilschritte des Verfahrens automatisiert durchzuführen: HeRA innerhalb der Analysekomponente und das UMLsec-Werkzeug mit dem Riskfinder-Plugin innerhalb der Abbildungskomponente.

Kapitel 8

Zusammenfassung und Ausblick

8.1 Zusammenfassung

Die Forschungsfrage dieser Diplomarbeit, ob es möglich ist, IT-Security-Policies direkt von den regulatorischen Texten abzuleiten, wurde durch zwei Fakten motiviert:

- Die verschiedenen Organisationen sind dazu verpflichtet, die Compliance Anforderungen der Gesetzgeber zu beachten.
- Die Rolle der IT in den Organisationen und implizit bei der Erfüllung dieser Compliance Anforderungen steigt.

Die Verwendung der Mittel der IT bringt nicht nur die Vorteile der Automatisierung der Abläufe mit, sondern auch die Herausforderung, die IT-Security Ziele zu schützen. Daher setzte sich diese Diplomarbeit das Ziel, durch die Entwicklung des Konzeptes eines Frameworks für die Abbildung der regulatorischen Compliance auf IT-Security-Policies eine integrierte Sicht auf die Compliance und IT-Security anzubieten.

Die Überführung der Gesetze in IT-Security-Policies setzt die Überwindung der Grenzen der juristischen Fachsprache voraus, in welcher die Gesetze verfasst werden. Aus diesem Grund wurde in Kapitel 3 die juristische Fachsprache mit ihren Eigenschaften und Schwierigkeiten ihrer Interpretation vorgestellt.

Da die untersuchten aktuellen Arbeiten aus dem Bereichen Compliance Management und IT-Security Management, welche im Kapitel 4 vorgestellt wurden, zur Erfüllung des Zieles dieser Diplomarbeit nicht beitragen konnten, erwies es sich als notwendig, ein neues Konzept für ein Framework für die Abbildung der regulatorischen Compliance auf IT-Security-Policies zu entwickeln. Dieses Framework wurde im Kapitel 5 vorgestellt. Das Framework enthält zwei Komponenten, welche nacheinander auf den regulatorischen Text angewendet werden: die Analysekomponente und die Abbildungskomponente:

1. Mit der Analysekomponente werden in dem ersten Schritt die Compliance Anforderungen identifiziert. Die Identifizierung erfolgt durch die Suche im Text nach Aktivitäten, welche durch Verben ausgedrückt werden. Die modalen Konstrukte, welche diese Aktivitätsverben begleiten, entscheiden die gesetzliche Natur der Compliance Anforderungen: in dem Fall des untersuchten Gesetzes *MaRisk VA* sind es Pflichten, Verbote und Erlaubnisse. Der nächste Schritt besteht aus der Untersuchung jeder einzelner Compliance Anforderung: geht es um eine direkte Anforderung an die IT-Security? In diesem Fall sind lexikosemantische Hinweise entscheidend. Adressieren die Compliance Anforderungen Geschäftsprozesse auf eine Art, dass bei der complianten Ausführung dieser Geschäftsprozesse Aspekte der IT-Security beachtet werden müssen? Der erste Schritt der Analyse ist für einen IT-Security Spezialisten zugänglich, der zweite Schritt setzt die Kenntnis der Abläufe in dem Versicherungsunternehmen voraus, was eine Zusammenarbeit zwischen Spezialisten aus beiden Bereichen notwendig macht.
2. Die zweite Komponente des Frameworks zur Abbildung der regulatorischen Compliance auf IT-Security-Policies ist die Abbildungskomponente. Es wird festgelegt, auf welche Aktivitäten oder Geschäftsprozesse aus dem Unternehmen die IT-Security-Anforderungen, welche mit der Analysekomponente identifiziert wurden, angewendet werden müssen. Abhängig von der Natur dieser Aktivitäten und von den IT-Security-Anforderungen wird mit Hilfe der BSI IT-Grundschutz-Kataloge untersucht, welche Gefährdungen an die IT-Security möglich sind und welche Maßnahmen dagegen existieren. Diese Maßnahmen werden als informelle IT-Security-Policies verfasst und diese können danach, abhängig von den technischen Möglichkeiten, automatisiert durchgesetzt werden.

In Kapitel 6 wird das Framework zur Abbildung der regulatorischen Compliance auf IT-Security-Policies in *10 Information und Dokumentation* aus der *MaRisk VA* angewendet.

Durch die Anwendung des Frameworks können IT-Security-Policies auf der Basis jedes regulatorischen Textes formuliert werden. Um dieses Framework anwenden zu können, bedarf der Benutzer bestimmter Fachkenntnisse. Die Anforderungen an die Ausbildung des Benutzers wurden im Kapitel 7 beschrieben. Weiter wurden in diesem Kapitel zwei Möglichkeiten vorgestellt, um Teilschritte des Verfahrens zu automatisieren: den heuristischen Editor HERA, der die Begriffe mit Bezug auf der IT-Security erkennt, und den UMLsec-Werkzeug mit dem Riskfinder-Plugin, welches relevante Stellen aus den BSI IT-Grundschutzkatalogen zur Erstellung der IT-Security-Policies abhängig von den Anforderungen an die IT-Security findet.

