technische universität
dortmund

Diplomarbeit

Ontologie-basierte Modellierung ausgewählter Compliance-Regelwerke mit Anforderungserhebung zur Toolauswahl

Christine Sarah Stahl
November 2011

Gutachter:
Prof. Dr. Jan Jürjens
Dr. Sven Wenzel

Technische Universität Dortmund
Fakultät für Informatik
Lehrstuhl Software Engineering (LS14)
http://ls14-www.cs.tu-dortmund.de/

In Kooperation mit:
Fraunhofer Institut für
Software- und Systemtechnik (ISST)

Inhaltsverzeichnis

1 Einleitung **1**

1.1 Motivation und Hintergrund . . . 1
1.2 Verwandte Arbeiten . . . 3
1.2.1 Fenz und Ekelhart - *Formalizing Information Security Knowledge* . . . 3
1.2.2 Schmidt, Bartsch und Oberhauser - *Ontology-based representation of compliance requirements for service processes* . . . 4
1.2.3 Arbeiten von *Fellman* und *Thomas* . . . 5
1.2.4 Fazit . . . 6
1.3 Aufbau der Arbeit . . . 6

2 Grundlagen **7**

2.1 Compliance . . . 7
2.1.1 Mindestanforderungen an das Risikomanagement . . . 9
2.1.2 ISO-Standards . . . 10
2.1.3 BSI IT-Grundschutz-Kataloge und BSI-Standards . . . 12
2.1.4 Bundesdatenschutzgesetz . . . 14
2.2 Ontologien . . . 14
2.2.1 Definition . . . 15
2.2.2 Arten von Ontologien . . . 17
2.2.3 Ontologiesprachen . . . 17
2.2.4 Legal Ontologies . . . 19

3 Modellierung der Ontologie **21**

3.1 Vorgehensweise . . . 21
3.1.1 Konventionen . . . 21
3.2 Analyse und Modellierung der Regelwerke . . . 22
3.2.1 Regelwerke . . . 22
3.2.2 Regeln . . . 23
3.2.3 Relationen . . . 26
3.3 Elemente der Regelwerke . . . 33
3.3.1 Beschreibung der Elemente . . . 34
3.3.2 Relationen zwischen den Elementen . . . 36
3.4 Relationen zwischen Regeln und Elementen . . . 38
3.4.1 Beschreibung der Relationen . . . 39
3.5 Zusammenfassung . . . 43

4 Anforderungserhebung und Toolauswahl **45**
4.1 Ontologie-Tools . . . 45
4.2 Vorgehensweise Toolauswahl . . . 46
4.3 Erste Phase: Vorauswahl . . . 47
4.4 Zweite Phase: Anforderungserhebung und Bewertungsschema . . . 48
4.4.1 Bewertungsschema für die Anforderungen . . . 48
4.4.2 Beschreibung der Anforderungen . . . 49
4.4.3 Einordnung der Anforderungen . . . 53
4.5 Dritte Phase: Toolauswahl . . . 54
4.5.1 Tools . . . 54
4.5.2 Bewertung . . . 59
4.6 Protégé . . . 59
4.6.1 Variantenauswahl . . . 60
4.6.2 Sprachenauswahl . . . 61
4.7 Zusammenfassung . . . 62

5 Umsetzung und Evaluierung **63**
5.1 Umsetzung der Ontologie in Protégé . . . 63
5.1.1 Konventionen . . . 63
5.1.2 Relationen in Protégé . . . 64
5.2 Evaluierung . . . 65
5.2.1 SPARQL . . . 65
5.2.2 Beispielszenario 1: Vertraulichkeit . . . 67
5.2.3 Beispielszenario 2: Risikomanagement . . . 69
5.2.4 Beispielszenario 3: Geschäftsprozess . . . 72
5.3 Zusammenfassung . . . 75

6 Zusammenfassung und Ausblick **77**
6.1 Zusammenfassung . . . 77
6.2 Bewertung . . . 78
6.3 Ausblick . . . 78

A Anhang **81**
A.1 Beispielszenario: Vertraulichkeit . . . 81
A.1.1 Gefährdungen für Vertraulichkeit . . . 81
A.1.2 Maßnahmen für Vertraulichkeit . . . 82
A.2 Beispielszenario: Risikomanagement . . . 83
A.2.1 Regeln für Teilprozesse von *Risikomanagement* . . . 83
A.2.2 Regeln für die Unterkonzepte von *Risikobehandlung* . . . 84
A.2.3 Regeln für die Unterkapitel von *MaRiskVA_Kap7* . . . 85
A.2.4 Regeln für die Unterunterkapitel von *MaRiskVa_Kap7* . . . 85
A.2.5 Regeln für die Unterkapitel von *MaRiskVA_Kap7.2.2* . . . 85
A.2.6 Regeln für die Unterkapitel von *MaRiskVA_7.3.2* . . . 86
A.3 Beispielszenario: Geschäftsprozess . . . 87
A.3.1 Dokumentation . . . 87
A.3.2 Speicherung . . . 90
A.3.3 Drucken . . . 91
A.3.4 Archivierung . . . 91
A.3.5 Vernichtung . . . 92

A.3.6 Scan 93
A.3.7 Sicherung 94
A.3.8 Löschung 95

Abbildungsverzeichnis **97**

Literaturverzeichnis **102**

Erklärung **103**

Kapitel 1

Einleitung

Dieses Kapitel stellt zunächst die Motivation, die Problemstellung und das Ziel dieser Diplomarbeit vor. Anschließend folgt ein kurzer Überblick über verwandte Arbeiten, sowie der Aufbau der Diplomarbeit.

1.1 Motivation und Hintergrund

Im Jahr 2011 gab es eine Vielzahl von Angriffen auf Systeme großer Unternehmen, wobei Millionen Daten von Kunden entwendet wurden. Bekanntestes Beispiel waren die Angriffe auf Sony (siehe [Eik11]). Zu den Arten der Angriffe zählten dabei sowohl *Denial-of-Service*-Attacken, bei denen die Server gezielt mit Anfragen überlastet wurden, als auch Server-Einbrüche über *SQL-Injections*. Das ist ein Angriff, bei dem gezielt SQL-Befehle eingeschleust werden, um so Datenbanken zu manipulieren. Die Ursachen für die Verwundbarkeit sehen die Experten dabei in Versäumnissen der Unternehmen, die nicht genug für die Sicherheit der Systeme investieren. So wird der Datenschutzbeauftragte des Landes Niedersachens zitiert:

> „Bei unseren Kontrollen stellen wir regelmäßig fest, dass Betreiber die in §9 Bundesdatenschutzgesetz vorgeschriebenen technisch organisatorischen Maßnahmen im Bereich Telemedien oft nur ungenügend umsetzen. Nach unseren Erkenntnissen mangelt es oft an der nötigen Sachkunde der Betreiber, wenn Telemedien nicht ausreichend gesichert sind."

Und ein anderer Experte, John Howie von Microsoft, kritisiert:

> „Sony wurde zu Fall gebracht, weil sie ihre Server nicht gepatcht, veraltete Software eingesetzt und schlecht programmiert haben. Das sind Anfängerfehler."

Leidtragende bei solchen Angriffen sind neben den Unternehmen selbst auch deren Kunden. In einem Artikel ([Sch10]) über Sicherheitslücken in den Webseiten von Banken, die von einem 16-jährigen Schüler aufgedeckt wurden, wird bemängelt, dass die Banken „elementare Sicherheitsrichtlinien" missachten. Bei einem weiteren Test drei Monate nach dem Erscheinen des Artikels wurden immer noch ernste Sicherheitsprobleme bei den Webseiten entdeckt ([Sch11]). Vor allem Banken und Versicherungen sind dabei äußerst sensible Branchen aufgrund ihres notwendigen Umgangs mit personenbezogenen Daten. Diese Probleme zeigen, dass es für Unternehmen notwendig ist ein angemessenes Sicherheitsniveau zu etablieren. Für die Sicherheit von IT-Systemen gibt es dabei eine Reihe von Standards,

die helfen können Gefährdungen im Voraus zu identifizieren. Sie bieten außerdem Maßnahmen anhand derer Vorkehrungen getroffen werden können, die verhindern sollen, dass z.B. personenbezogene Daten durch Fehler in IT-Systemen in die falschen Hände geraten.

2007 gab es eine Finanzkrise, die ausgehend von den USA auch weitreichende Auswirkungen auf den europäischen Finanzmarkt hatte (nähere Informationen z.B. in [Ins09]). Diese Krise hat dabei auch gezeigt, dass durch die weltweite Vernetzung der Märkte und Abhängigkeiten untereinander, die Auswirkungen der Krisen einzelner Unternehmen globale Folgen haben können. Aus diesem Grund existieren für diese Bereiche Regularien, die versuchen die negativen Auswirkungen präventiv zu reduzieren, indem die Unternehmen ein angemessenes Risikomanagement einrichten. Auch im Versicherungsbereich, dessen Geschäftsmodell auf der Kalkulation von Risiken besteht, ist das passende Risikomanagement von großer Bedeutung, um auf besondere Ereignisse vorbereitet zu sein.

Unternehmen sehen sich somit immer mehr Regularien, Gesetzen und Standards ausgesetzt, die die unterschiedlichsten Bereiche der Unternehmen betreffen. Durch die Vielzahl dieser Regeln wird es immer schwieriger den Überblick über diese zu bewahren und solche Regeln zu identifizieren, die in einem bestimmten Fall von Bedeutung sind und eingehalten werden müssen. Dabei gibt es zwischen verschiedenen Regelwerken durchaus Überschneidungen und das Potenzial sich gegenseitig zu unterstützen, um so effektiver Maßnahmen zur Einhaltung bestimmter Regeln treffen zu können.
Bedingt durch die unterschiedlichen Bereiche, aus denen die Regelwerke kommen und auf die sich diese beziehen, bilden sich verschiedene Problematiken heraus, die beachtet werden müssen:

- **Sprache:** Die Regelwerke sind in natürlicher Sprache formuliert und wurden für unterschiedliche Branchen entwickelt. Dadurch ergeben sich unterschiedliche Begrifflichkeiten für eventuell gleiche Sachverhalte. Zudem können Regelwerke auch in unterschiedlichen Sprachen vorliegen, je nachdem in welchen Ländern ein Unternehmen operiert oder für welchen Bereich das Regelwerk entwickelt wurde (national/international).

- **Detailebene:** Je nach Regelwerk sind die Formulierung und die Detailtiefe sehr abstrakt, um Interpretationsspielraum zu lassen, oder auch sehr spezifisch, um eine konkrete Anleitung zur Umsetzung zu liefern.

- **Dynamik:** Regelwerke verändern sich regelmäßig, weil sie überarbeitet und neuen Gegebenheiten angepasst werden müssen.

- **Unterschiedliche Verbindlichkeit:** Manche Regelwerke sind verpflichtend einzuhalten, während andere freiwillig umgesetzt werden können.

Einen wichtigen Platz in Unternehmensabläufen nehmen Geschäftsprozesse ein. Diese beschreiben elementare Prozessabläufe und dienen z.B. als Wegweiser beim Treffen von Entscheidungen. Bei den einzelnen Schritten der Geschäftsprozesse kann sich die Notwendigkeit ergeben Regeln der Regelwerke zu beachten und einzuhalten oder unterstützende Maßnahmen umzusetzen.
Die Beziehungen zwischen den Regelwerken und zwischen den Regeln und Geschäftsprozessen können genutzt werden, um eine effizientere Unterstützung bei der Umsetzung der Regelwerke im Unternehmen zu erhalten. So können Hinweise auf Regeln gegeben werden,

die unter Umständen beachtet werden müssen. Angesichts der Vielzahl von Regeln wäre es daher von Vorteil dies durch maschinelle Hilfe effektiver gestalten zu können. Für eine maschinelle Unterstützung könnte durch die Modellierung semantischer Beziehungen zwischen den Regelwerken einen Ansatz gefunden werden, den vorher genannten Problemen zu begegnen und eine Lösung für diese zu finden. Semantische Beziehungen zwischen zwei Objekten bieten den Vorteil, dass bei unterschiedlichen Sprachen ein Bezug zwischen zwei Regelwerken hergestellt werden kann. Das wäre bei bloßem Vergleichen der Begriffe wegen der unterschiedlichen Sprachen sonst nicht möglich.
Eine Möglichkeit diese semantischen Beziehungen zwischen den Regelwerken darzustellen, wäre der Einsatz von Ontologien. Ontologien sind eine Form, um Wissen zu repräsentieren. Diese bieten den Vorteil eigene Relationen mit semantischem Kontext definieren zu können und werden zudem durch eine breite Auswahl an Tools unterstützt, mit denen sich eine Ontologie umsetzen lässt.

Ziel dieser Diplomarbeit ist es daher aus der Analyse verschiedener Arten von ausgewählten Regelwerken eine Ontologie zu modellieren. Dabei soll durch die Modellierung die Darstellung semantischer Beziehungen zwischen den verschiedenen Regelwerken ermöglicht sowie für einen Geschäftsprozess die relevanten Regeln identifiziert werden können. Anhand dieser Modellierung werden dann Anforderungen an ein Ontologie-Tool definiert. Auf der Grundlage dieser Anforderungen werden Ontologie-Tools verglichen und schlussendlich ein Tool ausgewählt werden, mit dem die modellierte Ontologie dann exemplarisch umgesetzt wird. Anhand mehrerer Beispielszenarien wird die Ontologie zudem evaluiert.

1.2 Verwandte Arbeiten

In diesem Abschnitt sollen thematisch ähnliche Arbeiten vorgestellt werden und eine Abgrenzung zu dieser Diplomarbeit stattfinden. Die Arbeiten bieten ontologie-basierte Ansätze und Methoden, die im Bereich von Compliance und Geschäftsprozessen mit unterschiedlichen Schwerpunkten zur Unterstützung entwickelt wurden.

1.2.1 Fenz und Ekelhart - *Formalizing Information Security Knowledge*

Der Artikel von Fenz und Ekelhart [FE09] beschreibt die Formalisierung von Wissen über Informationssicherheit in einer Ontologie, der *Security Ontology*. Der Fokus liegt dabei auf dem Risikomanagement der Informationssicherheit. Die Ontologie besteht aus 500 Konzepten und 600 formalen Einschränkungen, welche auf der Grundlage von Richtlinien oder Standards aus dem Bereich Informationssicherheit und organisationsspezifischem Wissen formalisiert wurden.
Die Abbildung 1.1 zeigt einen Ausschnitt aus der Ontologie mit den wichtigsten Informationssicherheitskonzepten (*Asset*, *Threat*, *Control*, *Vulnerability*). Die Konzepte werden in drei Unterontologien unterteilt: *Security*, *Enterprise* und *Location*. Um weiteres Wissen über die Informationssicherheit neben den Relationen in der Ontologie formal zu modellieren, wurden formale Axiome hinzugefügt.
Auf der Basis dieser Ontologie ist es möglich Anfragen zu stellen, z.B. welche *Assets* von einer bestimmten Gefahr (*Threat*) bedroht sind.

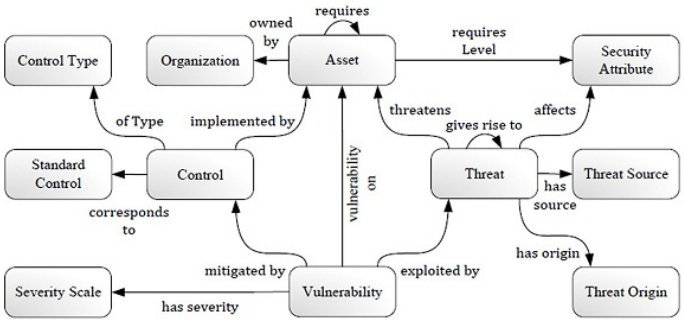

Abbildung 1.1: Ausschnitt aus der *Security Ontology*

1.2.2 Schmidt, Bartsch und Oberhauser - *Ontology-based representation of compliance requirements for service processes*

In der Arbeit *Ontology-based representation of compliance requirements for service processes* ([SBO07]) von Schmidt, Bartsch und Oberhauser wird eine Repräsentation von Compliance-Anforderungen und Serviceprozessen in Form von Ontologien vorgestellt. So ist es möglich die Serviceprozesse auf die Einhaltung der Anforderungen zu prüfen.
Es werden in der Arbeit zwei Ontologien definiert: eine Prozess-Ontologie und eine Compliance-Ontologie. Die Prozess-Ontologie ist die Basis für die Repräsentation der Serviceprozesse. Die Compliance-Ontologie repräsentiert Anforderungen an die Serviceprozesse, die diese erfüllen müssen. Es wird zwischen drei Arten von Anforderungen unterschieden: syntaktische, semantische und pragmatische Anforderungen.

- Syntaktische Anforderungen sind Regeln für die Beschreibung der Serviceprozesse.
- Semantische Anforderungen verlangen das Vorhandensein bestimmter Objekte oder Strukturen in den Prozessdefinitionen.
- Pragmatische Anforderungen beschreiben Ziele, die in dem Serviceprozess realisiert werden müssen.

Die Abbildung 1.2 zeigt ein Anwendungsszenario aus [SBO07]. Der Serviceprozess wird mit Hilfe der Prozess-Ontologie in eine ontologie-basierte Prozessrepräsentation gebracht. Die Überprüfung auf Compliance geschieht über die Klassifizierung der Prozesselemente durch einen *Reasoner*. Dieser überprüft, ob die notwendigen und zu erfüllenden Bedingungen von Anforderungen der Compliance-Ontologie erfüllt und daher diesen zugeordnet werden können. Erfüllte Anforderungen werden mit Instanzen assoziiert. Die Anforderungen, die nach der Klassifizierung keine Instanzen haben, werden von dem Prozess nicht erfüllt.

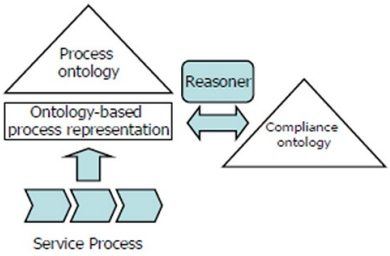

Abbildung 1.2: Anwendungsszenario aus [SBO07]

1.2.3 Arbeiten von *Fellman* und *Thomas*

Die Arbeiten [TF06b], [TF06a], [TF07] und [TFM09] beschäftigen sich mit der ontologiebasierten Repräsentation von Geschäftsprozessen, die in Form von *Ereignisgesteuerten Prozessketten* oder der *Business Process Model and Notation (BPMN)* vorliegen. Diese Repräsentation soll z.B. die Suche und Navigation in Modelldatenbanken erleichtern und neue Validierungsmöglichkeiten der Prozessmodelle eröffnen.
Die grundlegende Idee dieser Arbeiten ist die Erweiterung von Prozessmodellierungssprachen durch eine Ontologie. Die vorliegende Problematik bei den Prozessmodellen ist, dass die Prozesselemente in natürlicher Sprache formuliert sind, was zu Interpretationsspielräumen führt und daher eine maschinelle Verarbeitung erschwert. Diese Prozesselemente sollen in dem Ansatz durch formale Begriffe einer Ontologie repräsentiert werden. Die Prozessmodelle sind gerichtete Graphen. Die Knoten werden in der Ontologie als Konzepte interpretiert und die Beziehungen zwischen den Knoten als Relationen.
Das erweiterte Modell ist mehrstufig. Es besteht aus der Prozessebene, einer Metadatenebene und der Ontologieebene. Die Prozessebene enthält das Modell des Geschäftsprozesses, die Ontologieebene enthält die relevanten Konzepte, Instanzen und Beziehungen eines Unternehmenskontextes und die Metadatenebene stellt die Verbindung zwischen der Prozess- und der Ontologieebene her.
Die Abbildung 1.3 zeigt dieses mehrstufige Modell anhand eines Geschäftsprozesses.