8.2 Ausblick

Das Konzept für die Abbildung der regulatorischen Compliance auf IT-Security-Policies, welches in dieser Diplomarbeit entwickelt wurde, kann weiter für die Arbeiten im Bereich der Compliance und der IT-Security in mindestens zwei Richtungen benutzt werden:

1. *Repository von IT-Security Kontrollen*: Die Anforderungen an die IT-Security, welche durch die Anwendung der Analysekomponente auf die regulatorischen Texte gewonnen werden, sowie die Maßnahmen, welche aus den BSI IT-Grundschutz-Katalogen abgeleitet werden, können als Kontrollen modelliert in einem Kontrollen-Repository gespeichert und bei Bedarf in bereits existierende Geschäftsprozesse eingefügt werden. Wenn bestimmte Geschäftsprozesse Compliance Anforderungen mit Schwerpunkt IT-Security erfüllen müssen, können passende Kontrollen aus dem Repository ausgesucht werden. Wichtig ist in diesem Fall, dass die Zurückverfolgbarkeit der Kontrollen gewährleistet wird, weil die Compliance Anforderungen sich von Organisation zur Organisation unterscheiden. Vorteilhaft wäre auch, wenn aus diesen Kontrollen automatisch Quellcode generiert werden könnte.
2. *Synergien von Geschäftsprozessen*: Die Abbildung 6.5 stellt einen möglichen Ablauf für den Geschäftsprozess *Dokument verfassen* dar. Dieser Geschäftsprozess wurde durch die Analyse der Compliance Anforderungen aus der *MaRisk VA* erstellt. Es ist sicher, dass in den Versicherungsunternehmen ein Geschäftsprozess *Dokument verfassen*, als Teil mehrerer Abläufe, bereits existiert. Der vollständige Ersatz der alten, nicht-complianten Geschäftsprozesse mit den neu Erstellten ist ineffizient, daher müssen Möglichkeiten für Synergien untersucht werden, damit die neuen, complianten Geschäftsprozesse und die alten Geschäftsprozesse zusammengeführt werden können.

Anhang A

Gefährdungen für verschiedene Aktivitäten

Unten werden die Gefährdungen gemäß den BSI IT-Grundschutzkatalogen für die Aktivitäten aus der Abbildung 6.3 detailliert dargestellt.

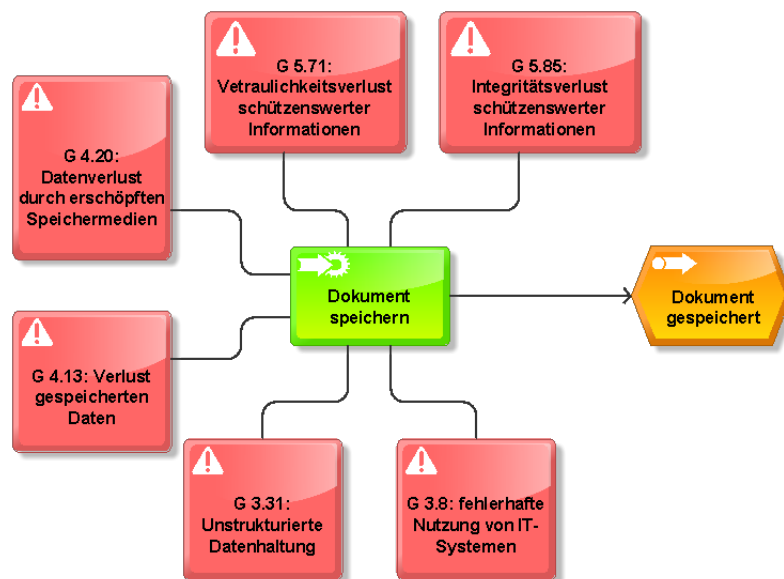
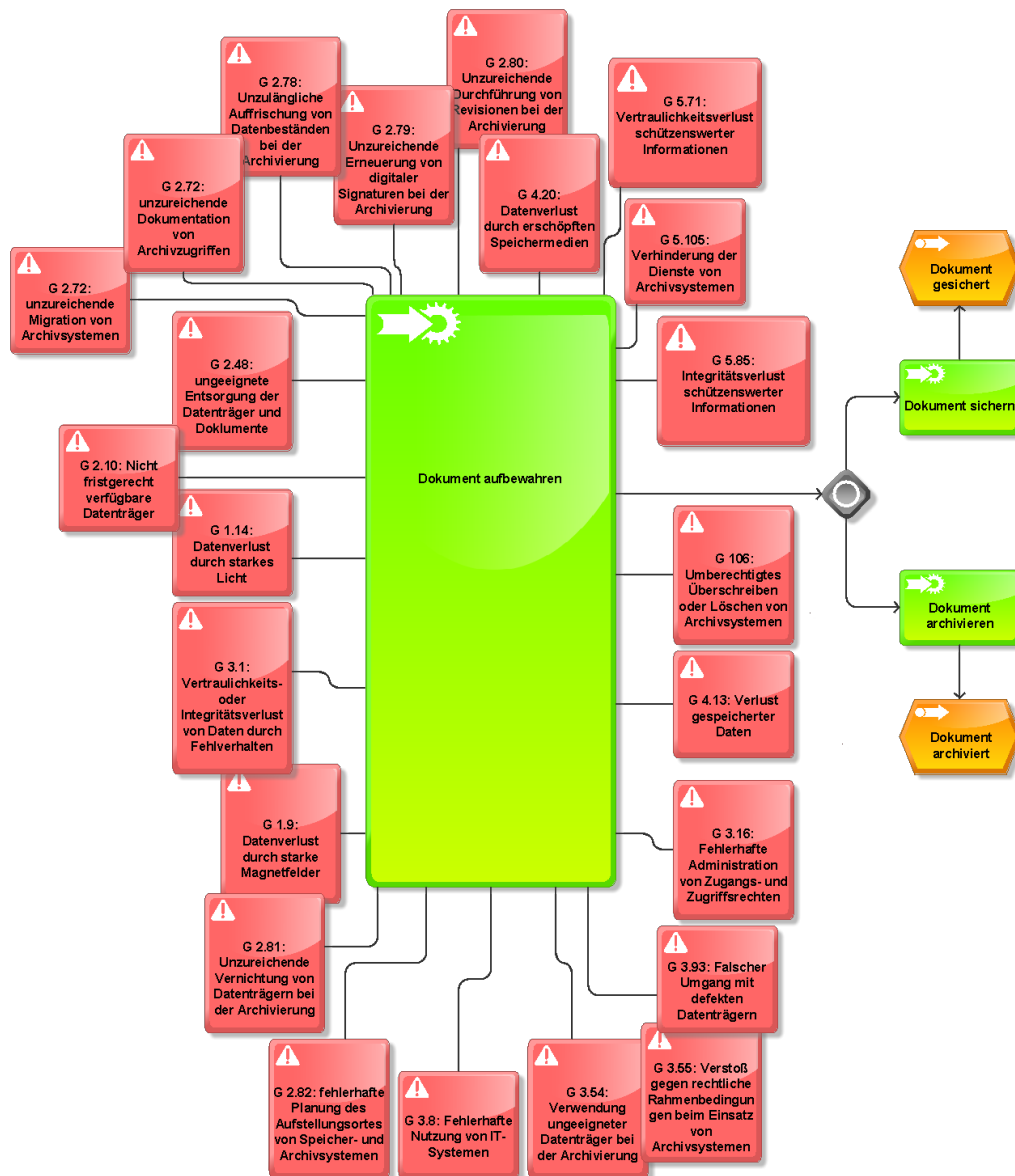