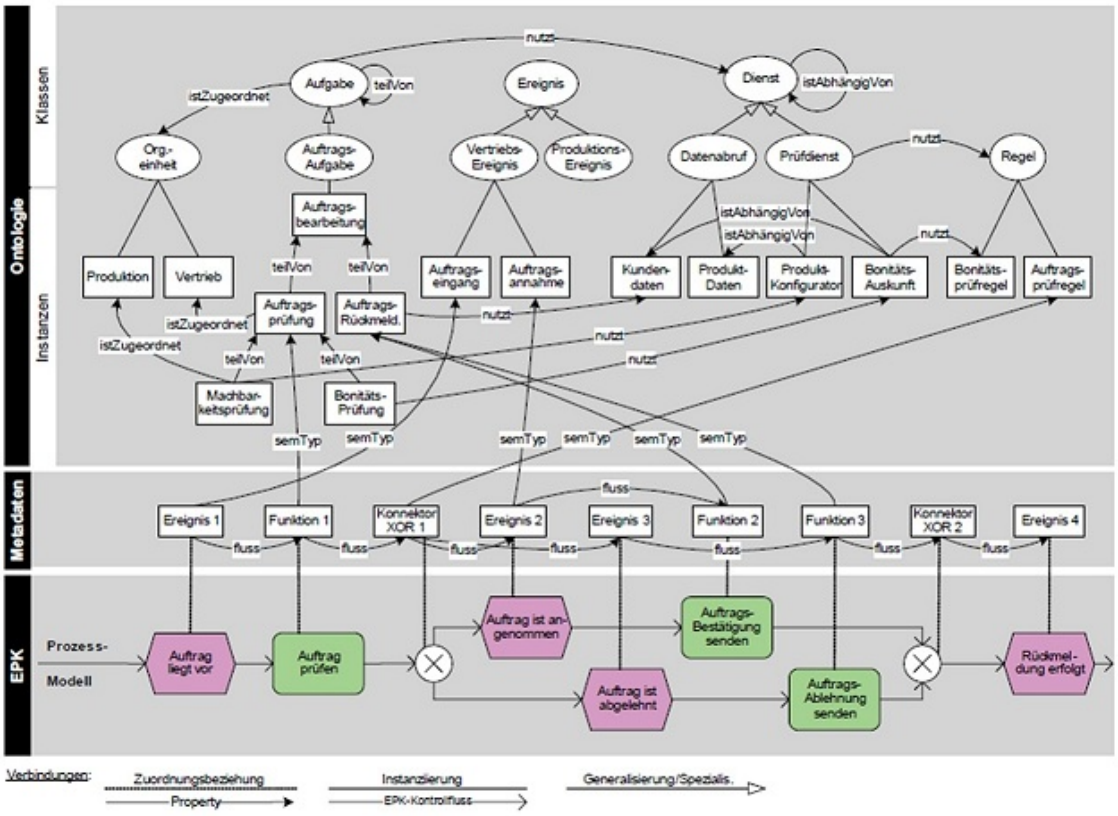

Abbildung 1.3: Semantische *Ereignisgesteuerte Prozesskette* [TF06b]

1.2.4 Fazit

Die präsentierten Arbeiten zeigen Möglichkeiten auf wie Geschäftsprozesse oder auch einzelne Regelwerke in Form einer Ontologie repräsentiert werden können. Es wurde eine Ontologie für Wissen über Informationssicherheit vorgestellt sowie Ansätze, die es erlauben Prozesse mit einer Ontologie zu formalisieren. So können diese Prozesse mit Anforderungen verglichen oder die Geschäftsprozesse auf Korrektheit überprüfen werden.
Diese Ansätze konzentrieren sich entweder schwerpunktmäßig auf die Darstellung der Prozesse oder nur auf einen bestimmten Themenbereich von Regelwerken. Sie liefern keine Ansätze für die Beziehungen zwischen mehreren unterschiedlichen Regelwerken sowie keine Hilfe bei der Frage, welche Regeln in Geschäftsprozessen beachtet werden müssen.

1.3 Aufbau der Arbeit

Kapitel 2 beschäftigt sich mit den Grundlagen für diese Diplomarbeit. Es wird auf den Begriff *Compliance* eingegangen und die relevanten Regelwerke beschrieben und eingeordnet. Darüber hinaus wird ein Überblick über den Bereich Ontologien gegeben. Dazu gehören die Begriffsdefinition, ein Überblick über Ontologiesprachen und der spezielle Bereich der *Legal Ontologies*. Kapitel 3 beschreibt die Analyse der betrachteten Regelwerke und ihre Modellierung in einer Ontologie. Aufbauend auf diesen Überlegungen werden in Kapitel 4 Anforderungen erhoben und ein Bewertungsschema erstellt. Anschließend wird aus einer Aufstellung vorhandener Ontologie-Tools ein passendes Tool bewertet und ausgewählt. In Kapitel 5 wird die Umsetzung der in Kapitel 3 entwickelten Ontologie mit Hilfe des in Kapitel 4 ausgewählten Tools anhand von mehreren Beispielszenarien evaluiert. Das letzte Kapitel dient einer Zusammenfassung und Bewertung der Ergebnisse sowie einem Ausblick auf mögliche Verbesserungen und weitergehende Aspekte.

Kapitel 2

Grundlagen

Dieses Kapitel soll einen Überblick über die Bereiche der Compliance und der Ontologien geben. Zunächst wird der Begriff Compliance eingehender erläutert und die in dieser Diplomarbeit betrachteten Regelwerke vorgestellt und thematisch eingeordnet. Dann wird der Begriff der Ontologie erklärt und es werden für die Diplomarbeit wichtige Aspekte vorgestellt. Dazu gehören die Ontologiesprachen und der Bereich der *Legal Ontologies*.

2.1 Compliance

Unter dem Begriff Compliance wird „die Einhaltung gesetzlicher und aufsichtsrechtlicher Regelwerke oder auch freiwilliger Kodizes“ verstanden[Hil08]. Der Begriff *Regelwerk* wird im weiteren Verlauf als Oberbegriff für die verschiedenen Arten von Regelwerken wie Gesetze, Standards und Richtlinien benutzt. Nur wenn eine genauere Unterscheidung der Art in dem zugehörigen Kontext notwendig ist, wird diese spezifiziert werden.
Die Anzahl sowie die Arten der relevanten Regelwerke ist von Unternehmen zu Unternehmen unterschiedlich. Es gibt sowohl Gesetze auf staatlicher Ebene, bei denen ein Unternehmen verpflichtet ist sie einzuhalten, als auch Gesetze nur auf Bundesländerebene. Dabei hängt es vom Standort des Unternehmens, seiner Tochtergesellschaften oder der Dienstleister für das Unternehmen ab, welche Gesetze relevant sind. Dann existieren noch Richtlinien, die auf bestimmte Branchen (z.B. Banken- oder Versicherungsbranche) abgestimmt sind und daher auch nur für Unternehmen aus diesen Branchen von Relevanz sind. Ein weiterer Faktor sind freiwillige Regelwerke wie verschiedene Arten von Standards, bei denen das Unternehmen selbst entscheiden kann, ob es diese umsetzen und erfüllen möchte. Ein Vorteil von diesen Standards ist, dass diese Anleitungen zur Verfügung stellen, welche Aspekte in bestimmten Bereichen beachtet werden müssen und welche Maßnahmen es für diese Aspekte gibt.
Einen weiteren Anreiz bieten Zertifikate für die Erfüllung der Regelwerke, die von Unternehmen bei Verhandlungen mit potenziellen Kooperationspartnern oder bei der eigenen Vermarktung als zusätzlicher Anreiz für das Unternehmen genannt werden können. Unternehmen können bei Ausschreibungen und Kooperationen von den Bewerbern verlangen, dass diese gewisse Standards erfüllen. Das Erfüllen dieser Standards kann ein angemessenes Qualitätsniveau der Bewerber garantieren, das den eigenen Ansprüchen oder dem eigenen Niveau genügt. Dies gewinnt vor allem dann an Bedeutung, wenn das Unternehmen Standards zur Vermarktung ihrer Produkte und Dienstleistungen benutzt, aber in den Prozessen auch auf Produkte und Dienstleistungen von anderen Unternehmen angewiesen ist.

Ein weiterer Faktor, der im Bereich der Compliance beachtet werden muss, sind die Konsequenzen, die aus der Nichterfüllung von Regelwerken resultieren können. Die Folgen bei Nichterfüllung der relevanten Regelwerke können sehr unterschiedlich ausfallen, aber unter Umständen äußerst gravierend für das Unternehmen sein. Das Unternehmen kann bei Gesetzesverstößen dazu verurteilt werden Bußgelder und Strafen zu bezahlen. Nach Audits können Zertifikate bei gravierenden Mängeln oder Verstößen aberkannt werden. Dazu können persönliche Strafen bei z.B. Haftbarkeit der Geschäftsleitung in Form von Gefängnisstrafen kommen. Die Außendarstellung des Unternehmens aufgrund von Fehlern kann aus Seiten der Kunden leiden und zu Umsatzeinbrüchen durch Imageverlust führen. Auch Schadensersatzklagen können zu den möglichen Folgen gehören.
In [Kal11] steht, dass „gegen deutsche Großunternehmen in der Vergangenheit schon Strafen in Millionenhöhe verhängt“ wurden, „weil sie etwa sensible Mitarbeiterdaten missbraucht hatten.“ Es wird in dem Artikel ebenfalls festgestellt, dass „der Imageverlust den monetären Schaden meist deutlich“ übersteigt.

Aus diesen potenziellen Konsequenzen ergibt sich die Notwendigkeit für Unternehmen Compliance ernst zu nehmen und bei der Umsetzung sorgfältig zu arbeiten. Die bereits erwähnte Vielzahl von Regelwerken, die ein Unternehmen dabei beachten muss, erschwert den Prozess der Compliance dabei beträchtlich. So wird in [Hil08] zum Thema Compliance festgestellt: „In einem regelrechten Compliance-Dschungel fällt es mittlerweile schwer, den Überblick zu behalten.“
In einer Umfrage aus dem Jahr 2006 zum Thema Compliance im Bereich IT-Sicherheit ([Hur06]) gaben 75 Prozent der befragten Unternehmen an, dass sie zwei oder mehr Regularien aus dem Bereich IT-Sicherheit beachten müssen. 43 Prozent der Unternehmen haben sogar drei oder mehr Regularien zu beachten.
Die Themenbereiche, die beachtet werden können, sind vielfältig. Eine Umfrage ([Bra11]) aus dem Jahr 2011 zum Bereich Internet-Sicherheit kommt zu folgenden Zahlen bezüglich der Wichtigkeit der Themen (Mehrfachnennung war erlaubt):

- 92% der Befragten stufen Datenschutz als wichtig ein
- 88% sehen ebenfalls die Sensibilisierung der Beschäftigten als wichtig an
- 81% finden die betriebliche Sicherheitskonzeption und die Beachtung der einschlägigen Richtlinien wichtig
- 78% halten Notfallplanung für wichtig
- 72% sind der Meinung, dass auch bei Lieferanten bzw. beauftragten Dienstleistern auf Sicherheit geachtet werden muss

Auch wenn sich diese Umfrage speziell auf das Internet bezieht, so kann eine allgemeine Relevanz dieser Themen im Unternehmen angenommen werden. Ein Standard wie die IT-Grundschutz-Kataloge (näheres in Abschnitt 2.1.3) kann zu diesen Themen eine praktische Anleitung liefern wie vorgegangen werden kann.
In einer weiteren Umfrage unter mittelständischen Unternehmen in [Kal11] geben nur 33,2% der Unternehmen an, dass sie eine Compliance-Strategie im IT-Bereich besitzen. Durch die Vielzahl an Möglichkeiten und Anforderungen, die durch die Regelwerke vorhanden sind, und den Ressourcen, die für eine vernünftige Compliance aufgewendet werden muss, kann die maschinelle Unterstützung bei der Compliance Vorteile bei der Entwicklung einer Strategie und deren Effizienz bieten.

Da ein Unternehmen eine Vielzahl an unterschiedlichen Gesetzen und Regelwerken betrachten muss und die Verbindungen dadurch beliebig komplex werden, wird die Anzahl der relevanten Regelwerke für diese Diplomarbeit eingegrenzt. Im Rahmen dieser Arbeit werden folgende Regelwerke betrachtet:

- Mindestanforderungen an das Risikomanagement (Versicherungen und Banken)
- ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27005
- BSI IT-Grundschutz-Kataloge und BSI-Standards
- Bundesdatenschutzgesetz

In den nächsten Abschnitten werden diese Regelwerke vorgestellt und eingeordnet.

2.1.1 Mindestanforderungen an das Risikomanagement

Die aufsichtsrechtlichen Mindestanforderungen an das Risikomanagement (MaRisk) werden von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)[1] als Rundschreiben veröffentlicht. Die BaFin ist für die Beaufsichtigung von Banken, Finanzdienstleistern, Versicherern und den Wertpapierhandel zuständig. Sie soll die Funktionsfähigkeit, Stabilität und Integrität des deutschen Finanzmarktes sichern, indem sie darauf achtet, dass sich die Marktteilnehmer an die einschlägigen Gesetze halten. Die BaFin ist eine Anstalt des öffentlichen Rechts und untersteht der Rechts- und Fachaufsicht des Bundesministeriums der Finanzen. Zu ihren Aufgaben gehören unter anderem die Solvenzaufsicht (Überwachung der Zahlungsfähigkeit sowie von fairen und transparenten Verhältnissen), der Verbraucherschutz und die Mitwirkung in europäischen und internationalen Gremien zur Entwicklung des Finanzmarktes.
Die *Bankenaufsicht* stellt sicher, dass nur zugelassene Unternehmen am Wettbewerb teilnehmen und dass diese Unternehmen von Vorständen geleitet werden, die über die fachliche und persönliche Zuverlässigkeit für diese Aufgabe verfügen. Außerdem überprüft die Bankenaufsicht die Einhaltung der gesetzlichen und der aufsichtsrechtlichen Grundsätze für Bankgeschäfte.
Die *Versicherungsaufsicht* soll die Belange der Versicherten wahren und sicherstellen, dass die Versicherungen ihre vertraglichen Verpflichtungen erfüllen können. Dazu gehört, dass nur zugelassene Versicherer ihre Dienste anbieten. Auch diese müssen von Vorständen geleitet werden, die über die fachliche Eignung und persönliche Zuverlässigkeit für die Leitung verfügen. Zudem überprüft die Versicherungsaufsicht, dass die Versicherungen ihr Kapital gemäß dem entsprechenden Risiko anlegt, in erster Linie also sicher und rentabel.
Die *Wertpapieraufsicht* sorgt für die Sicherstellung fairer und transparenter Marktbedingungen, indem sie z.B. bei Verdacht auf Marktmanipulationen eingreift oder die Einhaltung von Veröffentlichungspflichten überprüft. Sie ist außerdem für die Überwachung von Finanzdienstleistern, Kapitalanlagegesellschaften und Investmentfonds verantwortlich.
Zu den Veröffentlichungen der BaFin gehören unter anderem Rundschreiben für Versicherungen und Banken, die aufsichtsrechtliche Mindestanforderungen an das Risikomanagement dieser Institutionen beschreiben, die sogenannten *MaRisk*. Diese geben einen Rahmen vor, wie das Risikomanagement in Versicherungen und Banken gestaltet werden kann. Die Versicherungen und Banken sind durch bereichsspezifische Gesetze dazu verpflichtet ein angemessenes Risikomanagement umzusetzen.

[1] http://www.bafin.de

Versicherung

Die MaRisk für Versicherungen (VA)[2] konkretisiert die Paragraphen §64a und §104s des Versicherungsaufsichtsgesetzes (VAG). Sie sollen einen flexiblen und praxisnahen Rahmen für die Ausgestaltung des Risikomanagements in Versicherungen darstellen. Das Rundschreiben beinhaltet zehn Kapitel, die im Wesentlichen die Rahmenbedingungen des Risikomanagements beschreiben. Neben den Verantwortlichkeiten der Geschäftsleitung gehören dazu Elemente wie die Organisation, die Kommunikation, die Dokumentation sowie die einzelnen Schritte des Risikomanagementprozesses. Die Ausführungen sind so gehalten, dass die Anforderungen an die Verhältnisse des Unternehmens entsprechend angepasst werden können.

Banken

Die MaRisk für Banken (BA)[3] beruft sich auf den Paragraphen §25a Abs.1 des Kreditwesengesetzes (KWG) und bietet einen flexiblen und praxisnahen Rahmen für die Ausgestaltung des Risikomanagements. Die MaRisk für Banken sind in einen allgemeinen Teil (AT) mit neun Kapiteln und in einen besonderen Teil aufgeteilt. Der besondere Teil konkretisiert dabei die besonderen Anforderungen an das Kredit- und Handelsgeschäft, an die Risikosteuerungs- und -controllingprozesse sowie an die Ausgestaltung der internen Revision.
Auch für die MaRisk für Banken gilt, dass diese an die Verhältnisse des Unternehmens angepasst werden können.

Der Schwerpunkt der Diplomarbeit liegt auf den MaRisk für Versicherungen. Die MaRisk für Banken werden zunächst nicht konkret in die Modellierung der Ontologie einbezogen, da sich die beiden MaRisk auf unterschiedliche Domänen beziehen und eine gemeinsame Modellierung aufgrund zu geringer Überschneidungen und fehlender praktischer Relevanz nicht sinnvoll ist.

2.1.2 ISO-Standards

Die International Organization for Standardization (ISO)[4] ist eine nicht-staatliche Organisation, die aus einem globalen Netzwerk besteht. Ihre Aufgabe ist die Identifikation internationaler Standards, die von der Wirtschaft, Regierungen und der Gesellschaft gefordert werden. Das Netzwerk besteht aus nationalen Standardkörperschaften aus über 160 Ländern, die inzwischen über 18600 verschiedene Standards aus allen Bereichen beschlossen haben.
Die International Electrotechnical Commission (IEC)[5] ist eine globale Schwesterorganisation der ISO, die internationale Standards und Konformitätsbewertungen für alle elektrischen, elektronischen und verwandte Technologien entwickelt. Die IEC kooperiert mit der ISO, wenn die thematischen Überschneidungen dies ermöglichen oder anbieten.
Die beiden Organisationen bieten für ihre Standards Zertifizierungen an. Den Unternehmen dienen diese als Bestätigung der zufriedenstellenden Erfüllung der jeweiligen Standards. Da

[2] http://www.bafin.de/cln_152/nn_721290/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2009/rs__0903__marisk__va.html? [02.07.2011]
[3] http://www.bafin.de/cln_152/nn_721290/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2010/rs__1011__ba__marisk.html? [02.07.2011]
[4] http://www.iso.org
[5] http://www.iec.ch

die Organisationen und ihre Standards mit internationalem Fokus ausgerichtet sind, werden die Zertifikate international anerkannt und verfügen über eine Akkreditierung. Ein solches Zertifikat, das die Konformität zu einem oder mehreren Standards bescheinigt, kann unter Umständen bei Geschäften oder Kooperationen zwischen verschiedenen Unternehmen vorausgesetzt oder gefordert werden.
Im Rahmen dieser Diplomarbeit werden drei ISO/IEC-Standards aus dem Bereich der Informationssicherheit betrachtet, die in einer Kooperation der beiden Organisationen ISO und IEC entwickelt wurden: ISO/IEC 27001 (Stand: 2005), ISO/IEC 27002 (Stand: 2005) und ISO/IEC 27005 (Stand: 2008). Diese drei Standards stammen aus der Reihe der ISO/IEC 2700x-Standards, die noch weitere Standards aus dem Bereich der Informationssicherheit enthält. Einige dieser Standards befinden sich aber noch in der Entwicklung oder werden zur Zeit überarbeitet.
Als Nächstes werden die betrachteten Standards kurz vorgestellt. Die Standards richten sich an Unternehmen aus verschiedenen Bereichen.

ISO/IEC 27001:2005

Der Standard ISO/IEC 27001:2005 (*Information technology – Security techniques – Information security management systems – Requirements*) [ISO05a] spezifiziert die Anforderungen an die Etablierung, Implementierung, Umsetzung, Kontrolle, Überarbeitung, Instandhaltung und Verbesserung eines Informationssicherheitmanagementsystems sowie die Anforderungen an die Implementierung von Sicherheitskontrollen.
Der Standard besteht aus acht Kapiteln und drei Anhängen, die generisch gestaltet wurden. Die gestellten Anforderungen können also an die Verhältnisse des Unternehmens angepasst oder ausgelassen werden. Diese Entscheidungen müssen gut begründet und dokumentiert werden. Für die Konformität mit diesem Standard müssen die Anforderungen aus den Kapiteln 4, 5, 6, 7 und 8 umgesetzt werden. Der Anhang A bietet eine Übersicht über die Kontrollziele und die zugehörigen Kontrollen zur Erreichung dieser Ziele, die in ISO/IEC 27002 ausführlicher dargestellt werden und daher die dort benutzten Bezeichnungen haben.

ISO/IEC 27002:2005

Der Standard ISO/IEC 27002:2005 (*Information technology – Security techniques – Code of practice for information security management*) [ISO05b] beinhaltet Richtlinien und generelle Prinzipien für die Einführung, Implementierung, Instandhaltung und Verbesserung des Informationssicherheitsmanagement in einem Unternehmen. Der Standard bietet eine generelle Orientierung in Form von *Best Practices* von Kontrollzielen und Kontrollen in verschiedenen Bereichen des Informationssicherheitsmanagement. Exemplarisch seien an dieser Stelle die Bereiche Sicherheitspolitiken (*security policy*), Zugangskontrollen (*access control*) und Notfallmanagement (*business continuity management*) genannt. Diese *Best Practices* sollen von den Unternehmen implementiert werden, um den Anforderungen gerecht zu werden, die im Rahmen einer Risikobewertung ermittelt wurden. Des Weiteren können diese dann als Basis und praktische Richtlinie zur Entwicklung von organisatorischen Sicherheitsstandards und effektiven Sicherheitsmanagementpraktiken verwendet werden.
ISO/IEC 27002 enthält 11 Sicherheitskontrollparagraphen, die aus 39 Hauptsicherheitskategorien und einem einführenden Paragraphen zum Thema Risikobewertung und -behandlung bestehen. Die Kategorien bestehen aus einem Kontrollziel und einer oder mehrerer

dazugehöriger Kontrollen zur Erreichung des Kontrollziels. Die Beschreibungen der Kontrollen enthalten eine Definition, Implementierungshilfen und weitere Informationen.

ISO/IEC 27005:2008

Der Standard ISO/IEC 27005:2008 (*Information technology – Security techniques – Information security risk management*)[ISO08] enthält Richtlinien für das Informationssicherheitsrisikomanagement und unterstützt die generellen Konzepte, die im Standard ISO/IEC 27001 spezifiziert sind. Um diesen Standard adäquat umsetzen zu können, wird das Wissen über Konzepte, Modelle, Prozesse und Terminologien aus ISO/IEC 27001 und 27002 gefordert.
Der Standard besteht aus 12 Kapiteln und sechs Anhängen, wobei die wesentlichen Bereiche die Beschreibung des Risikomanagementprozesses (Kapitel 6) und die dazugehörigen Aktivitäten (Kapitel 7-12) sind.

2.1.3 BSI IT-Grundschutz-Kataloge und BSI-Standards

Das Bundesamt für Sicherheit in der Informationstechnik (BSI)[6] ist eine Bundesoberbehörde und untersteht dem Bundesministerium des Innern. Es wird durch den Artikel 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)) aus dem „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ (vom 14.8.2009)[7] legitimiert.
Zu den Aufgaben des BSI gehört u.a. die Abwehr von Gefahren für die Sicherheit der Informationstechnik, die Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und die Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen. Alle Aufgaben des BSI werden in §3 (Aufgaben des Bundesamtes) des BSIG aufgezählt.
Das BSI bietet diverse Veröffentlichungen sowohl für Unternehmen als auch den normalen Bürger, die Informationen zum Bereich IT-Sicherheit bieten. Dazu gehören auch Dokumente wie sich Informationssicherheit im Unternehmen umsetzen lässt, von welchen die wichtigsten die IT-Grundschutz-Kataloge und BSI-Standards sind. Der IT-Grundschutz soll den Aufbau eines IT-Sicherheitsmanagement und die arbeitsökonomische Erstellung von IT-Sicherheitskonzepten unterstützen. Ziel des IT-Grundschutz ist die Erreichung eines angemessenen und ausreichenden Sicherheitsniveaus für IT-Systeme mit normalem Schutzbedarf. Für Systeme mit höherem Schutzbedarf kann dieses Sicherheitsniveau als Ausgangsbasis genutzt werden. Für die Umsetzung hat das BSI die IT-Grundschutz-Kataloge und vier BSI-Standards zusammengestellt. Das BSI bietet zudem eine eigene Zertifizierung an, die zwar in Deutschland anerkannt wird, aber auf internationaler Ebene unter Umständen nicht. Das BSI hat sich nicht als Zertifizierungsstelle akkreditieren lassen und die Zertifikate fallen daher „nicht unter die internationalen Anerkennungsvereinbarungen“ ([KRS08]). Die „ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz“ ist so gestaltet, dass sie die Anforderungen von ISO/IEC 27001 erfüllt, allerdings ist dieses Zertifikat kein offizielles ISO/IEC-Zertifikat. Dieses muss bei Bedarf zusätzlich zum BSI-Zertifikat beantragt werden. Um die Anforderungen an die „ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz“ zu erfüllen, müssen die Vorgehensweise aus den BSI-Standards und die entsprechenden Maßnahmen aus den IT-Grundschutz-Katalogen umgesetzt worden sein. Diese werden in den folgenden Abschnitten bezüglich Inhalt und Aufbau beschrieben.

[6] http://www.bsi.bund.de
[7] https://www.bsi.bund.de/ContentBSI/dasBSI/Gesetz/gesetz.html[06.07.2011]

BSI IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge ([BSIa]) bestehen aus drei Elementen: Bausteine, Gefährdungen und Maßnahmen.
Die Bausteine sind in fünf Schichten unterteilt:

1. Übergreifende Aspekte
2. Infrastruktur
3. IT-Systeme
4. Netze
5. IT-Anwendungen

Die Bausteine aus diesen Bereichen werden je nach Relevanz im Rahmen der IT-Grundschutz-Vorgehensweise von BSI-Standard 100-2 ausgewählt. Sie enthalten eine Beschreibung der Thematik und eine Auflistung der Gefährdungen sowie die entsprechenden Maßnahmen, die in dem Bereich beachtet werden müssen und eingesetzt werden können. Falls in dem Unternehmen bereits ein System zur Informationssicherheit vorhanden ist, ermöglichen diese Bausteine einen Soll-/Ist-Abgleich.
Die Gefährdungen werden in den Bausteinen und in dem Gefährdungskatalog nach den folgenden Kategorien eingeordnet:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

Die Maßnahmen sind ebenfalls in den Bausteinen und in dem Maßnahmenkatalog nach Kategorien eingeteilt:

- Infrastruktur
- Organisation
- Personal
- Hardware/Software
- Kommunikation
- Notfallvorsorge

Für den Baustein über Datenschutz gibt es noch eine weitere Kategorie, die aber nicht in den Katalogen, sondern nur im Baustein aufgeführt wird.
Als weiteres Hilfsmittel zu den IT-Grundschutz-Katalogen stellt das BSI „Kreuztabellen“ zur Verfügung, in denen Gefährdungen und Maßnahmen gegenübergestellt werden. Durch ein Kreuz in der Tabelle wird eine Verbindung zwischen einer Gefährdung und einer oder mehrerer Maßnahmen hergestellt, die diese Gefährdung minimieren oder verhindern können.

BSI-Standard 100-1

Der BSI-Standard 100-1 „Managementsysteme für Informationssicherheit“ [BSI08b] beschreibt den Aufbau eines solchen Managementsystems und wie dieses im Unternehmen generell initiiert und gesteuert werden kann.

BSI-Standard 100-2

Der BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“ [BSI08a] baut auf dem BSI-Standard 100-1 auf und beschreibt die Vorgehensweise zur Einführung eines dort initiierten Managementsystems. Das BSI will mit diesem Standard eine praktische Anleitung geben, wie die allgemeiner formulierten Anforderungen der ISO/IEC 2700x-Standards umgesetzt werden können. In den einzelnen Schritten werden auch die Bausteine der IT-Grundschutz-Kataloge genutzt.

BSI-Standard 100-3

Der BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ [BSI08d] soll dazu dienen ein bereits bestehendes IT-Grundschutz-Sicherheitskonzept zu ergänzen und baut daher auf der Umsetzung bestimmter Teile des BSI-Standards 100-2 auf. Er wird z.B. dann benötigt, wenn der Schutzbedarf einzelner Elemente höher als normal ist und daher weitere Risiken identifiziert und bewertet werden müssen.

BSI-Standard 100-4

Der BSI-Standard 100-4 „Notfallmanagement“ [BSI08c] liefert eine Anleitung, um ein Notfallmanagement in einem Unternehmen systematisch aufzubauen. Mit diesem soll ein Unternehmen in der Lage sein die Vorkehrungen treffen zu können, um in einem Notfall den Geschäftsbetrieb zumindest eingeschränkt aufrecht zu erhalten und möglichst schnell wieder den ursprünglichen Zustand wiederherzustellen.

2.1.4 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG)[8] ist ein Gesetz der Bundesrepublik Deutschland und wurde im Jahr 1990 beschlossen und verkündet. Seitdem gab es einige Anpassungen. Die letzte Änderung war im Jahr 2009. Als Bundesgesetz ist es verpflichtend in Deutschland einzuhalten.
Das Gesetz besteht aus insgesamt 63 Paragraphen (§1 bis §48) in sechs Abschnitten und enthält Bestimmungen über die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Damit sind die Daten einer „natürlichen Person“ gemeint, die Angaben über persönliche oder sachliche Verhältnisse dieser Person enthalten. Das Bundesdatenschutzgesetz regelt insbesondere die Datenverarbeitung bei öffentlichen Stellen und nicht-öffentlichen Wettbewerbsunternehmen.

2.2 Ontologien

In diesem Abschnitt wird geklärt, was eine Ontologie ist. Dann wird ein kurzer Überblick über Ontologiesprachen gegeben. Zuletzt wird ausführlicher auf die spezielle Art der *Legal Ontologies* eingegangen.

[8] http://bundesrecht.juris.de/bdsg_1990/index.html[06.07.2011]

2.2.1 Definition

In der Literatur lassen sich viele Definitionen des Begriffes *Ontologie* finden. Der ursprüngliche Begriff stammt aus dem Bereich der Philosophie, wo Aristoteles Ontologie als die „Wissenschaft des Seins“ definierte ([GG95]). [BLHL+01] beschreibt Ontologie als Theorie über die Natur der Existenz, über die Typen von Dingen, die existieren. Seit dem Beginn der 90er Jahre wird der Begriff auch zunehmend im Bereich der *Künstlichen Intelligenz* verwendet.
In [Cas08] und [GG95] geben die Autoren einen Überblick über einige Definitionen von verschiedenen Autoren. Eine der ersten Definitionen im Bereich der *Künstlichen Intelligenz* ist von Neches et al. ([NFF+91]), die eine Ontologie als die Definition von elementaren Begriffen und Relationen als Vokabular eines Themenbereichs sehen. Regeln zur Kombination der Begriffe und Relationen sind als Definition von Erweiterungen zu diesem Vokabular zu sehen.
Die wohl meist zitierte Definition ist von Gruber ([Gru93]), der unter einer Ontologie eine explizite Spezifikation einer Konzeptualisierung versteht. Eine Konzeptualisierung stellt für Gruber eine abstrakte, vereinfachte Sicht auf die Welt dar, die man für einen bestimmten Zweck repräsentieren möchte.
Uschold und Jasper(1999)([JU99]) haben in ihrer Definition einer Ontologie festgestellt, dass eine Ontologie eine Vielzahl von Formen haben kann. Sie enthält aber immer ein Vokabular von Begriffen und eine Spezifikation ihrer Bedeutung.
In [BLHL+01] wird eine Ontologie als Dokument oder Datei beschrieben, die formal die Relationen zwischen Termen beschreibt.
Valente(2005)([Val05]) betont zwei Hauptprobleme bei der Abgrenzung des Begriffes *Ontologie*. Zum einen, dass verschiedene Autoren verschiedene Dinge mit dem Begriff *Ontologie* verbinden und zum anderen, dass Ontologien in sehr unterschiedlichen Weisen benutzt werden. Der angestrebte Nutzen beziehungsweise die Rolle der Ontologie bestimmen:

- wie die Ontologie aufgebaut wird,
- welchen Inhalt und welchen Strukturierungsgrad die Ontologie hat,
- welche Repräsentationssprache gewählt wird, und
- wie viel Wert auf die Nutzbarkeit und Wiederverwendbarkeit gelegt wird.

Auch für eine etwas formalere Definition des Begriffes *Ontologie* finden sich unterschiedliche Ansätze. [CS06] identifiziert folgende Elemente als Teil einer Ontologie:

- Konzepte: Beschreibungen von Dingen, die in der Domäne der Ontologie existieren
- Relationen: Beschreibungen von Abhängigkeiten zwischen mehreren Konzepten
- Funktionen: Spezielle Relationen, die in einem einzelnem Wert resultieren
- Instanzen: Fakten, die durch die Benutzung der Konzepte beschrieben wird
- Axiome: Logische Ausdrücke für verschiedene Zwecke (z.B. Definition der Beschränkungen von Daten)

Für diese Diplomarbeit wird eine Ontologie wie folgt definiert. Diese Definition ist an die Definitionen in [ES07] und [RFP08] angelehnt, enthält aber nur die gemeinsamen Elemente, die an dieser Stelle ausreichend sind. Bei Bedarf kann diese elementare Definition um weitere Elemente, wie Funktionen oder Axiome, erweitert werden.

2.2.1 Definition (Ontologie). Eine Ontologie ist ein Tupel o = <K,I,R>. Dabei ist:

- K = $\{K_1,...,K_j\}$ eine Menge von Konzepten, wobei ein Konzept K_i, $1 \leq i \leq j$, die Repräsentation einer Menge von Objekten mit gemeinsamen Eigenschaften ist
- I = $\{I_1,...,I_k\}$ eine Menge von Instanzen, wobei eine Instanz I_i, $1 \leq i \leq k$, ein individuelles Objekt eines Konzeptes repräsentiert
- R = $\{R_1,...,R_m\}$ eine Menge von Relationen, wobei eine Relation R_i, $1 \leq i \leq m$, die Beziehung zwischen zwei Konzepten oder zwischen einem Konzept und einer Instanz oder zwischen zwei Instanzen beschreibt

Zur Verdeutlichung folgt ein kleines Beispiel für Elemente einer Ontologie und eine mögliche grafische Darstellung dieser.

2.2.2 Beispiel (Ontologie). Die Ontologie besteht aus den folgenden Mengen:

- K = {Student, Informatik-Student, Mathematik-Student}
- I = {Tim, Julia}
- R = {ist-ein, ist-Instanz-von}

Eine grafische Darstellung dieser einfachen Ontologie findet sich in Abbildung 2.1. Das Konzept *Student* ist ein Oberkonzept der Konzepte *Informatik-Student* und *Mathematik-Student*. Die Instanzen dieser Konzepte sind auch Elemente des Oberkonzepts. Diese Beziehung wird in dem Beispiel über die Relation *ist-ein* formalisiert. Informell würde das heißen: Ein Informatik-Student ist ein Student. Bei *Tim* und *Julia* handelt es sich um Instanzen, also um konkrete Objekte. *Tim* wird in dem Beispiel dem Konzept *Informatik-Student* zugeordnet und ist damit auch eine Instanz des Konzeptes *Student*.

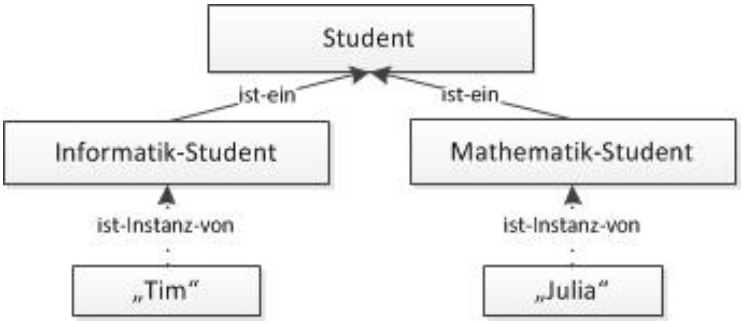

Abbildung 2.1: Beispiel-Ontologie

2.2.2 Arten von Ontologien

Die Einsatzmöglichkeiten und -gebiete für Ontologien sind vielfältig: Verarbeitung natürlicher Sprache, Wissensmanagement, E-Commerce, intelligente Informationsintegration, Semantic Web, Medizin, Chemie, etc. (aus [CFLGP03] und [GPFLC04]). Die Modellierung von Ontologien kann sich stark nach dem gewünschten Einsatzgebiet und der dabei gewünschten Funktionalität unterscheiden.
Valente ([Val05]) unterscheidet in seinem Artikel die Strukturierung von Ontologien in drei unterschiedliche Stärken: leicht strukturierte, moderat strukturierte und stark strukturierte Ontologien. Leicht strukturierte Ontologien werden als Bäume, Taxonomien oder in Aussagen über Fakten dargestellt. Es werden nur einfache Vererbung oder taxonomische Schlussfolgerungen benutzt. Moderat strukturierte Ontologien fügen dem einfaches Schlussfolgern für einfache Klasse und *Frames* hinzu. Stark strukturierte Ontologien werden in formalen Wissensrepräsentationssprachen dargestellt. Diese basieren auf Prädikatenlogik, Beschreibungslogik oder *Frames*. Dadurch sind auch die automatische Klassifizierung von Instanzen und regelbasiertes Schlussfolgern möglich.
In [CFLGP03] wird nur zwischen zwei Arten differenziert, den leichtgewichtigen und den schwergewichtigen Ontologien. Leichtgewichtige Ontologien enthalten demnach Konzepte, Konzept-Taxonomien, Relationen zwischen Konzepten und Eigenschaften zur Beschreibung der Konzepte. Schwergewichtige Ontologien fügen diesen Elementen noch Axiome und Einschränkungen hinzu. [GPFLC04] unterscheidet neben den leichtgewichtigen und schwergewichtigen Ontologien nach dem Grad der Formalität:

- stark informell: Ontologie wird in natürlicher Sprache ausgedrückt
- halb-informell: Ontologie wird in einer eingeschränkten und strukturierten Form der natürlichen Sprache ausgedrückt
- halb-formal: Ontologie ist einer künstlichen und formal definierten Sprache (z.B. Ontolingua, OWL)
- streng formal: Ontologie hat sorgfältig definierte Ausdrücke mit formaler Semantik, Theoremen und Beweisen von Eigenschaften

Die Art der gewünschten Ontologie bezüglich der Strukturierung und dem Abstraktionsgrad beeinflusst stark die Wahl der Ontologiesprache. Im nächsten Abschnitt soll ein Überblick über die verschiedenen Arten von Ontologiesprachen gegeben werden.