Abbildung A.1: Gefährdungen für die Aktivität *Dokument speichern*

Abbildung A.2: Gefährdungen für die Aktivität *Dokument aufbewahren*

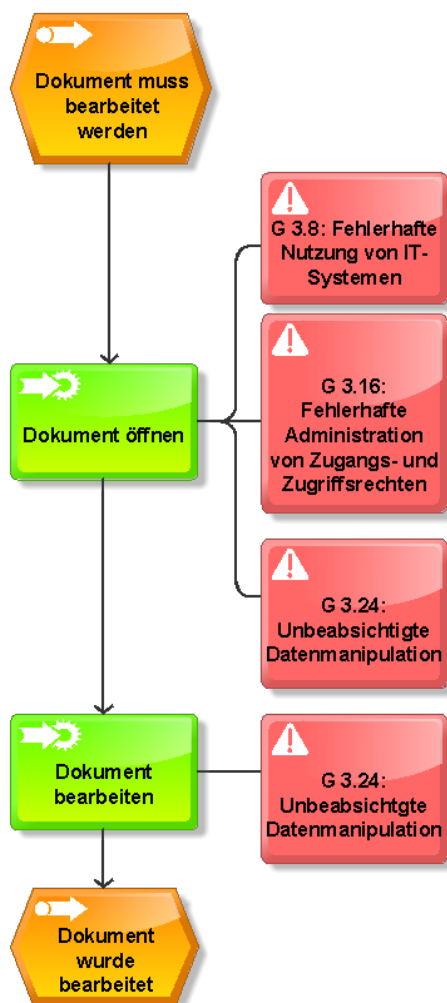


Abbildung A.3: Gefährdungen für die Aktivität *Dokument bearbeiten*

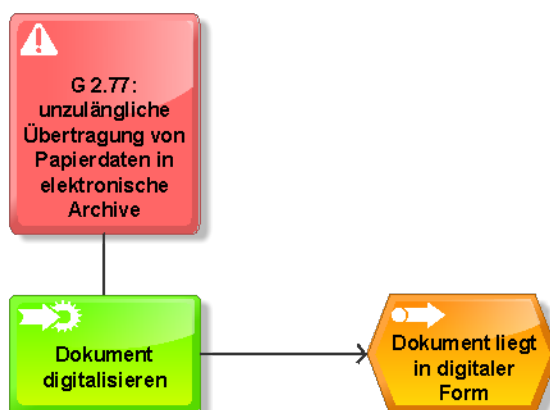


Abbildung A.4: Gefährdungen für die Aktivität *Dokument digitalisieren*

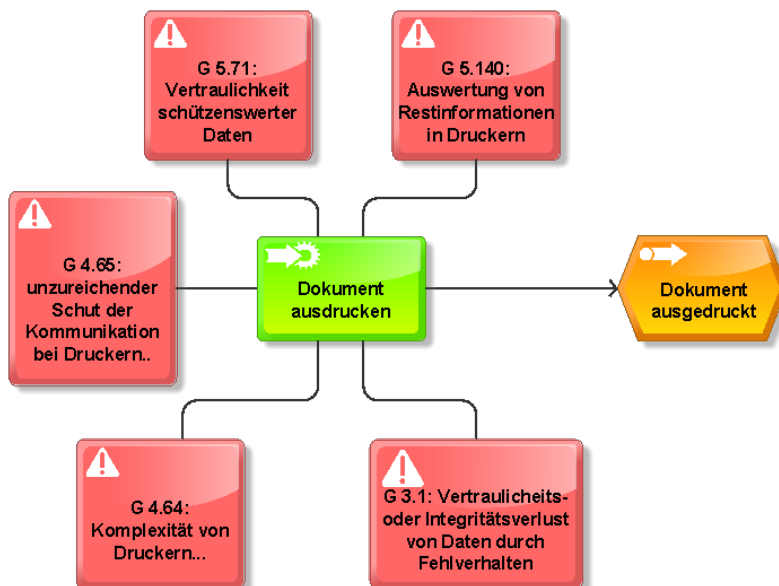


Abbildung A.5: Gefährdungen für die Aktivität *Dokument ausdrucken*

Literaturverzeichnis

- [1] *Gesetzgebung in der EU*. <http://www.parteien-online.de/thema/eu-gesetzgebung/> (abgerufen am 21.02.2011).
- [2] *Governance, Risk & Compliance und SAP*. <http://www.e3cms.de/index.php?id=1811> (abgerufen am 04.09.2010).
- [3] *Pons: das Sprachenportal*. <http://de.pons.eu/latein-deutsch/compleo> (abgerufen am 20.02.2011).
- [4] ANTÓN, ANNIE I., TRAVIS D. BREAUX, DIMITRIS KARAGIANNIS und JOHN MYLOPOULOS: *First International Workshop on Requirements Engineering and Law (RE-LAW)*. In: *Proceedings of the 2008 Requirements Engineering and Law, RELAW '08*, Seiten i–iv, Washington, DC, USA, 2008. IEEE Computer Society.
- [5] ASHLEY, PAUL, SATOSHI HADA, GÜNTER KARJOTH und MATTHIAS SCHUNTER: *E-P3P privacy policies and privacy authorization*. In: *Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society, WPES '02*, Seiten 103–109, New York, NY, USA, 2002. ACM.
- [6] BALLWIESER, WOLFGANG: *Bilanzskandale: Ursachen und Folgen*. <http://www.rwp.bwl.uni-muenchen.de/files/download/bilanzskandale.pdf> (abgerufen am 20.09.2010).
- [7] BIAGIOLI, C., P. MARIANI und D. TISCORNIA: *Esplex: A rule and conceptual model for representing statutes*. In: *Proceedings of the 1st international conference on Artificial intelligence and law, ICAIL '87*, Seiten 240–251, New York, NY, USA, 1987. ACM.
- [8] BISKUP, JOACHIM: *Security in Computing Systems: Challenges, Approaches and Solutions*. Springer Publishing Company, Incorporated, 1st Auflage, 2008.
- [9] BITKOM, DIN: *Leitfaden Kompass IT-Sicherheitsstandards*. (abgerufen am 04.03.2011).