2.2.3 Ontologiesprachen

Für die Darstellung von Ontologien existieren eine Vielzahl von Ontologiesprachen, die sich oft stark in ihrer Ausdrucksstärke unterscheiden.
Anfang der 90er Jahre, als Ontologien auch immer mehr Verwendung im Bereich der *Künstlichen Intelligenz* fanden, wurden einige Sprachen für die Implementierung von Ontologien entwickelt ([CFLGP03] und [GPFLC04]). Zunächst wurden vor allem logische Sprachen entwickelt, die auf Prädikatenlogik (z.B. KIF), *Frames* in Kombination mit Prädikatenlogik (z.B. CycL, Ontolingua, OCML, FLogic) und Beschreibungslogiken (z.B. LOOM) basierten. Abbildung 2.2 zeigt eine Übersicht über einige dieser Sprachen. Das OKBC (*Open Knowledge Base Connectivity*)-Protokoll wurde für den Zugang zu, in verschiedenen Sprachen formulierten, Ontologien entwickelt. Im Zuge der wachsenden Popularität des *Semantic Web* sind die so genannten *Markup Languages* mehr in den Fokus gerückt und

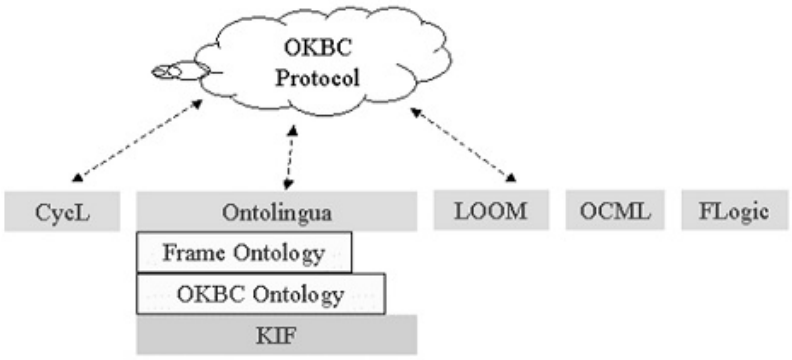

Abbildung 2.2: Traditionelle Ontologiesprachen aus [GPFLC04]

haben die Ontologieentwicklung stark beeinflusst. Diese Sprachen haben zur Entstehung und Entwicklung des *Semantic Web* maßgeblich beigetragen. Das *Semantic Web* erweitert das Web um semantische Informationen, die es Computern und Menschen ermöglichen besser zusammen zu arbeiten ([BLHL+01]).
Abbildung 2.3 zeigt eine hierarchische Übersicht dieser *Markup Languages*, die allerdings nicht alle für die Darstellung von Ontologie geeignet sind. Die Sprachen, die in der Grafik dargestellt werden, sind ([CFLGP03]):

- **SHOE:** Wurde 1996 als Erweiterung von HTML entwickelt und erlaubt das Einfügen von Ontologien in HTML-Dokumente. Die Sprache kombiniert Frames und Regeln und erlaubt die Darstellung von Konzepten und ihren Taxonomien, Relationen, Instanzen und Deduktionsregeln, um neues Wissen zu folgern.

- **XML (Extensible Markup Language):** Die Entwicklung von XML zu einer Standardsprache für den Informationsaustausch im Web hat dazu geführt, dass die Syntax von SHOE an XML angepasst wurde. Weitere Sprachen für Ontologien im *Semantic Web* bauen ebenfalls auf der XML-Syntax auf. Mit XML kann zwar Struktur in Dokumente gebracht werden, aber es wird nichts über die Bedeutung dieser Strukturen gesagt ([BLHL+01]).

- **XOL:** XOL ist eine kleine Untermenge des OKBC-Protokolls, die an XML angepasst wurde und sehr eingeschränkt bezüglich ihrer Ausdrucksfähigkeit ist, weil nur Konzepte, Konzepttaxonomien und binäre Relationen möglich sind.

- **RDF, RDF Schema, RDF(S):** Dies sind Standards, die vom W3C entwickelt wurden. Das *World Wide Web Consortium (W3C)*[9] ist eine internationale Gemeinschaft, die es sich zur Aufgabe gemacht hat Standards für das Web zu entwickeln. RDF wird zur Beschreibung von Webressourcen benutzt und basiert auf semantischen Netzwerken([Sow91]). Die Beschreibungen bestehen aus einer Menge von Tripeln, die aus Subjekt, Verb und Objekt bestehen. RDF Schema ist eine Erweiterung zu RDF. RDF(S) ist die Kombination aus beiden, aber nur beschränkt ausdrucksfähig zur Darstellung von Ontologien, da nur Konzepte, Konzept-Taxonomien und binäre Relationen dargestellt werden können.

- **OIL, DAML+OIL:** OIL und DAML+OIL wurden, aufbauend auf RDF(S), als Erweiterungen in Projekten der EU bzw. der EU und den USA entwickelt. Diese

[9] http://www.w3.org/

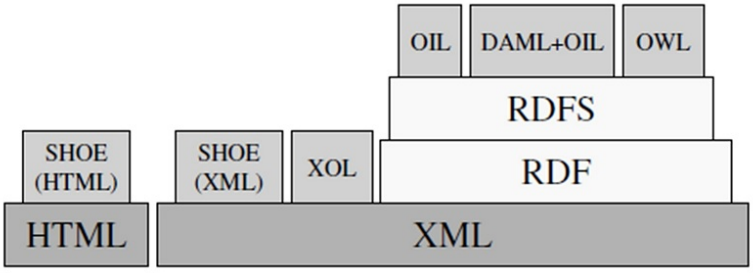

Abbildung 2.3: Markup Languages aus [CFLGP03]

Sprachen basieren auf Beschreibungslogiken und können neben Konzepten, Konzept-Taxonomien und binären Relationen auch Funktionen und Instanzen darstellen.

- **OWL (Web Ontology Language)**: OWL baut ebenfalls auf RDF(S) auf und wurde ebenfalls als Standard vom W3C entwickelt und 2004 veröffentlicht. OWL unterstützt die gleichen Elemente wie OIL und DAML+OIL. OWL wurde inzwischen ebenfalls erweitert und überarbeitet, woraus OWL2 entstanden ist ([MPSP+09]).

Von den Ontologierepräsentationssprachen RDF(S), DAML+OIL und OWL hat sich nach [dBG+07] OWL als Standard etabliert.

2.2.4 Legal Ontologies

Ein spezielle Form der Ontologien findet sich im juristischen Bereich. Die Bezeichnung für Ontologien aus diesem Bereich lautet *Legal Ontologies*. [BCBG05] erklärt, dass Personen aus dem juristischen Bereich Informationen aus juristischen Dokumenten nutzen, um anhand dieser Entscheidungen treffen. Aber auch andere Personen müssen zunehmend mit Regularien umgehen. Gerade im juristischen Bereich ist es schwierig mit der Komplexität und den Arten juristischen Wissens umzugehen. Die großen Mengen an Informationen müssen vernünftig gespeichert, gefunden und strukturiert werden können. *Legal Ontologies* sollen helfen mit diesen Mengen und Arten von Informationen umgehen zu können. Zu den Kernelementen der *Legal Ontologies* gehören so z.B. Normen, Fälle, Personen, Agenten, Rollen, Besitz, Verbrechen oder Strafen.
Valente hat in seinem Artikel [Val05] fünf elementare Typen von Ontologien identifiziert und beschreibt die Nutzung dieser Typen im Bereich der *Legal Ontologies*. Ontologien können demnach folgende Nutzen haben:

a) Informationen organisieren und strukturieren,
b) begründen und Probleme lösen,
c) semantische Indexierung und Suche,
d) semantische Integration und Interoperation und
e) die Domäne verstehen.

Ontologien aus a) stellen ein Mittel dar, um Dinge oder Phänomene in der Domäne zu beschreiben. Die Ontologie hat in diesem Bereich die Rolle eines Vokabular. Es geht um die Beantwortung der Fragen „Welche Begriffe können benutzt werden?“ und „Welche (gültigen) Sätze können ausgedrückt werden?“. Im Bereich der *Legal Ontologies* werden in dieser Art von Ontologie Begriffe definiert, die in den Regularien verwendet werden. Es

wird argumentiert, dass diese Art nicht unbedingt eine *Legal Ontology* ist, aber eine Repräsentation der Welt oder Domäne, auf denen die Gesetze arbeiten.
Bei b) wird das Wissen einer Domäne so abgebildet, dass ein automatischer *Reasoner* in der Lage ist die Probleme zu repräsentieren und auch Lösungen für diese zu generieren. Die Ontologie dient als Struktur einer Wissensbasis. Weitere Ziele sind Wissensbasen zu erschaffen, die wiederverwendbar, effizient, erklärbar, modular, etc. sind. Im Bereich der *Legal Ontologies* können damit Expertensysteme (Problemlöser) und Entscheidungsfindungssysteme realisiert werden.
Der Nutzen von c) besteht in der Repräsentation des Inhalts von Dokumenten oder anderen *soften* Wissensquellen. Es soll ein semantischer Index von Informationen aufgebaut werden, der eine semantische Suche nach Inhalten ermöglicht. Für die *Legal Ontologies* ist diese Art ein Schlüssel, um verschiedenste Formen von Dokumenten, die in der juristischen Praxis auftauchen, zu organisieren und wiederzufinden.
Ontologien nach d) können Anwendungen unterstützen, um elektronisch Informationen auszutauschen, indem sie ein Vokabular für den Informationsaustausch zur Verfügung stellen. Laut dem Autor ist diese Form aber noch nicht gängig in der juristischen Domäne, auch wenn seiner Meinung nach Potential für deren Einsatz vorhanden ist.
Mit Hilfe von e) soll durch die Ontologie ein Überblick über eine Domäne gegeben werden. Es soll eine Art Karte sein, welche Arten von Informationen identifiziert werden können und die als Basis zum Gestalten spezialisierter Repräsentationen genutzt werden kann. Die Bezeichnung für diese Form der Ontologien ist *Core Ontologies*. Im Bereich der *Legal Ontologies* werden so Theorien (im Speziellen aus dem juristischen Bereich) miteinander verbunden. Einige dieser speziellen Ontologien werden auch entworfen, um das *Reasoning* zu unterstützen und dabei zu helfen die Probleme zu lösen.

Kapitel 3

Modellierung der Ontologie

In diesem Kapitel werden die, in Kapitel 2 vorgestellten, Regelwerke bezüglich ihrer Struktur und ihrem Inhalt analysiert. Anhand der Ergebnisse wird eine Modellierung der Regelwerke in einer Ontologie entwickelt. Dabei steht im Fokus, wie die Regelwerke zueinander in Beziehung stehen und wie eine Verbindung zwischen Geschäftsprozessen eines Unternehmens und diesen Regelwerken hergestellt werden kann. Die Überlegungen werden so unabhängig wie möglich von der Betrachtung einer bestimmten Ontologiesprache sein, da sich in diesem Kapitel noch nicht auf eine Sprache festgelegt werden soll.

3.1 Vorgehensweise

In diesem Abschnitt wird die Vorgehensweise in den weiteren Abschnitten dieses Kapitels beschrieben sowie Konventionen für die Modellierung festgelegt.
Die Vorgehensweise bei der Analyse der Regelwerke und der Modellierung der Ontologie besteht aus den folgenden Schritten:

1. Analyse der Regelwerke
2. Modellierung der Regelwerke und Regeln
3. Identifikation von Relationen zwischen den Regelwerken
4. Identifikation der Elemente in den Regelwerken
5. Modellierung der Verbindungen zwischen den Regeln und den Elementen

Die Schritte 1 bis 3 und deren Ergebnisse werden in Abschnitt 3.2 beschrieben.
Schritt 4 wird in Abschnitt 3.3 beschrieben.
Die Beschreibung von Schritt 5 befindet sich in Abschnitt 3.4.

3.1.1 Konventionen

Vor der Modellierung werden ein paar Konventionen bezüglich der Bezeichnungen bei der Modellierung der Ontologie und den Grafiken in den nächsten Abschnitten festgelegt.
Für die Benennung der Konzepte und Relationen in der Ontologie werden folgende Richtlinien festgelegt:

- **Sprache:** Die Konzepte in der Ontologie werden in Deutsch benannt. Deshalb werden auch die Namen der selbst definierten Relationen auf Deutsch formuliert.

- **Groß-/Kleinschreibung:** Relationen fangen mit einem Kleinbuchstaben an. Da die Relationen aus zwei oder mehr Wörtern zusammengefügt sind, fangen weitere Wörter zur besseren Abgrenzung mit einem Großbuchstaben an.
- **Bezeichnungen:** Die Namen der Relationen werden so gewählt, dass sie die Funktion der Relation möglichst gut verdeutlichen.

Da die Richtung der Relationen zwischen den Regeln vorher nicht bekannt ist, wird für jede Relation auch eine inverse Relation definiert. So kann die Suche nach relevanten Regeln in beide Richtungen ermöglicht werden. Die mathematische Definition einer Relation und einer inversen Relation ist wie folgt (siehe [TT07]):

3.1.1 Definition (Relation und inverse Relation).
Die **Relation** R zwischen den Mengen A und B ist wie folgt definiert:

$$R \subseteq A \times B.$$

Wenn $(a, b) \in R$ gilt, steht das Element a in Relation R zu Element b.
Die **inverse Relation** R^{-1} der Relation R ist wie folgt definiert:

$$R^{-1} = \{\ (\text{b,a}) \mid (\text{a,b}) \in \text{R}\ \} \subseteq B \times A$$

Für die Darstellung von Relationen in den Grafiken dieses Kapitels werden für die Hierarchie zwischen Konzepten und die Zuordnung von Instanzen folgende Beschreibungen benutzt:

- *ist-Unterkonzept-von*: Beschreibt die hierarchische Beziehung zwischen zwei Konzepten. Ein Konzept kann ein Unterkonzept eines anderen Konzeptes sein. Das Konzept erbt alle Eigenschaften seines Oberkonzepts, während das Oberkonzept aus vielen Unterkonzepten bestehen kann.
- *ist-Instanz-von*: Beschreibt die Zuordnung einer Instanz zu ihrem Konzept.

3.2 Analyse und Modellierung der Regelwerke

In diesem Abschnitt wird zunächst überlegt, wie die verschiedenen Regelwerke in der Ontologie modelliert werden können. Dann wird auf die Struktur und Modellierung der Regeln eingegangen. Im dritten Abschnitt werden die Relationen zwischen den Regeln und Regelwerken identifiziert und erläutert.

3.2.1 Regelwerke

Der Begriff *Regelwerk* wurde bereits in Kapitel 2 als Oberbegriff für die verschiedenen Arten von Regelwerken wie Gesetz, Standard und Richtlinie verwendet. Er kann als ein elementares Konzept der Ontologie betrachtet werden und dient daher als Ausgangspunkt. Gesetz, Standard und Richtlinie sind ebenfalls Konzepte und können als Unterkonzepte des Konzeptes *Regelwerk* betrachtet werden.
Das *Bundesdatenschutzgesetz* gehört zum Konzept *Gesetz*, allerdings stellt es selbst kein eigenes Konzept dar, sondern ist eine Instanz von *Gesetz*. Für die ISO- und BSI-Standards

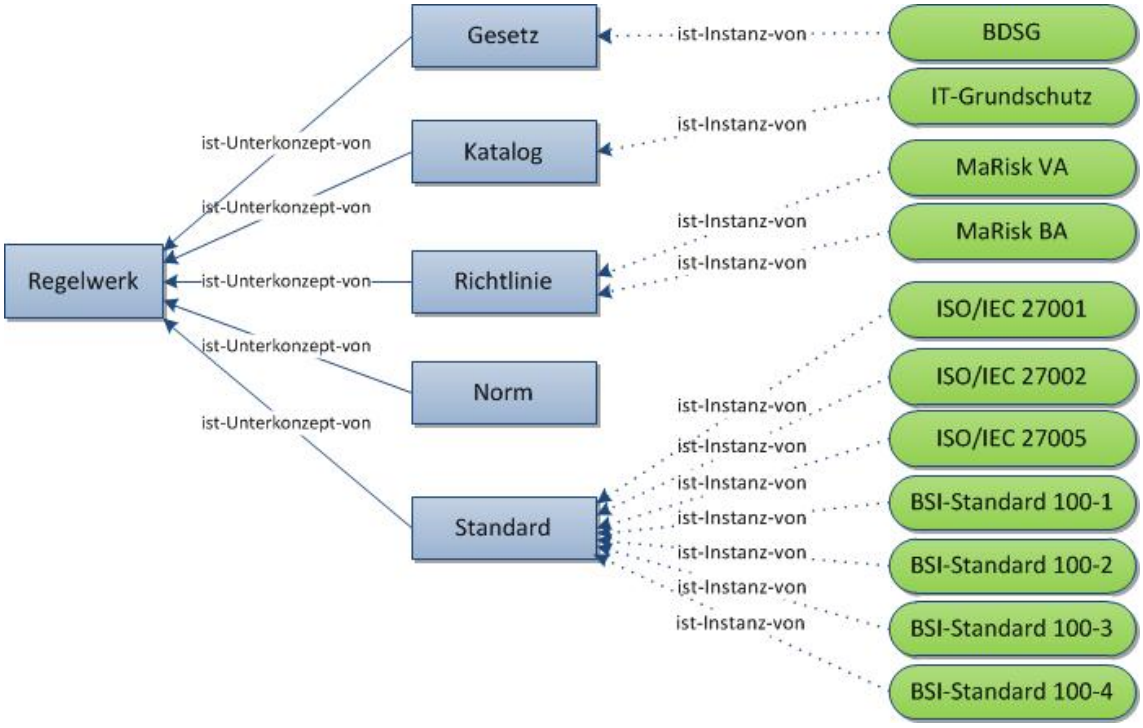

Abbildung 3.1: Regelwerke

gilt dies analog für das Konzept *Standard*.
Die *IT-Grundschutz-Kataloge* sind zwar auch ein Standard, verfügen allerdings über eine andere Struktur als die anderen Standards wie in Kapitel 2 beschrieben. Daher werden die *IT-Grundschutz-Kataloge* dem neuen Konzept *Katalog* zugeordnet.
Grafisch dargestellt entsprechen diese Überlegungen der Konzepthierarchie in Abbildung 3.1. Die Instanzen der Regelwerke wurden in der Grafik ihren Konzepten zugeordnet.

3.2.2 Regeln

Bei der Analyse wurden zunächst der Aufbau und die Struktur der einzelnen Regelwerke untersucht. In der Abbildung 3.2 sieht man den hierarchischen Aufbau der Mindestanforderungen an das Risikomanagement für Versicherungen (im Folgenden nur noch *MaRisk VA* genannt). Die Regelwerke verfügen über einen hierarchischen Aufbau und eine thematische Gliederung und bestehen aus einzelnen Regeln. Diese Regeln werden teilweise in weitere Regeln auf verschiedene Ebenen unterteilt. Zur besseren Anschaulichkeit wird diese Gliederung am Beispiel der *MaRisk VA* verdeutlicht.

3.2.1 Beispiel (MaRisk VA).
Die erste Ebene der MaRisk VA besteht aus zehn Kapiteln. Kapitel 7 ist das einzige Kapitel, das in weitere fünf Unterkapitel unterteilt wird. Von diesen Unterkapiteln sind wiederum zwei Kapitel (7.2 und 7.3) nochmal aufgeteilt in insgesamt sieben weitere Unterkapitel. Zwei dieser Kapitel (7.2.2 und 7.3.2) haben ebenfalls noch sieben weitere Unterkapitel.

> Die MaRisk VA besteht damit aus vier Ebenen und die Kapitel jeder Ebene können als Regeln betrachtet werden. Diejenigen Kapitel jeder Ebene, die nicht weiter in nummerierte Kapitel unterteilt werden, bestehen meist noch aus nummerierten Abschnitten. Da diese Abschnitte aber selbst keine eigenen Überschriften haben, können sie als thematisch zugehörig innerhalb einer Regel betrachtet werden und werden daher nicht mehr als eigene Regeln betrachtet.

Diese Gliederung der Regelwerke ist für den Aufbau der Ontologie nützlich. Es gibt verschiedene Ebenen der Gliederung der Thematik und je tiefer man in den Ebenen geht, desto feiner wird eine bestimmte Thematik beschrieben. Dabei kann jede Gliederungsebene als eigene Regel aufgefasst werden.
Zur Beschreibung der Regeln in der Ontologie wird das Konzept *Regel* eingeführt. Um den unterschiedlichen Aufbau der Regelwerke zu berücksichtigen und Unterscheidungen bezüglich der Wichtigkeit der Regeln vornehmen zu können, werden verschiedene Unterkonzepte für *Regel* eingeführt. Eine Regel aus einem *Gesetz* ist z.B. grundsätzlich wichtiger als eine Regel aus einem *Standard*. Die Unterkonzepte orientieren sich an den Arten der Regelwerke und werden dementsprechend benannt:

- *Regel Gesetz*: Die Regeln gehören zu einem Gesetz.
- *Regel Katalog*: Die Regeln gehören zu einem Katalog.
- *Regel Richtlinie*: Die Regeln gehören zu einer Richtlinie.
- *Regel Standard*: Die Regeln gehören zu einem Standard.

Zur Darstellung der Hierarchie und der Zuordnung der Regeln zu den Regelwerken, wird im nächsten Abschnitt eine Relation definiert, weil sich diese über die Unterkonzepte-Hierarchie nicht vernünftig darstellen lassen.
Die Regelwerke sind unterschiedlich strukturiert, was sich auf die Art der Regeln auswirkt. Die Struktur der Regelwerke in der Ontologie wird nach den Regelwerken aus Kapitel 2 modelliert. Das Konzept *Regel Gesetz* wird aufgrund der Strukturierung des *Bundesdatenschutzgesetzes* in *Abschnitt*, *Unterabschnitt* und *Paragraph* unterteilt.
Die Konzepte *Regel Richtlinie* und *Regel Standard* enthalten die Unterkonzepte *Kapitel*, *Unterkapitel*, *Unterunterkapitel* und im Fall der *Regel Richtlinie* zusätzlich das Unterkonzept *Unterunterunterkapitel*. Durch die Benennung soll klar werden, in welcher Ebene der Hierarchie sich eine Instanz dieser Konzepte befindet. Zur Unterscheidung der Regeln werden diese durch den Zusatz *Richtlinie* oder *Standard* erweitert.
Das Konzept *Regel Katalog* besteht aufgrund der Beschaffenheit der *IT-Grundschutz-Kataloge* aus den folgenden Elementen: Es gibt ebenfalls *Kapitel* (erweitert um *Katalog*), zudem die Konzepte *Baustein Schicht*, *Baustein*, *Maßnahme*, *Gefährdung* und *Kategorien* für Maßnahmen und Gefährdungen.
Die Anzahl der Ebenen, die für die Regelwerke festgelegt werden, sind:

- *Richtlinie*: 4 Ebenen
- *Standard* und *Gesetz*: 3 Ebenen
- *Katalog*: 2 Ebenen

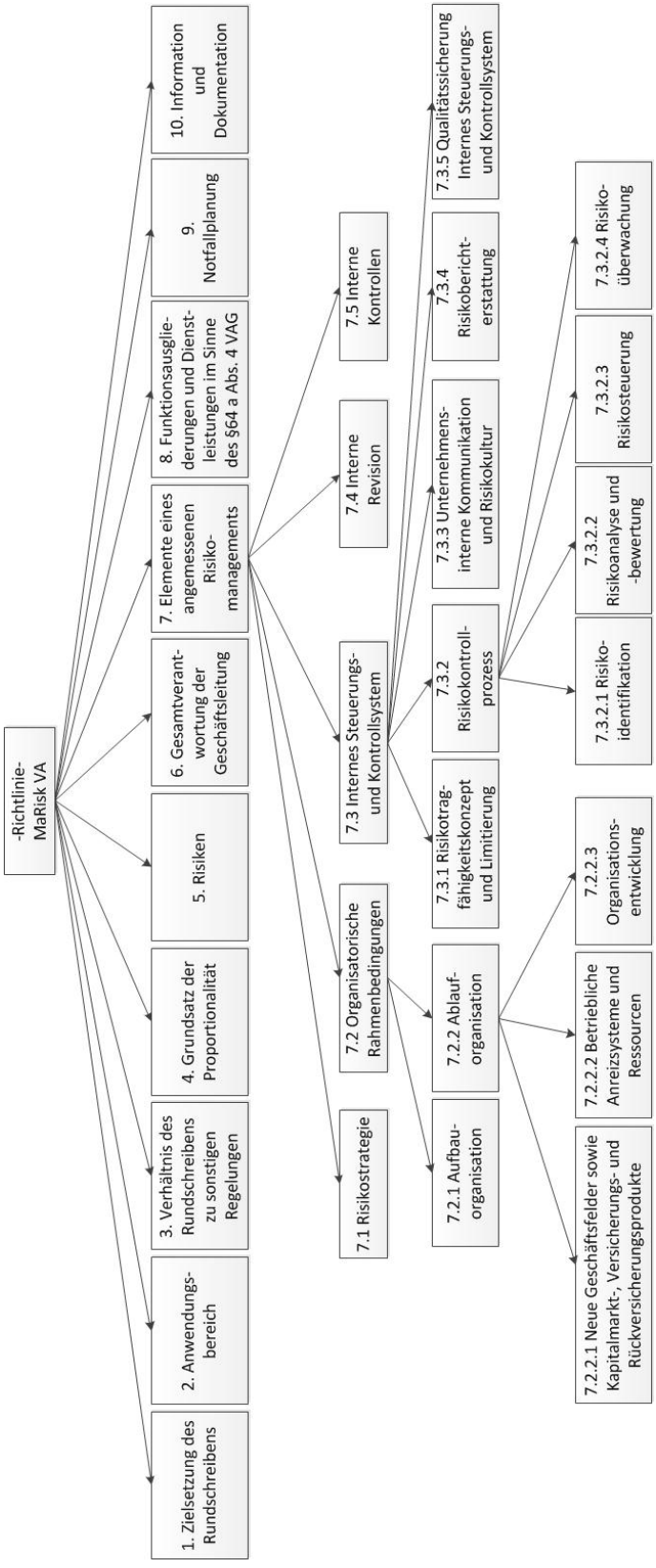

Abbildung 3.2: Übersicht über die MaRisk VA

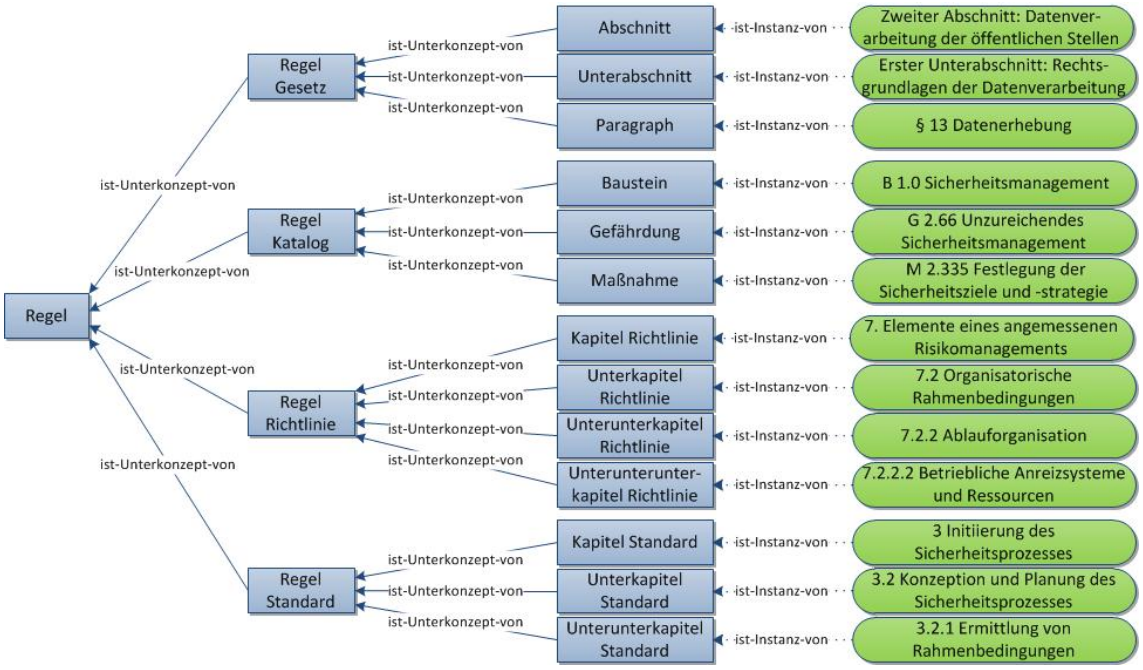

Abbildung 3.3: Modellierung der Regeln

Die Abbildung 3.3 zeigt eine Darstellung der Überlegungen zur Modellierung der Regeln. Die Beispiele für die Instanzen der Regeln stammen aus den folgenden Regelwerken:

- *Gesetz:* Bundesdatenschutzgesetz
- *Katalog:* BSI IT-Grundschutz-Kataloge
- *Richtlinie:* MaRisk VA
- *Standard:* BSI-Standard 100-2

Die Modellierung der Regelwerke und ihrer Regeln in dieser Ontologie hängt stark von dem Aufbau der betrachteten Regelwerke ab. Für die Einbeziehung weiterer Regelwerke müsste diese Modellierung bei Strukturabweichungen angepasst werden.

3.2.3 Relationen

Für die Verbindungen zwischen den Regelwerken lassen sich verschiedene Arten von Relationen definieren. Die Verbindungen konzentrieren sich meist auf gemeinsame Themenbereiche, die in den unterschiedlichen Regelwerken enthalten sind. Zu den gemeinsamen Themen gehören z.B. Risikomanagement mit unterschiedlichen Schwerpunkten, Notfallmanagement oder technische und organisatorische Maßnahmen zur Sicherstellung bestimmter Eigenschaften wie Vertraulichkeit oder Integrität.
Verbindungen zum *Bundesdatenschutzgesetz* sind grundsätzlich an den Stellen möglich, wo explizit Datenschutz oder die Beachtung von Gesetzen gefordert wird. Außerdem an den Stellen, wo z.B. Daten, Informationen oder Dokumente eine Rolle spielen.

Relation	Inverse Relation
verweistAufRegelwerk	hatVerweisVon
verweistImplizitAufRegelwerk	hatVerweisImplizitVon
verweistAufRegel	hatVerweisVonRegel
hatTeilelement	istTeilelementVon
erfordertBeachtungVon	hatBeachtetZuWerdenIn
unterstütztVon	bietetUnterstützungFür
istSpezialisiertIn	istVerallgemeinertIn
istKomplementärZu	istKomplementärZu

Abbildung 3.4: Relationen für die Regelwerke und Regeln mit ihren inversen Relationen

Abbildung 3.4 fasst die definierten Relationen mit den zugehörigen inversen Relationen zusammen. Für die Definition der Relationen für die Regelwerke und Regeln werden folgende Mengen festgelegt:

- RW = { r | r ist ein *Regelwerk* oder Unterkonzept oder eine Instanz des Konzeptes *Regelwerk*}
- R = { r | r ist eine *Regel* oder Unterkonzept oder eine Instanz des Konzeptes *Regel*}
- G = { g | g ist ein *Gesetz* oder eine Instanz des Konzeptes *Gesetz*}
- RG = { g | g ist eine *Regel Gesetz* oder eine Instanz des Konzeptes *Regel Gesetz*}

Die Menge G ist eine Teilmenge von RW und die Menge RG ist eine Teilmenge von R. Die Mengen werden zur genaueren Abgrenzung der Bereiche der Relationen gebraucht. Die Bereiche geben an, welche Elemente mit der Relation überhaupt verbunden werden können.
In den nächsten Unterabschnitten werden die Relationen beschrieben sowie anhand eines oder mehrerer Beispiele verdeutlicht. Die Beispiele sind Ausschnitte aus den angegebenen Regeln. Von den Relationen und ihren inversen Relationen aus Abbildung 3.4 wird im Folgenden nur die Relation (erste Spalte von Abbildung 3.4) beschrieben.

Relation: unterstütztVon

- Bereich: $unterstütztVon \subseteq \{RW, R\} \times \{RW, R\}$
- Beschreibung: Diese Relation beschreibt die Verbindung zu Regelwerken oder Regeln, die helfen können die Umsetzung einer Regel oder eines Regelwerks zu unterstützen.

Am Beispiel des Paragraphen §9 des *Bundesdatenschutzgesetzes* soll diese Relation verdeutlicht werden:

3.2.2 Beispiel (BDSG). §9 Technische und organisatorische Maßnahmen
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die *technischen und organisatorischen Maßnahmen* zu treffen, die erforderlich sind, um die *Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen*, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die schräg gestellten Wörter in dem Beispiel sind für diese Relation relevante Stellen. In der Anlage werden als Anforderung z.B. Zugangs-, Zugriffs- und Eingabekontrolle genannt. Die Maßnahmen können durch ein Informationssicherheitsmanagementsystem umgesetzt werden, wie es in *ISO/IEC 27001* und dem *BSI-Standard 100-1* beschrieben wird.
Damit sind

- (BDSG §9, ISO/IEC 27001) $\in$ *unterstütztVon* und
- (BDSG §9, BSI-Standard 100-1) $\in$ *unterstütztVon*.

3.2.3 Beispiel (MaRisk VA). Kapitel 7.2.2.2: Betriebliche Anreizsysteme und Ressourcen [...]
3 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 [...]

Zur Sicherstellung dieser Eigenschaften können u.a. kryptographische Verfahren eingesetzt werden. Dabei kann der Baustein *B1.7 Kryptokonzept* aus dem IT-Grundschutz-Katalog Unterstützung bieten. Deswegen gilt:

- (MaRisk VA Kap.7.2.2.2, BSI Baustein B1.7) $\in$ *unterstütztVon*

Relation: erfordertBeachtungVon

- Bereich: $erfordertBeachtungVon \subseteq \{RW, R\} \times \{G, RG\}$
- Beschreibung: Die Relation verweist auf die verpflichtende Beachtung von Regeln. Das ist bei Gesetzen der Fall. Daher verweist diese Relation auf Elemente des Konzeptes *Gesetz* oder auf Elemente des Konzeptes *Regel Gesetz*.

3.2.4 Beispiel (BSI-Standard 100-4). Kapitel 3.3: Sicherheit und Datenschutz [...]
Da die Dokumente zum Notfallmanagement sowohl sensitive Daten über die Institution als auch *personenbezogene Daten* beinhalten, muss die Informationssicherheit und der *Datenschutz* gewährleistet werden. [...]

Diese Regel erfordert die Beachtung des *Bundesdatenschutzgesetzes*, da dort spezifiziert ist, was beim Datenschutz und im Umgang mit personenbezogenen Daten beachtet werden muss. Es gilt also:

- (BSI 100-4 Kap.3.3, BDSG) $\in$ *erfordertBeachtungVon*

> **3.2.5 Beispiel (MaRisk VA). Kapitel 5:Risiken** [...]
> - Operationelles Risiko [...]
> **Erläuterungen zu den Anforderungen**
> Das operationelle Risiko bezeichnet das Risiko von *Verlusten* aufgrund von *unzulänglichen oder fehlgeschlagenen internen Prozessen* oder aus *mitarbeiter- und systembedingten oder aber externen Vorfällen*. Das operationelle Risiko umfasst auch *Rechtsrisiken*, jedoch nicht strategische Risiken und Reputationsrisiken. [...]

Relevant für diese Regel können die Paragraphen §43 und §44 des *BDSG* sein. In diesen Paragraphen werden die Bußgelder und Strafen für die Nichteinhaltung des *BDSG* spezifiziert und können somit ein operationelles Risiko darstellen.
Es gelten also:

- (MaRisk VA Kap.5, BDSG Paragraph 43) $\in$ *erfordertBeachtungVon*
- (MaRisk VA Kap.5, BDSG Paragraph 44) $\in$ *erfordertBeachtungVon*

Relation: hatTeilelement

- Bereich: $hatTeilelement \subseteq \{RW, R\} \times R$
- Beschreibung: Die Relation wird zur Darstellung der hierarchischen Beziehungen zwischen den Instanzen der Regelwerke und Regeln verwendet. Zu den Instanzen der *Kapitel* können die passenden Instanzen der *Unterkapitel* zugeordnet werden, zu den *Unterkapiteln* die *Unterunterkapitel* etc.

> **3.2.6 Beispiel (BSI-Standard 100-3).** [...]
> 6 Behandlung von Risiken
> 6.1 Handlungsalternativen zum Umgang mit Risiken
> 6.2 Risiken unter Beobachtung [...]

Dieser Ausschnitt aus dem *BSI-Standard 100-3* wird mit der Relation *hatTeilelement* folgendermaßen dargestellt:

- (BSI 100-3, BSI 100-3 Kap.6) $\in$ *hatTeilelement*
- (BSI 100-3 Kap.6, BSI 100-3 Kap.6.1) $\in$ *hatTeilelement*
- (BSI 100-3 Kap.6, BSI 100-3 Kap.6.2) $\in$ *hatTeilelement*

Relation: verweistAufRegelwerk

- Bereich: $verweistAufRegelwerk \subseteq R \times RW$

- Beschreibung: Die Relation wird für explizite Verweise einer Regel auf ein anderes Regelwerk eingesetzt. Unter explizitem Verweis wird die Nennung des Namens eines Regelwerkes in den Regeln oder in offiziellen Erläuterungen oder Anhängen zu den Regelwerken verstanden.

> **3.2.7 Beispiel (MaRisk VA). Kapitel 7.2.2.2: Betriebliche Anreizsysteme und Ressourcen** [...]
> 3 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. Ihre Eignung ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.
> **Erläuterungen der Anforderungen**
> Standards zur Ausgestaltung der IT-Systeme:
> Zu solchen Standards zählen z.B. das *IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der internationale Sicherheitsstandard ISO/IEC 27002 der International Standards Organization*. Das Abstellen auf gängige Standards zielt nicht auf die Verwendung von Standardhardware beziehungsweise -software ab. Eigenentwicklungen sind grundsätzlich ebenso möglich. [...]

In den Erläuterungen werden das *IT-Grundschutzhandbuch des BSI* und *ISO/IEC 27002* als Regelwerke genannt, die zur Umsetzung der Anforderungen in der Regel benutzt werden können. Es gilt also:

- (MaRisk VA Kap.7.2.2.2, BSI IT-Grundschutz-Kataloge) $\in$ *verweistAufRegelwerk*

- (MaRisk VA Kap.7.2.2.2, ISO/IEC 27002) $\in$ *verweistAufRegelwerk*

Relation: verweistImplizitAufRegelwerk

- Bereich: $verweistImplizitAufRegelwerk \subseteq R \times RW$

- Beschreibung: Die Relation beschreibt die Verbindung einer Regel mit einem Regelwerk, wenn das Regelwerk nicht explizit angegeben wird. Die Relation wird für die Regeln benutzt, in denen zwar auf andere Regelwerke verwiesen wird, aber wo keine genauere Angabe vorhanden ist. Abhängig vom Kontext kann die Art der Regelwerke eventuell auch eingeschränkt werden.

3.2.8 Beispiel (BSI-Standard 100-4). Kapitel 4.4: Erstellung einer Leitlinie zum Notfallmanagement [...]
Eine Leitlinie zum Notfallmanagement sollte kurz und übersichtlich gehalten werden und mindestens folgende Aspekte enthalten: [...]
- die *relevanten Gesetze, Richtlinien und Vorschriften*, die zu beachten sind, [...]