- [10] BREAU, TRAVIS D.: *Legal Requirements Acquisition for the Specification of Legally Compliant Information Systems*. Doktorarbeit, North Carolina State University, Raleigh, North Carolina, USA, April 2009.
- [11] BREAU, TRAVIS D. und ANNIE I. ANTÓN: *Analyzing Goal Semantics for Rights, Permissions, and Obligations*. In: *RE '05: Proceedings of the 13th IEEE International Conference on Requirements Engineering*, Seiten 177–188, Washington, DC, USA, 2005. IEEE Computer Society.
- [12] BREAU, TRAVIS D., ANNIE I. ANTÓN und JON DOYLE: *Semantic parameterization: A process for modeling domain descriptions*. *ACM Trans. Softw. Eng. Methodol.*, 18(2):1–27, 2008.
- [13] BREAU, TRAVIS D. und ANNIE I. ANTON: *Deriving Semantic Models from Privacy Policies*. In: *POLICY '05: Proceedings of the Sixth IEEE International Workshop on Policies for Distributed Systems and Networks*, Seiten 67–76, Washington, DC, USA, 2005. IEEE Computer Society.
- [14] BREAU, TRAVIS D., MATTHEW W. VAIL und ANNIE I. ANTÓN: *Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations*. In: *In: Proceedings of the 14th IEEE International Requirements Engineering Conference. (2006)*, Seiten 46–55. IEEE Computer Society, 2006.
- [15] BROSCINSKI, RALPH: *Kerngeschäftsprozesse eines Versicherungsunternehmens*. In: AL., M. ASCHENBRENNER ET (Herausgeber): *Informationsverarbeitung in Versicherungsunternehmen*, Seiten 71–96. Springer-Verlag Berlin Heidelberg, 2010.
- [16] CARALT, NÚRIA CASELLAS: *Modelling Legal Knowledge through Ontologies. OPJK: the Ontology of Professional Judicial Knowledge*. Doktorarbeit, Departament de Ciència Política i Dret Públic. Universitat Autònoma de Barcelona, 2008.
- [17] CONWAY, PAUL: *Syntactic Ambiguity*. [http://www.lawfoundation.net.au/ljf/site/articleIDs/63B6C5E2ABB6A511CA25714C000CFF37/\\$file/syntactic.pdf](http://www.lawfoundation.net.au/ljf/site/articleIDs/63B6C5E2ABB6A511CA25714C000CFF37/$file/syntactic.pdf) (abgerufen am 09.03.2011).
- [18] DANCIU, VITALIAN: *Entwicklung einer policy-basierten Managementanwendung für das prozeßorientierte Abrechnungsmanagement*. Diplomarbeit, Ludwig-Maximilians-Universität München, 2003.
- [19] DELOITTE: *2009 Survey on IT-business balance. Shaping the relationship between business and IT for the future*. http://www.deloitte.com/view/de/_DE/de/dienstleistungen/wirtschaftspruefung/enterprise-risk-services/security-privacy/security-management/bf81bf29bff0210VgnVCM100000ba42f00aRCRD.htm (abgerufen am 17.09.2010).

- [20] ECKARDT, BIRGIT: *Fachsprache als Kommunikationsbarriere?* Deutscher Universitäts-Verlag; Dissertation Universität Jena, 1. Auflage, 1999.
- [21] ECKERT, CLAUDIA: *IT-Sicherheit*. Oldenbourg, München [u.a.], 3., überarb. und erw. Aufl Auflage, 2004.
- [22] EGE, KONRAD: *Enron und der Reißwolf*. <http://www.freitag.de/politik/0205-usa> (abgerufen am 04.09.2010).
- [23] EKOTO NYANGONO, ARMELLE CLAUDE: *Geschäftsprozessmodellierung und Compliance*. Diplomarbeit, TU Dortmund, Fraunhofer ISST, September 2010.
- [24] FABRICIUS-HANSEN, CATHRINE; GALLMANN, PETER; EISENBERG PETER; FIEHLER REINHARD; PETERS JÖRG: *Duden 04. Die Grammatik: Unentbehrlich für richtiges Deutsch. Band 4*. Bibliographisches Institut, Mannheim, 8. Auflage, 2009.
- [25] FINANZDIENSTLEISTUNGSAUFSICHT, BUNDESANSTALT FÜR: *Versicherungsaufsicht*. http://www.bafin.de/DE/BaFin/Aufgaben/Versicherungsaufsicht/versicherungsaufsicht_node.html?_nnn=true (abgerufen am 08.05.2011).
- [26] FREUND, JAKOB UND RÜCKER, BERND: *Praxishandbuch BPMN 2.0*. Carl Hanser Verlag, 2., aktualisierte Auflage Auflage, 2010.
- [27] GENETTE, GÉRARD: *Palimpseste. die Literatur auf zweiter Stufe*. Edition Suhrkamp. Aesthetica. 1683 = N.F., 683. Suhrkamp, Dt. Erstausg., 1. Aufl., [Nachdr.] Auflage, 2004.
- [28] GOVERNANCE-INSTITUTE, IT: *IT Governance für Geschäftsführer und Vorstände*. http://www.isaca.org/Knowledge-Center/Research/Documents/BoardBriefing/Boardbriefing_German.pdf(abgerufen am 22.02.2011).
- [29] GOVERNATORI, GUIDO, ZORAN MILOSEVIC und SHAZIA SADIQ: *S.: Compliance checking between business processes and business contracts*. In: *Proceedings of the 10th IEEE Conference on Enterprise Distributed Object Computing*, 2006.
- [30] GREGOR WECKER, HENDRIK VAN LAAK (HRSG.): *Compliance in der Unternehmerpraxis. Grundlagen, Organisation und Umsetzung*. GWV Fachverlage GmbH, Wiesbaden, 2008.
- [31] HARRIS, JAMES und MAEVE CUMMINGS: *Compliance issues and IS degree programs*. J. Comput. Small Coll., 23:14–20, October 2007.
- [32] HAUSCHKA, CHRISTOPH E.: *Corporate Compliance. Handbuch der Haftungsvermeidung im Unternehmen*. Beck, München, 2., neu bearb. Auflage Auflage, 2007.

- [33] HILDEBRAND, KNUT und STEFAN MEINHARDT (Herausgeber): *Compliance Risk Management*. HMD. dpunkt, Heidelberg, 2008.
- [34] HILTY, M., A. PRETSCHNER, D. BASIN, C. SCHAEFER und T. WALTER: *A Policy Language for Distributed Usage Control*. Seiten 531–546. 2008.
- [35] HOFFMANN, LUDGER: *Wie verständlich können Gesetze sein*. In: GREWENDORF, GÜNTHER (Herausgeber): *Rechtskultur als Sprachkultur*, Seiten 122–157. Frankfurt, 1992.
- [36] HOFSTEDDE, A. M. TER, W. M. P. VAN DER AALST, M. ADAMNS und N. RUSSELL (Herausgeber): *Modern Business Process Automation: YAWL and its Support Environment*. Springer, 2010.
- [37] HOHFELD, WESLEY NEWCOMB: *Fundamental Legal Conceptions as Applied in Judicial Reasoning, and other legal essays*. Yale University Press, 1920.
- [38] HOUMB, SIV, SHAREEFUL ISLAM, ERIC KNAUSS, JAN JÜRJENS und KURT SCHNEIDER: *Eliciting security requirements and tracing them to design: an integration of Common Criteria, Heuristics, and UMLsec*. Requirements Engineering.
- [39] INFORMATIONSTECHNIK, BUNDESAMT FÜR SICHERHEIT IN DER: *BSI-IT-Grundschatz-Kataloge, 11. Ergänzungslieferung*, 2009.
- [40] ISLAM, SAHREEFUL, HARALAMBOS MOURATIDIS und JAN JÜRJENS: *A framework to support alignment of secure software engineering with legal regulations*. Software and Systems Modeling, March 2010.
- [41] ISLAM, SHAREEFUL und JAN JÜRJENS: *Incorporating Security Requirements from Legal Regulations into UMLsec model*. Requir. Eng., 15(1), 2010.
- [42] JÜRJENS, JAN: *Secure Systems Development with UML*. SpringerVerlag, 2003.
- [43] KAGAL, LALANA, TIM FININ und ANUPAM JOSHI: *A Policy Language for a Pervasive Computing Environment*. In: *Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks, POLICY '03*, Seiten 63–, Washington, DC, USA, 2003. IEEE Computer Society.
- [44] KAPPES, MARTIN: *Netzwerk- und Datensicherheit*. Vieweg+Teubner, 2007.
- [45] KELLER, A. und H. LUDWIG: *Policy-basiertes Management: State-of-the-Art und zukünftige Fragestellungen*. PIK - Praxis der Informationsverarbeitung und Kommunikation, Band 27, Heft 2, 2004.

- [46] KERRIGAN, SHAWN und KINCHO H. LAW: *Logic-based regulation compliance-assistance*. In: *Proceedings of the 9th international conference on Artificial intelligence and law*, ICAIL '03, Seiten 126–135, New York, NY, USA, 2003. ACM.
- [47] KERSTEN, HEINRICH, JÜRGEN REUTER und KLAUS-WERNER SCHRÖDER: *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung*. Vieweg+Teubner, 1 Auflage, Oktober 2007.
- [48] KEUNE, CHRISTINA: *Neufassung der MaRisk BA und Rechtsnatur der MaRisk VA*. <http://www.ivr-blog.de/category/versicherungsaufsichtsrecht> (abgerufen am 27.04.2011).
- [49] KÄHMER, M.: *ExPDT. Vergleichbarkeit von Richtlinien für Selbstregulierung und Selbstdatenschutz*. Vieweg + Teubner, 1st Auflage, Wiesbaden 2010.
- [50] KIYAVITSKAYA, NADZEYA, ALZBETA KRAUSOVÁ und NICOLA ZANNONE: *Why Eliciting and Managing Legal Requirements Is Hard*. In: *RELAW '08: Proceedings of the 2008 Requirements Engineering and Law*, Seiten 26–30, Washington, DC, USA, 2008. IEEE Computer Society.
- [51] KLEMENT, STEFAN: *Entwicklung und Einsatz von Security Policies*. Diplomarbeit, Johannes Kepler Universität Linz, 2006.
- [52] KRUMM, HEIKO: *Policies zum automatisierten technischen Netz-, System- und Anwendungsmanagement*. Forschungsbericht GFFT-2007-002 2007, GFFT e.V., 2003.
- [53] LORCH, MARKUS, SETH PROCTOR, REBEKAH LEPRO, DENNIS KAFURA und SUMIT SHAH: *First experiences using XACML for access control in distributed systems*. In: *Proceedings of the 2003 ACM workshop on XML security*, XMLSEC '03, Seiten 25–37, New York, NY, USA, 2003. ACM.
- [54] LÖSLER, THOMAS: *Das moderne Verständnis von Compliance im Finanzmarktrecht*. De Gruyter Recht, Berlin, 2005.
- [55] LUDWIG, BERND PETER: *IT-Governance,-Risk Management und -Compliance: Ein GRC-Modell für die IT von KMU*. www.global-it-security.com (abgerufen am 03.05.2011).
- [56] LUPU, EMIL, MORRIS SLOMAN, NARANKER DULAY und NICODEMOS DAMIANOU: *Ponder: Realising Enterprise Viewpoint Concepts*. In: *Proceedings of the 4th International conference on Enterprise Distributed Object Computing*, EDOC '00, Seiten 66–75, Washington, DC, USA, 2000. IEEE Computer Society.
- [57] MANNING, WILLIAM: *CEH Certified Ethical Hacker Certification Exam Preparation*. Emereo Publishing, 2009.