In dieser Regel ist von der Beachtung von Richtlinien die Rede, dazu kann auch die *MaRisk VA* zählen. Die Gesetze werden über die Relation *erfordertBeachtungVon* speziell behandelt. Deshalb gilt für diese Regel:

- (BSI 100-4 Kap.4.4, MaRiskVA) $\in$ *verweistImplizitAufRegelwerk*
- (BSI 100-4 Kap.4.4, Gesetz) $\in$ *erfordertBeachtungVon*

Relation: verweistAufRegel

- Bereich: $verweistAufRegel \subseteq R \times R$
- Beschreibung: In den Regelwerken wird oft auf andere Regeln innerhalb des Regelwerks oder innerhalb einer Reihe von Standards verwiesen. Insbesondere bei den ISO-Standards werden oft Verweise auf die anderen ISO-Standards gemacht.

3.2.9 Beispiel (MaRisk VA). Kapitel 5: Risiken [...]
Die Bestimmung der wesentlichen Risiken ist das Ergebnis der unternehmensindividuellen Risikoidentifikation *(7.3.2.1)* sowie Risikoanalyse und -bewertung *(7.3.2.2)* und der unternehmensindividuellen Skalierung der Wesentlichkeit. [...]

Hier wird definiert, dass

- (MaRisk VA Kap.5, MaRisk VA Kap.7.3.2.1) $\in$ *verweistAufRegel*
- (MaRisk VA Kap.5, MaRisk VA Kap.7.3.2.2) $\in$ *verweistAufRegel*

sind.

Relation: istKomplementärZu

- Bereich: $istKomplementärZu \subseteq \{RW, R\} \times \{RW, R\}$
- Beschreibung:
  Für die *IT-Grundschutz-Kataloge*, die *BSI-Standards* und die ISO-Standards *ISO 27001* und *ISO 27002* bietet das BSI eine Zuordnungstabelle an (siehe [BSIb]). Es werden zu jedem Kapitel der ISO-Standards die ergänzenden Regeln aus den BSI-Veröffentlichungen aufgestellt. Die Relation beschreibt diese Zuordnungen. Die Standards sollen sich ergänzen und da die BSI-Veröffentlichungen mit einer praktischen Ausrichtung formuliert sind als die Regeln der ISO-Standards, ist es mit der Relation möglich genauere Angaben für die Umsetzung der ISO-Standards zu finden.

3.2.10 Beispiel (Zuordnungstabelle).
Ein Ausschnitt aus der Tabelle sieht folgendermaßen aus:

ISO 27001	**IT-Grundschutz**
4.2.1 Establish the ISMS	B 1.0 Sicherheitsmanagement BSI-Standard 100-2 Kapitel 3, 4 und 5 BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz M 2.192 Erstellung einer Leitlinie zur Informationssicherheit M 2.335 Festlegung der Sicherheitsziele und -strategie

Diese Regeln werden folgendermaßen zugeordnet:

- (ISO/IEC 27001 Kap.4.2.1, BSI Baustein B1.0) $\in$ *istKomplementärZu*
- {(ISO/IEC 27001 Kap.4.2.1, BSI 100-2 Kap.3), (ISO/IEC 27001 Kap.4.2.1, BSI 100-2 Kap.4), (ISO/IEC 27001 Kap.4.2.1, BSI 100-2 Kap.5)} $\in$ *istKomplementärZu*
- (ISO/IEC 27001 Kap.4.2.1, BSI 100-3) $\in$ *istKomplementärZu*
- {(ISO/IEC 27001 Kap.4.2.1, BSI Maßnahme M2.192), (ISO/IEC 27001 Kap.4.2.1, BSI Maßnahme M2.335)} $\in$ *istKomplementärZu*

Relation: istSpezialisiertIn

- Bereich: $istSpezialisiertIn \subseteq \{RW, R\} \times \{RW, R\}$
- Beschreibung:
  Die Relation *istSpezialisiertIn* beschreibt die Spezialisierung der Elemente einer Regel. Das bedeutet, dass der Inhalt einer Regel in einer anderen Regel für einen spezifischeren Fall beschrieben wird oder genauere Angaben zu einer Aktivität oder einem Prozess gemacht werden.

3.2.11 Beispiel (MaRisk VA). Kapitel 10: Information und Dokumentation [...]
Hinsichtlich der Dokumentation gelten die Anforderungen des § 64a Abs. 3 VAG. [...]
Erläuterungen zu den Anforderungen [...]
Die *Dokumentation* soll einen systematischen Überblick über *Risiken, Prozesse und Kontrollen* geben. [...]

In der *MaRisk VA* wird eine Dokumentation von Risiken, Prozessen und Kontrollen gefordert. In *ISO 27001* werden in Kapitel 4.3 genauere Anforderungen für das Informationssicherheitsmanagementsystem bezüglich der Dokumentation gestellt. Da die spezifischen Risiken aus dem Bereich der Informationssicherheit eine Teilmenge der Risiken eines Unternehmens sind, könnten die Anforderungen auch bei der allgemeinen Dokumentation als Bestandteil für die Risiken dieses Bereichs genutzt werden. Deswegen gilt:

- (MaRisk VA Kap.10, ISO/IEC 27001 Kap.4.3) $\in$ *istSpezialisiertIn*

In Kapitel 10 der *MaRisk VA* könnte zudem eine Verbindung zum *§64a Abs.3 VAG* mit der Relation *erfordertBeachtungVon* hergestellt werden. In dieser Arbeit wird diese Verbindung aber nicht beachtet, weil das *VAG (Gesetz über die Beaufsichtung der Versicherungsunternehmen)* nicht zu den in Kapitel 2 genannten Regelwerken zählt.

Im nächsten Abschnitt soll nun überlegt werden, wie die Verbindung der Regelwerke zu Geschäftsprozessen möglich ist.

3.3 Elemente der Regelwerke

In den Regelwerken und in Geschäftsprozessen lassen sich verschiedene Arten von Elementen identifizieren. Bezüglich dieser Elemente können die folgenden Fragen gestellt werden:

- Welche *Person* macht etwas?
- Welche *Aktivität* oder welcher *Prozess* wird aus- oder durchgeführt?
- Welches *Objekt* wird dabei benutzt?
- Welche *Eigenschaft* will man erreichen oder muss man beachten?

Für die Ontologie wird zunächst das Konzept *Regelelement* als Oberbegriff gewählt. Die Elemente, die in den Regelwerken und Geschäftsprozessen identifiziert werden können, und als Unterkonzepte von *Regelelement* gewählt werden, sind: *Person*, *Objekt*, *Aktivität*, *Eigenschaft* und *Prozess*. Die Abbildung 3.5 zeigt die Struktur dieser Konzepte mit einer beispielhaften Auswahl von Konzepten als Unterkonzepte für die fünf Elemente.

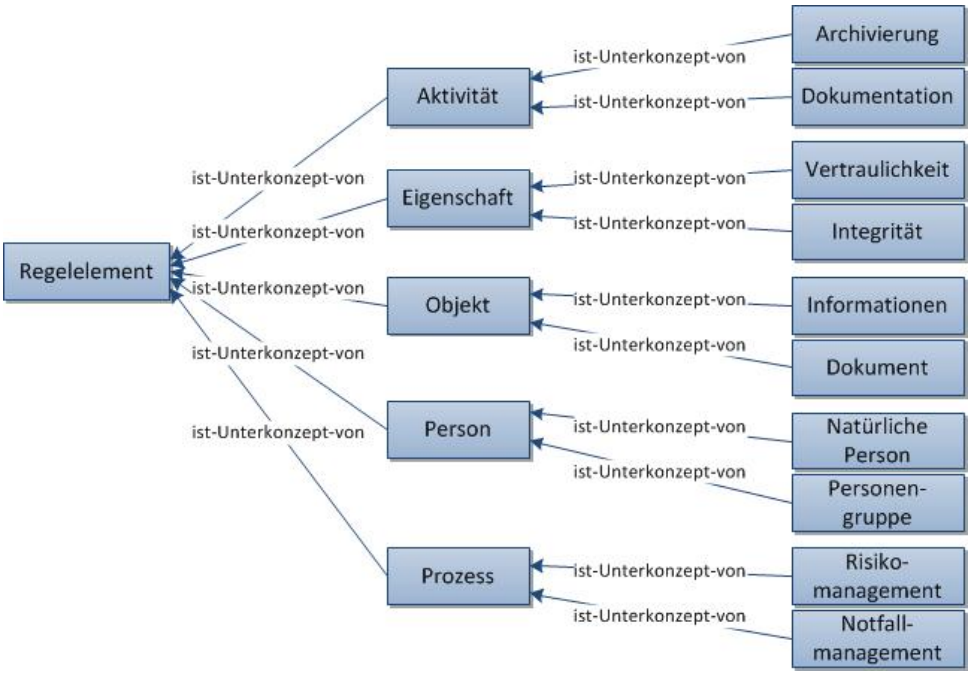

Abbildung 3.5: Elemente der Regelwerke

Die fünf Elemente werden in den nächsten Abschnitten beschrieben. Für diese Arbeit sind dabei vor allem die Elemente interessant, die in verschiedenen Regelwerken von Bedeutung sind oder denen innerhalb eines Regelwerkes viel Bedeutung zugemessen wird. Nach der Beschreibung der Elemente werden für die Verbindungen zwischen den Regelelementen Relationen definiert.

3.3.1 Beschreibung der Elemente

Person

In den Regeln werden eine Vielzahl von Personen erwähnt, für die:

- Rollen und Aufgaben definiert,
- Verantwortlichkeiten festgelegt,
- Maßnahmen gefordert,
- Gefährdungen genannt oder
- deren Mitwirkung an Aktivitäten gefordert wird.

Die grundsätzliche Unterscheidung von *Person* erfolgt in natürliche und Personengruppe erfolgen. Unter dem Konzept *Natürliche Person* werden in der Ontologie einzelne Menschen mit ihren Rollen im Unternehmenskontext zusammengefasst. Unter dem Konzept *Personengruppe* werden in dieser Ontologie verschiedene Arten der Gruppen von Personen mit gemeinsamen Eigenschaften oder Aufgaben verstanden. Für das Konzept *Person* werden daher die Unterkonzepte *Natürliche Person* und *Personengruppe* angelegt. In diese Unterkonzepte werden die in den Regelwerken auftretenden Personen einsortiert.
Exemplarisch sollen für *Person* ein paar Konzepte aufgezählt werden:

3.3.1 Beispiel (Konzepte für *Person*).

- Natürliche Person: Mitarbeiter, Beauftragte, Betroffene
- Persongruppe:
  - Organisationseinheit: Finanzabteilung, Geschäftsleitung, Management, IT-Abteilung
  - Unternehmen
  - Stelle: Öffentliche und Nicht-öffentliche Stellen
  - Externe: Kunde, Lieferant, Dienstleister, Behörde
  - Personal: Reinigungspersonal, Fremdpersonal

Objekt

Das Konzept *Objekt* wird als Oberbegriff für materielle und immaterielle Gegenstände verwendet. Das können greifbare Objekte, wie Einrichtungsgegenstände im Unternehmen sein oder nicht greifbare Objekte wie Software oder Risiken.

3.3.2 Beispiel (Konzepte für *Objekt*).

- System (Betriebssystem, IT-System)
- Anwendung (Datenbank, E-Mail)
- Dokument (Anleitung, Datei, Vertrag)
- Risiko

Aktivität

Aktivitäten sind ein elementarer Bestandteil von Geschäftsprozessen und bezeichnen ausführbare Aktionen. In den Regelwerken werden Regeln definiert, die sich auf bestimmte Aktivitäten beziehen und deren Rahmenbedingungen festlegen. Die Unterkonzepte des Konzeptes *Aktivität* werden als Substantive in der Ontologie formuliert. Das Beispiel enthält zur Verdeutlichung eine exemplarische Auswahl an Aktivitäten aus den Regelwerken.

3.3.3 Beispiel (Konzepte für *Aktivität*).

- Erhebung, Nutzung, Verarbeitung
- Aktivität Risikomanagement (Risikoanalyse, Risikobewertung, Risikosteuerung)
- Archivierung, Entsorgung

Eigenschaft

In den Regelwerken werden Eigenschaften genannt, die z.B. für Objekte, Aktivitäten oder die Rollen von Personen wichtig sind. In dem Beispiel sind vier Eigenschaften aufgeführt, die im Bereich der Informationssicherheit eine tragende Rolle spielen und denen daher in den ISO- und BSI-Standards ein hoher Stellenwert eingeräumt wird.

3.3.4 Beispiel (Konzepte für *Eigenschaft*).
Elementare Eigenschaften in den Regelwerken sind:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität

Prozess

Neben den einzelnen Aktivitäten werden in den Regelwerken auch Regeln für größere (Management-) Prozesse festgelegt. Diese Prozesse bestehen wiederum aus einzelnen Aktivitäten. Das Konzept *Prozess* wird daher als eigenes Unterkonzept für das Konzept *Regelelement* eingeführt.

3.3.5 Beispiel (Konzepte für *Prozess*).
Wichtige Prozesse, die in unterschiedlichen Ausprägungen in den verschiedenen Regelwerken auftreten, sind:

- Risikomanagement (Besteht aus Aktivitäten, die zu *Aktivität Risikomanagement* gehören)
- Notfallmanagement
- Sicherheitsmanagement

3.3.2 Relationen zwischen den Elementen

Zwischen den Elementen der fünf Kategorien können auch Verbindungen bestehen. Die Abbildung 3.6 zeigt die Relationen zwischen den Regelelementen und die zugehörigen inversen Relationen.
Ergänzend zu den definierten Mengen in Kapitel 3.2.3, werden für die Beschreibung der Relationen folgende Mengen festgelegt:

- A = { a | a ist ein Unterkonzept des Konzeptes *Aktivität*}
- P = { p | p ist ein Unterkonzept des Konzeptes *Person*}
- O = { o | o ist ein Unterkonzept des Konzeptes *Objekt* oder eine Instanz von *Objekt*}
- E = { e | e ist ein Unterkonzept des Konzeptes *Eigenschaft*}
- Pro = { p | p ist ein Unterkonzept des Konzeptes *Prozess*}

Relation	Inverse Relation
hatTeilprozess	istTeilprozessVon
hatTeil	istEinTeilVon
benutztObjekt	wirdBenutztFür

Abbildung 3.6: Relationen zwischen den Regelelementen

Relation: hatTeil

- Bereich: $hatTeil \subseteq (P \times P) \cup (A \times A)$
- Beschreibung: Diese Relation beschreibt die Bestandteile von Personengruppen oder von umfassenderen Aktivitäten, die keine Prozesse sind. Für eine Personengruppe können damit die Mitglieder dieser Gruppe benannt werden. Aktivitäten können in Teilaktivitäten aufgeteilt werden.

3.3.6 Beispiel (BSI-Standard 100-4).
Der *Krisenstab* besteht aus einem Kernteam, dem erweiterten Krisenstab und dem Leiter des Krisenstabs.

3.3.7 Beispiel (Bundesdatenschutzgesetz).
Die Aktivität *Verarbeitung* besteht aus den Aktivitäten Speicherung, Veränderung, Löschung, Übermittlung und Sperrung.

Für diese Beispiele gilt dann:

- {(Krisenstab, Kernteam), (Krisenstab, Erweiterter Krisenstab), (Krisenstab, Leiter Krisenstab)} $\in hatTeil$
- {(Verarbeitung, Speicherung), (Verarbeitung, Veränderung), (Verarbeitung, Löschung), (Verarbeitung, Übermittlung), (Verarbeitung, Sperrung)} $\in hatTeil$

Relation: hatTeilprozess

- Bereich: $hatTeilprozess \subseteq Pro \times A$
- Beschreibung: In Abschnitt 3.3.1 wurde bereits erwähnt, dass Prozesse aus einzelnen Aktivitäten bestehen. Mit dieser Relation werden dem Prozess die zugehörigen Aktivitäten zugeordnet.

3.3.8 Beispiel (Risikomanagement).
Folgende Aktivitäten, die Unterkonzepte von *Aktivität Risikomanagement* sind, gehören unter anderem zum Prozess Risikomanagement:

- Risikobewertung
- Risikoanalyse
- Risikosteuerung

Es gilt somit:

- {(Risikomanagement, Risikobewertung), (Risikomanagement, Risikoanalyse), (Risikomanagement, Risikosteuerung)} $\in hatTeilprozess$

Relation: benutztObjekt

- Bereich: $benutztObjekt \subseteq \{A, Pro\} \times O$
- Beschreibung: Bei Aktivitäten und Prozessen können bestimmte Objekte benutzt werden oder bei der Durchführung sogar notwendig sein. Mit dieser Relation werden die Objekte diesen Aktivitäten und Prozessen zugeordnet.

3.3.9 Beispiel (Benutzte Objekte).

- Für die Aktivität *Drucken* wird das Objekt *Drucker* benötigt.
- Für die Aktivität *Berichten* kann das Objekt *Bericht* benutzt werden.
- In dem Prozess *Risikomanagement* können das Objekt *Dokument Risikomanagement* oder die Objekte, die Unterklassen von diesem Konzept sind, benutzt werden.

Für diese Beispiele gilt daher:

- (Drucken, Drucker) $\in$ *benutztObjekt*
- (Berichten, Bericht) $\in$ *benutztObjekt*
- (Risikomanagement, Dokument Risikomanagement) $\in$ *benutztObjekt*

3.4 Relationen zwischen Regeln und Elementen

In den beiden vorherigen Abschnitten wurden bisher nur Relationen definiert, die sich auf die Verbindungen zwischen den Regeln und Regelwerken oder zwischen den Regelelementen bezogen. In diesem Abschnitt werden Relationen eingeführt, die diese Mengen auch untereinander verbinden können. Abbildung 3.7 zeigt die Relationen mit ihren inversen Relationen.
Zu den Bestandteilen der *IT-Grundschutz-Kataloge* des BSI gehören ein Gefährdungskatalog und ein Maßnahmenkatalog. In Kapitel 2.1.3 wurde bereits beschrieben, dass diese Kataloge gängige Gefährdungen und Maßnahmen für Unternehmen enthalten, die in Kategorien unterteilt sind. Diese Gefährdungen und Maßnahmen bieten den Vorteil, dass sie elementare Informationen und Vorschläge zu bestimmten Elementen liefern können. Deswegen werden für diese Elemente zwei zusätzliche Relationen definiert, die speziell für die

Relation	Inverse Relation
istDefiniertIn	hatDefinitionVon
istEigenschaftIn	hatEigenschaft
istAktivitätIn	hatAktivität
istObjektIn	hatObjekt
istPersonIn	hatPerson

Abbildung 3.7: Relationen zwischen den Regelwerken und Regelelementen

Relation	Inverse Relation
hatMaßnahme	istMaßnahmeFür
hatGefährdung	istGefährdungFür

Abbildung 3.8: Relationen für Maßnahmen und Gefährdungen

Verbindung von Elementen zu einzelnen Regeln der Gefährdungs- und Maßnahmenkataloge benutzt werden können. Abbildung 3.8 zeigt die beiden Relationen mit ihren inversen Relationen.

3.4.1 Beschreibung der Relationen

Für die Beschreibung der Relationen zur Verbindung der Regeln mit den Regelelementen müssen noch weitere Mengen definiert werden:

- RE = A ∪ O ∪ E ∪ P ∪ Pro
- M = { m | m ist eine Instanz des Konzeptes *Maßnahme*}
- G = { g | g ist eine Instanz des Konzeptes *Gefährdung*}

Relation: istDefiniertIn

- Bereich: $istDefiniertIn \subseteq RE \times \{RW, R\}$
- Beschreibung: Die Relation verweist von einem Element auf Regeln, in denen das Element oder Aufgaben und Funktionen des Elementes definiert werden. Diese Relation ist wichtig, wenn zunächst eine Definition oder Erklärung eines Elementes gefunden werden soll und z.B. nicht nur die Regeln, die Anweisungen für den Umgang mit diesem Element enthalten.