- [58] MCCARTY, L. THORNE: *A language for legal Discourse I. basic features*. In: *Proceedings of the 2nd international conference on Artificial intelligence and law, ICAIL '89*, Seiten 180–189, New York, NY, USA, 1989. ACM.
- [59] MILOSEVIC, ZORAN, SHAZIA WASIM SADIQ und MARIA E. ORLOWSKA: *Translating business contract into compliant business processes*. In: *2006 10th IEEE International Enterprise Distributed Object Computing Conference (EDOC'06)*, Seiten 211–220. IEEE, December 2006.
- [60] MÜLLER, KLAUS-RAINER: *Handbuch Unternehmenssicherheit; umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System*. Viewveg+Teubner, Wiesbaden, 2., neu bearb. Auflage Auflage, 2010.
- [61] MOORE, B.: *Request for Comments 3460. Policy Core Information Model (PCIM) Extensions*, 2003.
- [62] MORRISON, EVA, ADITYA GHOSE und GEORGE KOLIADIS: *Dealing with imprecise compliance requirements*. In: *Enterprise Distributed Object Computing Conference Workshops, 2009. EDOCW 2009. 13th*, Seiten 6 –14, 2009.
- [63] MOUCHTCHININA, MARIA: *Recht des geistigen Eigentums: Zur Fachterminologie im russischen und deutschen Urheberrecht*. <http://rechtsinformatik.jura.uni-sb.de/portal/diplomarbeiten/mouchtchinina/RS-als-FS.pdf> (abgerufen am 22.08.2010).
- [64] OTTO, P.N. und A.I. ANTON: *Addressing Legal Requirements in Requirements Engineering*. Seiten 5 –14, oct. 2007.
- [65] PESCHKE, MARC.: *Werkzeuggestützte Modell-basierte Sicherheitsanalyse für IT-Sicherheitsmanagement*. Diplomarbeit, TU Dortmund, Fraunhofer ISST, September 2010.
- [66] RATH, MICHAEL: *Rechtliche Aspekte von IT-Compliance*. http://www.dsri.de/veranstaltungen/it-compliance/it-compliance_2007-materialien.html (abgerufen am 06.03.2011).
- [67] REGIERUNGSKOMMISSION: *Deutscher Corporate Governance Kodex. Fassung vom 26. Mai 2010*. <http://www.corporate-governance-code.de/> (abgerufen am 12.03.2011).
- [68] ROSS, STEVEN J.: *Automating Compliance*. <http://www.isaca.org/Journal/Past-Issues/2007/Volume-5/Pages/Automating-Compliance1.aspx> (abgerufen am 20.02.2011=).