> **3.4.1 Beispiel (BDSG). §3 Weitere Begriffsbestimmungen**
> (1) *Personenbezogene Daten* sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). [...]

Personenbezogene Daten werden in diesem Paragraphen des *BDSG* definiert und damit gilt:

- (Personenbezogene Daten, BDSG §3) ∈ *istDefiniertIn*

Relation: istEigenschaftIn

- Bereich: $istEigenschaftIn \subseteq E \times \{RW, R\}$
- Beschreibung: Diese Relation verweist von einer Eigenschaft auf Regeln oder Regelwerke, in denen diese Eigenschaft eine Rolle spielt.

3.4.2 Beispiel (BSI-Standard 100-4). Kapitel 5.5.1: Feinkonzeption, Sicherheit und Kontrollen [...]
Es ist sicherzustellen, dass sowohl im Notbetrieb wie auch beim Wechsel zurück in den Normalbetrieb die Sicherheit gewährleistet ist, wie beispielsweise die Einhaltung der gesetzlichen Vorgaben zum Schutze der Mitarbeiter oder die Gewährleistung der *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* von Informationen. [...]

3.4.3 Beispiel (IT-Grundschutz-Kataloge). B1.7 Kryptokonzept [...]
Gefährdungslage
Kryptographische Verfahren werden eingesetzt zur Gewährleistung von
- *Vertraulichkeit*,
- *Integrität*,
- *Authentizität* und
- Nichtabstreitbarkeit. [...]

In den beiden Ausschnitten aus den Regelwerken sind die Eigenschaften *Vertraulichkeit*, *Integrität*, *Authentizität* und *Verfügbarkeit* zu beachten. Daher gilt für dieses Beispiel:

- {(Vertraulichkeit, BSI 100-4 Kap.5.5.1), (Vertraulichkeit, BSI Baustein B1.7)} $\in$ *istEigenschaftIn*
- {(Integrität, BSI 100-4 Kap.5.5.1), (Integrität, BSI Baustein B1.7)} $\in$ *istEigenschaftIn*
- (Verfügbarkeit, BSI 100-4 Kap.5.5.1) $\in$ *istEigenschaftIn*
- (Authentizität, BSI Baustein B1.7) $\in$ *istEigenschaftIn*

Relation: istAktivitätIn

- Bereich: $istAktivitätIn \subseteq \{Pro, A\} \times \{RW, R, A\}$
- Beschreibung: Diese Relation beschreibt die Verbindung von Prozessen oder Aktivitäten zu Regeln, Regelwerken oder anderen Aktivitäten. So können Regeln gefunden werden, die Rahmenbedingungen für die Durchführung von Aktivitäten vorgeben. Die Verbindung zu anderen Aktivitäten tritt auf, wenn eine Aktivität in einem speziellen Kontext auch als Teil einer anderen Aktivität ausgeführt werden kann.

3.4.4 Beispiel (BDSG). §31 Besondere Zweckbindung
Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der *Datensicherung* oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

3.4.5 Beispiel (IT-Grundschutz-Kataloge). B1.4 Datensicherungskonzept [...]
Eine *Datensicherung* soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen. [...]

In diesen Regeln spielt die Datensicherung eine Rolle. Das allgemeinere Konzept *Sicherung* wird mit diesen Regeln in Relation gesetzt:

- {(Sicherung, BDSG §31), (Sicherung, BSI Baustein B1.4)} $\in$ *istAktivitätIn*

Relation: istObjektIn

- Bereich: $istObjektIn \subseteq O \times \{RW, R\}$
- Beschreibung: Diese Relation beschreibt, wenn in welchen Regeln ein Objekt vorhanden ist.

3.4.6 Beispiel (IT-Grundschutz-Kataloge). B3.406 *Drucker*, *Kopierer*
und *Multifunktionsgeräte*
Beschreibung
Zur Grundausstattung in Büroumgebungen gehören typischerweise *Kopierer* sowie bei IT-Arbeitsplätzen *Drucker*. [...]
Dieser Baustein behandelt die Sicherheit von vernetzten *Druckern*, Druckservern, *Dokumentenscannern*, *Kopierern* und *Multifunktionsgeräten*. [...]

Dieser Baustein enthält Informationen für *Drucker*, *Kopierer*, *Scanner* und *Multifunktionsgeräte* und daher gilt:

- {(Drucker, BSI Baustein B3.406), (Kopierer, BSI Baustein B3.406), (Scanner, BSI Baustein B3.406), (Multifunktionsgerät, BSI Baustein B3.406)} $\in$ *istObjektIn*

Relation: istPersonIn

- Bereich: $istPersonIn \subseteq P \times \{RW, R\}$
- Beschreibung: Die Relation verbindet Personen mit den Regeln,
  - in denen die Mitarbeit von bestimmten Personen gefordert ist,
  - die bestimmte Personen oder Personengruppen betreffen, oder
  - in denen Verantwortlichkeiten festgelegt werden.

3.4.7 Beispiel (MaRisk VA). Kapitel 6: Gesamtverantwortung der *Geschäftsleitung*
1 Alle *Geschäftsleiter* sind - unabhängig von der internen Zuständigkeitsregelung - für die ordnungsgemäße Geschäftsorganisation des Unternehmens *verantwortlich* (§ 64a Abs. 1 Satz 2, § 104s Satz 3 VAG). [...]

3.4.8 Beispiel (BSI-Standard 100-2). Kapitel 3.6: Einbindung aller *Mitarbeiter* in den Sicherheitsprozess
Informationssicherheit betrifft ohne Ausnahme alle *Mitarbeiter*. Jeder Einzelne kann durch verantwortungs- und sicherheitsbewusstes Handeln dabei helfen, Schäden zu vermeiden und zum Erfolg beitragen. Sensibilisierung für Informationssicherheit und fachliche Schulungen der *Mitarbeiter* sind daher eine Grundvoraussetzung für Informationssicherheit. [...]

Aus diesen Beispielen folgt:

- (Geschäftsleitung, MaRisk VA Kap.6) $\in$ *istPersonIn*
- (Mitarbeiter, BSI 100-2 Kap.3.6) $\in$ *istPersonIn*

Relation: hatMaßnahme

- Bereich: $hatMaßnahme \subseteq RE \times M$
- Beschreibung: Diese Relation kann für die Regelelemente benutzt werden, um diesen einzelne Maßnahmen aus den Maßnahmen-Katalogen der IT-Grundschutz-Kataloge zuzuordnen.

3.4.9 Beispiel (IT-Grundschutz-Kataloge). M2.31 *Dokumentation der zugelassenen Benutzer* und Rechteprofile [...]
Es muss eine *Dokumentation* der am *IT-System* zugelassenen *Benutzer*, angelegten Benutzergruppen und Rechteprofile erfolgen. [...]

In dieser Maßnahme werden drei Elemente identifiziert, für die gilt:

- Aktivität: Dokumentation
  - (Dokumentation, BSI Maßnahme M2.31) $\in$ hatMaßnahme
- Objekt: IT-System
  - (IT-System, BSI Maßnahme M2.31) $\in$ hatMaßnahme
- Person: Benutzer
  - (Benutzer, BSI Maßnahme M2.31) $\in$ hatMaßnahme

Relation: hatGefährdung

- Bereich: $hatGefährdung \subseteq RE \times G$
- Beschreibung: Diese Relation kann den Regelelementen einzelne Gefährdungen aus den Gefährdungs-Katalogen der IT-Grundschutz-Kataloge zuordnen.

3.4.10 Beispiel (IT-Grundschutz-Kataloge). G3.1 *Vertraulichkeits*- oder *Integritäts*verlust von *Daten* durch Fehlverhalten
Durch Fehlverhalten von *Personen* aller Art kann der *Vertraulichkeits*- bzw. *Integritäts*verlust von *Informationen* und *Daten* herbeiführt bzw. ermöglicht werden. [...]

Diese Gefährdung kann mit fünf Regelelementen assoziiert werden:

- Eigenschaften: Vertraulichkeit und Integrität
  - {(Vertraulichkeit, BSI Gefährdung G3.1), (Integrität, BSI Gefährdung G3.1)} $\in$ *hatGefährdung*
- Objekte: Informationen und Daten
  - {(Informationen, BSI Gefährdung G3.1), (Daten, BSI Gefährdung G3.1)} $\in$ *hatGefährdung*
- Person
  - (Person, BSI Gefährdung G3.1) $\in$ *hatGefährdung*

3.5 Zusammenfassung

Ziel dieses Kapitels war die Modellierung der Ontologie. Die Aufgabe der Ontologie ist die Unterstützung beim Auffinden von relevanten Regeln für andere Regeln oder für einen Geschäftsprozess. Dazu mussten Konzepte, Instanzen und Relationen identifiziert und in Zusammenhang gebracht werden. Der Schwerpunkt lag darauf, die Relationen zwischen den einzelnen Regelwerken zu modellieren sowie eine Verbindung zwischen den Regeln und Geschäftsprozessen herzustellen. Diese Verbindung wurde über die Modellierung von Regelelementen umgesetzt, die sowohl in den Regeln als auch in den Geschäftsprozessen von Relevanz sind.
Die wichtigsten Elemente und der grundsätzliche Aufbau der Ontologie sind in Abbildung 3.9 dargestellt. Die Regelwerke werden in verschiedene Arten unterteilt, die wiederum aus einzelnen Regeln bestehen. In diesen Regeln sind Elemente enthalten, die in fünf Kategorien unterteilt sind: Aktivitäten, Personen, Objekte, Eigenschaften und Prozesse. Mit diesen Elementen ist es möglich eine Verbindung zu den Geschäftsprozessen herzustellen, die ebenfalls solche Elemente beinhalten.

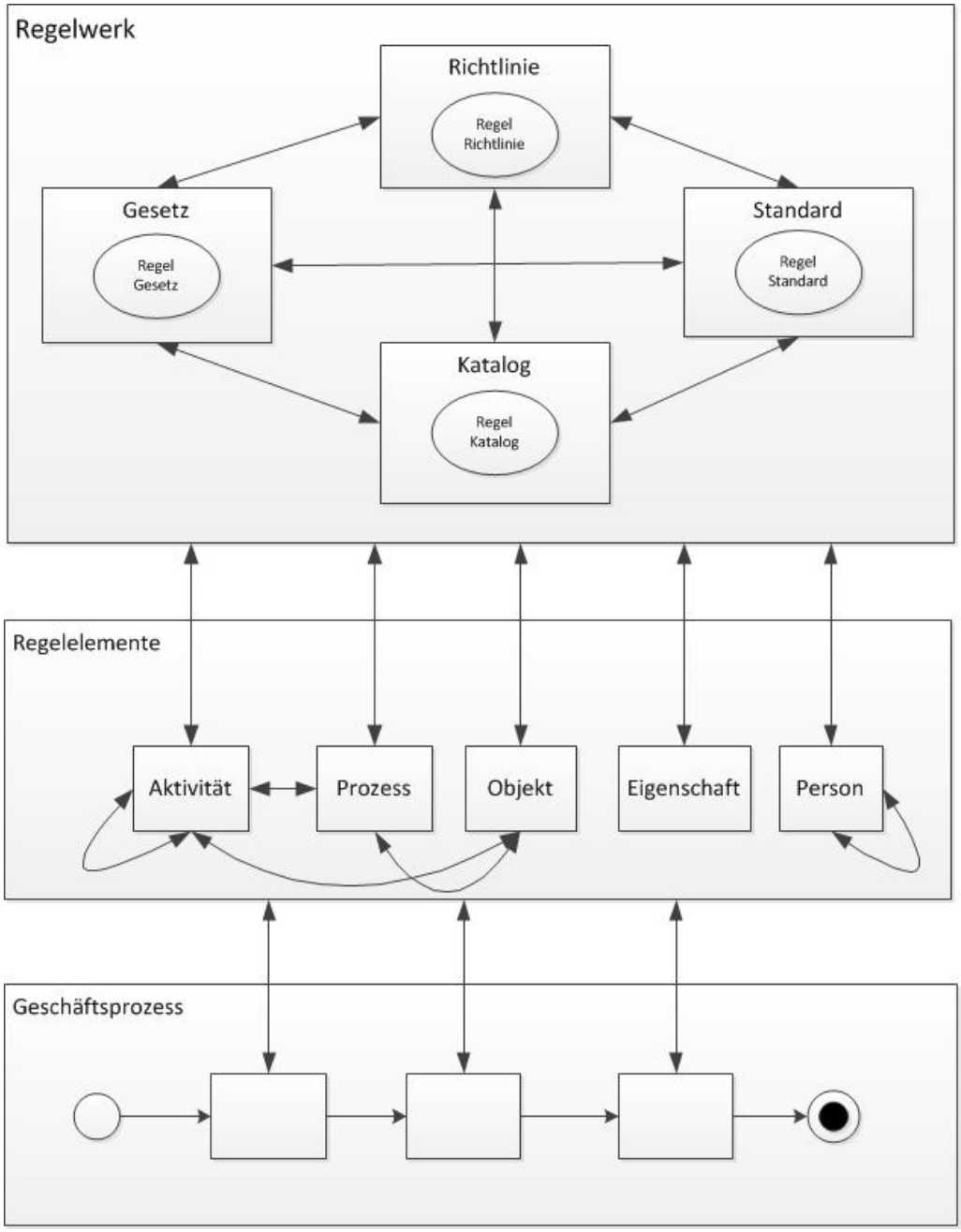

Abbildung 3.9: Gesamtaufbau der Ontologie

Kapitel 4

Anforderungserhebung und Toolauswahl

Dieses Kapitel behandelt die Anforderungserhebung und die darauf basierende Toolauswahl. Um die im vorherigen Kapitel entwickelte Modellierung umzusetzen, soll in diesem Kapitel ein für diesen Zweck passendes Tool zur Ontologie-Erstellung ausgewählt werden. Dieses Ziel erfordert zunächst eine Anforderungserhebung, um die Anforderungen zu identifizieren und definieren, die für die Ontologie als wichtig erachtet werden. Die Menge von Anforderungen an das Ontologie-Tool soll unter anderem Anforderungen enthalten, die zur Erleichterung der Arbeit mit dem Tool beitragen oder zur Modellierung der Ontologie aus Kapitel 3 benötigt werden. Hinsichtlich dieser Anforderungen werden dann vorhandene Ontologie-Tools bewertet und eine Entscheidung getroffen, welches Tool zur Umsetzung der Modellierung verwendet wird.

4.1 Ontologie-Tools

Bei der Entwicklung und Nutzung von Ontologien steht eine Vielzahl von Tools zur Verfügung. Es gibt Systeme, die viele Funktionen anbieten und für verschiedene Aktivitäten genutzt werden können. Es existieren aber auch viele Tools, die sich auf wenige Funktionen konzentrieren und nur für bestimmte Aspekte eingesetzt werden können. In [GPAFL+02] werden folgende Arten von Ontologie-Tools unterschieden:

- Entwicklung von Ontologien:
  Diese Tools legen den Schwerpunkt auf die Erstellung neuer Ontologien oder die Veränderung bereits vorhandener Ontologien. Gängige Zusatzfunktionen in diesen Tools dienen der Dokumentation und dem Import und Export der erstellten Ontologien.

- Zusammenfügen und Integration von Ontologien:
  Diese Tools dienen der Unterstützung beim Zusammenfügen mehrerer Ontologien oder der Integration einer Ontologie in eine andere, um so bessere und umfassendere Ontologien zu generieren.

- Evaluierung von Ontologien:
  Zur Steigerung der Qualität können diese Tools eingesetzt werden, um Ontologien zu evaluieren und so Probleme bei der Integration der Ontologien zu vermeiden.

- Ontologie-basierte Anmerkungen:
  Diese Tools sind im Bereich des *Semantic Web* zur besseren und automatisierten Verwaltung von ontologie-basierten Markierungen in Webseiten hilfreich.

- Anfragen an Ontologien:
  Tools zur Nutzung von Anfragefunktionalitäten an Ontologien.

- Lernen von Ontologien:
  Diese Tools sollen bei der (teilweise) automatischen Generierung von Ontologien aus natürlichsprachlichen Texten Unterstützung leisten, indem sie entsprechende Techniken wie z.B. aus dem *Natural Language Processing* einsetzen.

Ergänzend zu dieser Liste können noch zwei weitere Arten von Ontologie-Tools identifiziert werden:

- Grafische Darstellung von Ontologien:
  Mit diesen Tools können bereits vorhandene Ontologien im Format gängiger Ontologiesprachen in grafischer Form dargestellt werden, um so einen besseren Überblick über die Ontologie zu erhalten.

- Konvertierung von Ontologien:
  Diese Art von Tools dient der Konvertierung einer vorhandenen Ontologie eines bestimmten Formats in ein anderes Format. Durch die unterschiedliche Ausdrucksfähigkeit der Ontologiesprachen kann dies aber problematisch sein, da unter Umständen bestimmte Informationen nicht konvertiert und so verloren gehen können.

Die Herkunft der Tools unterscheidet sich ebenso wie ihre Arten. Die Tools werden in größeren Projekten von Forschung und Wirtschaft, im Rahmen wissenschaftlicher Arbeiten wie z.B. Dissertationen, als Produkt von Unternehmen mit kommerziellem Interesse oder auch als Privatprojekt von einzelnen Personen entwickelt. Deswegen ist der Fokus, die Funktionalität, die Ausgereiftheit und die Verfügbarkeit dieser Tools auch recht unterschiedlich.

4.2 Vorgehensweise Toolauswahl

Eine grundsätzliche Vorgehensweise zur Anforderungsanalyse und Auswahl von Tools wird in den Artikeln [KJ97a], [KJ97b], [KJ97c] und [KJ97d] behandelt. Anhand dieser Artikel wurde eine Vorgehensweise für die Anforderungserhebung und Toolauswahl in dieser Diplomarbeit entwickelt.
Als erster Schritt muss eine Auflistung von potentiellen Tools erstellt werden. Dazu werden zunächst die Listen von zwei Studien zum Thema Ontologie-Tools verwendet ([Den04] und [GPAFL+02]). Da die Studien aus den Jahren 2002 und 2004 stammen und daher nicht den aktuellen Stand widerspiegeln, werden zur Ergänzung die Listen mit Ontologie-Tools von den Webseiten unter [Ber10], [Ber] und [Tec] verwendet.
Dieser Schritt führte zu einer Auflistung von 269 Tools.

Aufgrund der Vielzahl an Tools wird der Auswahlprozess in drei Phasen unterteilt: In der ersten Phase findet eine Auswahl anhand weniger und strenger Kriterien statt (Kapitel 4.3). Dabei handelt es sich um K.O.-Kriterien. Wenn ein Tool eines dieser Kriterien nicht erfüllt, dann wird es direkt aus dem Auswahlprozess ausgeschlossen. In der zweiten Phase wird eine Anforderungserhebung gemacht, bei der Anforderungen für wichtige Funktionalitäten definiert und ein Bewertungsschema zur Beurteilung der Anforderungserfüllung

entwickelt werden (Kapitel 4.4). In der dritten Phase werden die Tools, die aus der ersten Phase hervorgegangen sind, dann anhand der Liste von Anforderungen mit Hilfe des erarbeiteten Schemas bewertet (Kapitel 4.5). Das Tool, das bezüglich der Erfüllung der Anforderungen bei der Bewertung am besten abschneidet, wird dann zur Umsetzung der Ontologie verwendet.