- [69] ROTH, JÖRG: *Pervasive Computing*. Seminar 01909 im Wintersemester 2005/2006. FernUniversität Hagen. <http://www.wireless-earth.de/teaching/FUseminarWS0506.pdf> (abgerufen am 14.05.2011).
- [70] SACKMANN, STEFAN, MARTIN KÄHMER, MAIKE GILLIOT und LUTZ LOWIS: *A Classification Model for Automating Compliance*. In: *Proceedings of the 2008 10th IEEE Conference on E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services*, Seiten 79–86, Washington, DC, USA, 2008. IEEE Computer Society.
- [71] SADIQ, SHAZIA, GUIDO GOVERNATORI und KIOUMARS NAMIRI: *Modeling Control Objectives for Business Process Compliance*. In: *Business Process Management*, Band Volume 4714/2007, Seiten 149–164. Springer Berlin / Heidelberg, 2007.
- [72] SANDER, GERALD G.: *Deutsche Rechtsprache: Ein Arbeitsbuch*. UTB, 1. Auflage, 2004.
- [73] SARTOR, GIOVANNI: *Fundamental legal concepts: a formal and teleological characterisation*. *Artif. Intell. Law*, 14:101–142, April 2006.
- [74] SCHAHINIAN, DAVID: *Interview mit Frankfurter Unwort-Professor / Sprachliche Besonderheiten im Einkauf*. <http://www.bme-rmr.de/news.php?item=523> (abgerufen am 28.02.2011).
- [75] SCHNEIER, BRUCE: *Secrets and Lies: Digital Security in a Networked World*. Wiley, 1. Auflage, January 2004.
- [76] SCHULEV-STEINDL, EVA: *Subjektive Rechte als rechtliche Positionen*. In: RASCHAUER, BERNHARD, GÜNTHER WINKLER und WALTER ANTONIOLLI (Herausgeber): *Subjektive Rechte*, Band 162 der Reihe *Forschungen aus Staat und Recht*, Seiten 101–147. Springer Vienna, 2008. 10.1007/978-3-211-09438-9_5.
- [77] SHIREY, R.: *Request for Comments 2828. Internet Security Glossary*, Mai 2000.
- [78] SIENA, ALBERTO, JOHN MYLOPOULOS, ANNA PERINI und ANGELO SUSI: *From Laws to Requirements*. *Requirements Engineering and Law*, 0:6–10, 2008.
- [79] SPONHOLZ, MICHAEL RATH ; RAINER (Herausgeber): *IT-Compliance: erfolgreiches Management regulatorischer Anforderungen*. ESV. Erich Schmidt Verlag, Berlin, 2009.
- [80] STECK, GUNNAR: *Die Regulierung der U.S. Wirtschaftsprüfung nach Enron*. REGEM Analysis No. 12, October 2004, Trier University. http://www.chinapolitik.de/studien/regem/regem_no12.pdf (abgerufen am 06.11.2011).

- [81] STEFANIE, RINDERLE-MA, LY LINH THAO und DADAM PETER: *Business Process Compliance (Aktuelles Schlagwort)*. EMISA Forum, 2(2008):24–29, 8 2008.
- [82] STURM, DETLEV: *Policy-Management*. <http://soa-know-how.de/index.php> (abgerufen am 05.03.2011).
- [83] TASHI, IGLI: *Regulatory Compliance and Information Security Assurance*. In: *ARES*, Seiten 670–674, 2009.
- [84] TESNIERE, LUCIEN: *Elements de Syntaxe Structurale*. Libraire C. Klincksieck, Paris, 2 Auflage, 1976.
- [85] THAO, LY LINH, GÖSER KEVIN, STEFANIE RINDERLE-MA und DADAM PETER: *Compliance of Semantic Constraints - A Requirements Analysis for Process Management Systems*. In: *Proc. 1st Int'l Workshop on Governance, Risk and Compliance - Applications in Information Systems (GRCIS'08)*, 2008.
- [86] UNGER, ULRIKE: *Der Anglizismus Compliance*. <http://blog.beck.de/2009/12/08/der-anglizismus-compliance> (abgerufen am 01.03.2011).
- [87] WAGNER, ANNE: *Introduction: The (Ab)use of Language in Legal Discourse*. International Journal for the Semiotics of Law, 15:323–324, 2002. 10.1023/A:1021295127333.
- [88] YIP, FREDERICK, NANDAN PARAMESWARAN und PRADEEP RAY: *Rules and Ontology in Compliance Management*. In: *EDOC*, Seiten 435–442, 2007.
- [89] YIP, FREDERICK, PRADEEP RAY und NANDAN PARAMESH: *Enforcing Business Rules and Information Security Policies through Compliance Audits; XISSF - A Compliance Specification Mechanism*. In: *Business-Driven IT Management, 2006. BDIM '06. The First IEEE/IFIP International Workshop on*, Seiten 81 – 90, 2006.
- [90] YIP, FREDERICK, ALFRED KA YIU WONG, NANDAN PARAMESWARAN und PRADEEP RAY: *Towards Robust and Adaptive Semantic-Based Compliance Auditing*. In: *EDOCW '07: Proceedings of the 2007 Eleventh International IEEE EDOC Conference Workshop*, Seiten 181–188, Washington, DC, USA, 2007. IEEE Computer Society.
- [91] YIP, FREDERICK, ALFRED KA YIU WONG, NANDAN PARAMESWARAN und PRADEEP RAY: *Semantic-Based Fuzzy Reasoning for Compliance Auditing*. In: *ICSC*, Seiten 299–306, 2008.
- [92] YIP, FREDERICK, ALFRED KA YIU WONG, PRADEEP RAY und NANDAN PARAMESH: *Corporate Security Compliance in a Heterogeneous Environment*. In: *NOMS*, 2006.

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst habe und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet sowie Zitate kenntlich gemacht habe.

Dortmund, den 21. Mai 2011

Elena-Crina Bostan