4.3 Erste Phase: Vorauswahl

Um die Anzahl der 269 Tools auf ein angemessenes Maß zu reduzieren, wird in der ersten Phase eine Vorauswahl anhand von K.O.-Kriterien getroffen. Diese Kriterien müssen von jedem Tool erfüllt werden. Ist dies nicht der Fall, so ist das Tool nicht geeignet für das weitere Vorgehen. Die Vorauswahl ist nötig, um eine bessere Bewertung der Tools nach spezifischeren Anforderungen zu ermöglichen.

In der nachfolgenden Beschreibung der Kriterien wird als erstes die grundsätzliche Fragestellung des Kriteriums aufgestellt. Dann folgt eine Erläuterung des Kriteriums und dessen Rechtfertigung.
Die Kriterien, die in der erste Phase betrachtet werden, sind:

- **Kosten des Tools**
  Frage: Ist das Tool als Open Source-Variante oder Freeware verfügbar oder handelt es sich um ein rein kommerzielles Werkzeug durch das Lizenzgebühren entstehen?
  Erläuterung: Durch die Beschränkung der zur Verfügung stehenden Ressourcen muss für diese Diplomarbeit der Einsatz eines frei verfügbaren Tools ausreichen. Die Tools, die nur als kommerzielle Produkte verfügbar sind, werden daher ausgeschlossen.

- **Funktionalität**
  Frage: Liegt der Fokus auf der Unterstützung bei der Erstellung und Entwicklung von Ontologien?
  Erläuterung: Die Tools sind, wie in Abschnitt 4.1 bereits erwähnt, teilweise nur auf bestimmte Funktionalitäten ausgelegt wie z.B. das Zusammenfügen von Ontologien, die Extrahierung von Ontologien aus Dokumenten, die grafische Darstellung von Ontologien oder die Konvertierung von Formaten. Das gesuchte Tool muss in erster Linie in der Lage sein die Erstellung und Entwicklung einer solchen Ontologie zu unterstützen. Hat das Tool diese Funktionalität nicht oder nur eingeschränkt, dann wird es ausgeschlossen.

- **Ontologiesprache**
  Frage: Können die Ontologien in gängigen Standardsprachen erstellt, gespeichert, importiert und exportiert werden?
  Erläuterung: Die Tools verwenden zum Speichern der Ontologien oft unterschiedliche Formate. Es gibt, wie in Kapitel 2.2.3 vorgestellt, etliche Sprachen und Formate, in denen Ontologien formuliert und gespeichert werden können. Das gewünschte Tool muss in der Lage sein mindestens zwei der gängigen Standardsprachen (RDF(S), OWL, etc.) zu unterstützen, sonst wird es an dieser Stelle ausgeschlossen. Mit der Verwendung von Standards kann die Portabilität der erstellten Ontologien gewährleistet werden.

Tools	Open Source	Funktionalität	Sprache	Aktualität/Reife
Amine	ja	Systementwicklung	XML, OWL	Oktober 2010, Version 7
Hozo	ja	Ontologieentwicklung	RDF, OWL, XML-DTD	August 2011, Version 5.2.35
NeOn Toolkit	ja (Basisversion)	Ontologieentwicklung	OWL2, RDF(S), FLogic	April 2011, Version 2.5
Protégé	ja	Ontologieentwicklung	RDF, OWL, XML Schema	Juli 2011, Version 4.1

Abbildung 4.1: Die vier Tools nach der Vorauswahl

- **Aktualität/Reife**
  Frage: Wann wurde die letzte Version des Tools veröffentlicht und was ist der Status des Projekts?
  Erläuterung: Die Tools entstehen aus den verschiedensten Projekten. Das kann bedeuten, dass bei Projekten, die zeitlich begrenzt sind, nach Ablauf des Projektes eine Weiterentwicklung, Benutzersupport oder Fehlerbehebung nicht mehr stattfinden oder das Tool nicht weiter verfügbar ist. Deswegen werden Tools, die in den letzten zwei bis drei Jahren nicht mehr weiterentwickelt wurden oder sich noch in zu frühen Entwicklungsphasen befinden, ausgeschlossen.

- **Verfügbarkeit des Tools**
  Frage: Ist das Tool nur als Webversion verfügbar oder als eigenständiges Programm?
  Erläuterung: Einige Tools stellen ihre Funktionalität ausschließlich über Webbrowser zur Verfügung. Dadurch besteht eine gewisse Abhängigkeit, welche selbst nicht beeinflussbar ist. Die Tools, die nicht als eigenständiges Programm verfügbar sind, sondern nur webbasiert zugänglich sind, werden ausgeschlossen.

Die Bewertung der Tools basiert auf Informationen der entsprechenden Webseiten der Tools und Informationen von [Cas08] und [NCY]. Dabei wurden bereits einige Tools aus der Auswahl ausgeschlossen, weil sie nicht mehr verfügbar waren. Wenn ein Tool eines der Kriterien nicht erfüllte, so wurde es direkt aus der Auswahl ausgeschlossen.
Von der Ausgangsbasis von 269 Tools verblieben nach der Bewertung anhand der fünf K.O.-Kriterien nur noch vier Tools. Diese sind in Abbildung 4.1 mit ihren Resultaten bezüglich der ersten vier Kriterien aufgeführt. Für das fünfte Kriterium erfüllen alle vier Tools die Anforderung eigenständige Programme zu sein.

4.4 Zweite Phase: Anforderungserhebung und Bewertungsschema

In der zweiten Phase werden nun die Anforderungen definiert, die an das Tool gestellt werden und nach denen die Bewertung der vier verbliebenen Tools fortgeführt wird. Diese Anforderungen beziehen sich vor allem auf hilfreiche Funktionalitäten und Benutzerfreundlichkeit.

4.4.1 Bewertungsschema für die Anforderungen

Es werden dabei zwei Kategorien von Anforderungen unterschieden. Die eine Kategorie sind die Ja/Nein-Anforderungen. Dies sind Anforderungen, die nur danach bewertet werden, ob die Anforderung erfüllt wird oder nicht. Dabei geht es darum, ob eine bestimmte Funktionalität oder eine bestimmte Eigenschaft bei dem Tool vorhanden ist. Die Bewertungsfunktion f für die Ja/Nein-Anforderungen ist wie folgt definiert:

Für jede Anforderung x_i aus der Menge der Ja/Nein-Anforderungen
X = $\{x_1, ..., x_n\}$ gilt:

$$f(x_i) = \begin{cases} 0, & \text{wenn } x_i \text{ nicht erfüllt wird,} \\ 1, & \text{wenn } x_i \text{ erfüllt wird.} \end{cases}$$

Die andere Kategorie der Anforderungen sind qualitativ bewertete Anforderungen. Bei diesen Anforderungen wird bei der Bewertung bezüglich dem Grad der Erfüllung der Anforderung differenziert. Es wird unterschieden, ob eine Anforderung aus subjektiver Perspektive lediglich erfüllt wird oder ob sie besonders gut erfüllt wird. Für diese Anforderungen gibt es deshalb eine erweiterte Bewertungsfunktion h. Die Funktion wird wie folgt definiert:

Für jede Anforderung y_k aus der Menge der qualitativ bewerteten Anforderungen
Y = $\{y_1, ..., y_m\}$ gilt:

$$h(y_k) = \begin{cases} 0, & \text{wenn } y_k \text{ nicht erfüllt wird,} \\ 1, & \text{wenn } y_k \text{ nur erfüllt wird,} \\ 2, & \text{wenn } y_k \text{ sehr gut erfüllt wird.} \end{cases}$$

Da es einige Anforderungen gibt, die als wichtiger betrachtet werden als andere, werden diese Anforderungen zusätzlich mit einem Wert gewichtet. Die Gewichtungsfunktion g sieht wie folgt aus:

Für jede Anforderungen z_j aus der Menge aller Anforderungen
Z = $\{z_1, ..., z_{n+m}\}$ gilt:

$$g(z_j) = \begin{cases} 2, & \text{wenn } z_j \text{ eine wichtige Anforderung ist,} \\ 1, & \text{sonst.} \end{cases}$$

Für die Bewertung der Tools wird die Summe über die erzielten und gewichteten Werte der Erfüllung der Anforderungen berechnet. Das Tool mit dem höchsten Wert wird für die Umsetzung der Ontologie ausgewählt. Die Summe für jedes Tool berechnet sich wie folgt:

$$\sum_{j=1}^{n+m} g(z_j) * z_j$$

4.4.2 Beschreibung der Anforderungen

Die Beschreibung der Anforderungen orientiert sich an der Struktur der Kriterien aus Abschnitt 4.3 mit den relevanten Fragen und der Erläuterung der Anforderung. Dadurch soll verdeutlicht werden, was diese Anforderung fordert und warum sie wichtig für die Bewertung der Tools ist. Bei einigen Anforderungen wurde zudem eine zusätzliche Unterteilung in zwei weitere Anforderungen vorgenommen, um so unterschiedliche Aspekte der Anforderung präziser bewerten zu können.

- **Sprache**
  - **Mehrsprachenunterstützung**
    Frage: Über welche Menüsprache verfügt das Tool? Ist es in der Ontologie möglich die Sprache von Konzepten, Relationen, etc. anzugeben? Ist die sprachliche Umsetzung angemessen?
    Erläuterung: Als Standard für die Sprache wird Englisch angenommen. Bei der Bewertung geht es um die Verfügbarkeit eines englischen Menüs und die Umsetzung z.B. bezüglich der Fehlerfreiheit. Zusätzlich wird bewertet, ob es möglich ist für die verwendeten Begriffe in der Ontologie die Sprache anzugeben.
  - **Synonyme**
    Frage: Ist es möglich Synonyme von Konzepten anzugeben?
    Erläuterung: Zwei namentlich verschiedene Konzepte können unter Umständen dasselbe Objekt/Subjekt oder dieselbe Aktivität/Eigenschaft bezeichnen. Das kann in derselben Sprache sein oder der äquivalente Begriff in einer anderen Sprache. Bewertet wird hier, ob es grundsätzlich die Funktion gibt Synonyme anzugeben.

- **Formate**
  Frage: In welchen Formaten kann man die Ontologie speichern und in welche Formate kann man die Ontologie exportieren und importieren?
  Erläuterung: Diese Anforderung war bereits Kriterium der ersten Phase und wird nochmal in die Bewertung einbezogen. Die Möglichkeit der Auswahl aus verschiedenen Sprachen bietet Flexibilität bei der Wahl einer passenden Sprache in Bezug auf die Ausdrucksfähigkeit. Ein Tool, das aktuelle Standards umsetzt und sich an neue Standards anpasst, bietet zudem Potenzial für die Zukunft.

- **Dokumentation**
  Frage: Wie gut ist die Dokumentation zu dem Tool?
  Erläuterung: Dazu zählen Kriterien wie der Umfang der Dokumentation, die Aktualität, die Übersichtlichkeit und die Sprache (auch hier wird wieder Englisch als Standard angesetzt). Die Dokumentation des Tools ist wichtig für viele Bereiche. Sie wird bei der Bewertung selbst benutzt, ist wichtig für die Einarbeitung in das Tool (Tutorials können hilfreich sein) und bei der eigentlichen Arbeit mit dem Tool, wenn z.B. Probleme auftreten sollten. Besonderer Wert wird neben der allgemeinen Verständlichkeit auf die Qualität gelegt.

- **Support**
  Frage: In welcher Form und welchem Umfang kann man Unterstützung bei Problemen mit dem Tool erhalten?
  Erläuterung: Bewertet werden die Anzahl der Möglichkeiten Unterstützung zu kriegen sowie die Art der Unterstützung. Dabei wird insbesondere beachtet, welche Möglichkeiten der Meldung von Programmfehlern es gibt, ob aktive Mailinglisten oder Gemeinschaften vorhanden sind (soweit dies beurteilbar ist) und ob auf der Webseite des Tools Ansprechpartner angegeben werden.

- **Benutzerfreundlichkeit**
  - **Bedienung allgemein**
    Frage: Ist die Bedienung einfach oder schnell und intuitiv zu erlernen?
    Erläuterung: Bewertet werden die ersten Versuche bei der Handhabung und die persönliche Einschätzung sowie das benötigte Hintergrundwissen zur Benutzung. Zu dem Hintergrundwissen gehören das Wissen über bestimmte Ontologiesprachen und Theorien, die der Konzeption des Tools zugrunde liegen.
  - **Eingabe und Verwaltung von Ontologien**
    Frage: In welchen Formen können Ontologien erstellt werden? Werden mehrere Möglichkeiten angeboten? Wie können neue Elemente hinzugefügt werden? Gibt es Unterstützung, wenn viele ähnliche Elemente hinzugefügt werden sollen?
    Erläuterung: Eine Ontologie kann beliebig groß werden und vor allem bei den Instanzen der Regeln aus Kapitel 3.2.2 gibt es viele und ähnliche Elemente. Bewertet wird daher, ob für diesen Fall Unterstützung vorhanden ist und die Form, in der man Elemente hinzufügen kann (z.B. Baum, Graph, Text). Auch hier zählt der persönliche Eindruck bei der Handhabung.
- **Grafische Darstellung**
  - **Übersichtlichkeit**
    Frage: Kann in der grafischen Darstellung der Überblick behalten werden?
    Erläuterung: Bei großen Ontologien mit vielen Konzepten, Instanzen und Relationen kann diese schnell unübersichtlich werden. Eine optimierte Darstellung mit einer Filterfunktion kann hilfreich sein. So können die wesentlichen Teile der Ontologie trotzdem als grafische Darstellung angezeigt werden. Wenn hingegen schon bei kleinen Ontologien die grafische Darstellung eine unübersichtliche Form hat, so wirkt sich dies negativ auf die Bewertung aus.
  - **Zoom**
    Frage: Kann bei der grafischen Darstellung gezoomt werden?
    Erläuterung: Zur genaueren Analyse bestimmter Teilelemente sollte das Tool über eine Zoom-Möglichkeit verfügen, um Teile der Ontologie vergrößern zu können. Diese Funktionalität wird wichtiger, je größer die Ontologie ist.
- **Eingabeüberprüfung**
  - **Sprachliche Eingabeüberprüfung**
    Frage: Gibt es Einschränkungen, die bei der Eingabe von Konzepten, Instanzen und Relationen beachtet werden müssen? Findet überhaupt eine Überprüfung der Eingabe statt? Wie verhält sich das Tool bei der Eingabe von bereits vorhandenen Konzepten?
    Erläuterung: Eine generelle Eingabeüberprüfung ist wichtig, um schon frühzeitig Probleme verhindern zu können. Ein Schwerpunkt ist dabei die Konsistenz zwischen verschiedenen Tools. Wenn jedes Tool andere Konventionen hat, so kann diese Konsistenz nicht gewährleistet werden, wenn es um die Portabilität von Ontologien geht. Mögliche Konventionen, die eingehalten werden müssen, sind z.B. keine Leerzeichen in einem Konzept. Wenn ein Tool Leerzeichen erlaubt, so kann die Übertragung der Ontologie in eine anderes Tool zu Fehlern führen. Als Bewertungsmaßstab werden daher die elementaren Konventionen der

vier Tools mit Bezug zu der Modellierung aus Kapitel 3 zugrunde gelegt. Ein weiterer Aspekt bei der Eingabeüberprüfung ist der Umgang mit doppelt verwendeten Begriffen bei Konzepten. Diese sollen möglichst eindeutig bestimmte Objekte, etc. identifizieren. Es sollte daher bereits vom Tool verhindert werden, dass schon vorhandene Begriffe ein weiteres Mal in einem anderen Kontext eingegeben werden können.

  - **Validierung/Reasoning**
    Frage: Kann die ganze Ontologie auf ihre logische Konsistenz überprüft werden? Gibt es die Möglichkeit automatisch logisch folgern zu können?
    Erläuterung: Diese Funktion ist wichtig, um grobe logische Fehler im Aufbau der Ontologie zu vermeiden. Es sollte erkennbar sein, ob durch bestimmte Eingaben Inkonsistenzen innerhalb der Ontologie auftauchen, die eventuell zu ungewollten Folgerungen führen. Bei vielen Elementen mit wiederkehrenden Mustern kann durch das automatische logische Schlussfolgern ein Teil der Klassifizierung automatisch unterstützt werden.

- **Erweiterbarkeit**
  Frage: Gibt es Möglichkeiten die Grundfunktionalität des Tools bei Bedarf um weitere Funktionen in Form von z.B. *Plug-ins* zu erweitern?
  Erläuterung: Die Möglichkeit zur Erweiterung des Tools mit weiteren Funktionen ist wichtig, da so die Flexibilität steigt und bei Bedarf zusätzliche Funktionen hinzugefügt werden können. Gegebenenfalls können auch selbst *Plug-ins* entwickelt werden, die gewünschte Funktionen umsetzen.

- **Systemanforderungen**
  Frage: Welche Betriebssysteme werden unterstützt und welche sonstigen Anforderungen werden an das System gestellt (z.B. eine aktuelle Version von Java)?
  Erläuterung: Zur Nutzung des Tools ist es von Vorteil, wenn es flexibel auf verschiedenen Systemen einsetzbar ist. Sonstige Systemanforderungen schränken die Nutzung unter Umständen ebenfalls ein. Systemanforderungen, die allgemein als Standard betrachtet werden können wie z.B. Java, wirken sich nicht negativ auf die Bewertung aus.

- **Inverse Relationen**
  Frage: Kann zu einer Relation auch eine inverse Relation definiert werden?
  Erläuterung: Die Möglichkeit zur Angabe von inversen Relationen erleichtert es in beide Richtungen passende Elemente zu finden und deutlich zu machen, dass diese Relationen zueinander gehören.

- **Suche/Anfrage**
  Frage: Gibt es eine Suchfunktion? Können Anfragen an die Ontologie formuliert werden?
  Erläuterung: Zur optimalen Nutzung der Ontologie sollte es möglich sein durch eine Suchfunktion und einen Anfragemechanismus relevante Inhalte in einem bestimmten Kontext zu erhalten.

- **Relationen zwischen Instanzen**
  Frage: Ist es möglich Relationen zwischen Instanzen von Konzepten zu definieren?
  Erläuterung: Für die Ontologie aus Kapitel 3 und insbesondere die Modellierung der Relationen zwischen den einzelnen Regeln und Regelwerken sollte es möglich sein diese Relationen in dem Tool umsetzen zu können.

Qualitativ bewertete Anforderungen
Mehrsprachenunterstützung
Formate
Dokumentation
Support
Bedienung allgemein
Eingabe und Verwaltung von Ontologien
Übersichtlichkeit
Sprachliche Eingabeüberprüfung
Systemanforderungen
Suche/Anfrage

Ja/Nein-Anforderungen
Synonyme
Zoom
Validierung/Reasoning
Erweiterbarkeit
Inverse Relationen
Relationen zwischen Instanzen

Abbildung 4.2: Übersicht über die Anforderungen

4.4.3 Einordnung der Anforderungen

Die im vorherigen Abschnitt vorgestellten Anforderungen müssen nun noch in die Kategorien einsortiert werden. Die Übersicht in Abbildung 4.2 zeigt in der linken Aufzählung die Kategorie mit den qualitativ bewerteten Anforderungen und in der rechten Aufzählung die Kategorie mit den Ja-/Nein-Anforderungen.
Von den aufgestellten Anforderungen werden fünf als besonders wichtig eingestuft und erhalten daher in der Bewertung eine besondere Gewichtung. In Abbildung 4.3 sind diese fünf Anforderungen aufgelistet.
Die Anforderungen *Dokumentation* und *Benutzerfreundlichkeit* werden als wichtig eingestuft, da sie für die Einarbeitung in das Tool und die Arbeit mit dem Tool und der Ontologie von besonderer Bedeutung sind. Die *Erweiterbarkeit* ist, wie die beiden vorherigen Anforderungen, eine wichtige Eigenschaft im allgemeinen Umgang mit dem Tool. So kann die Möglichkeit gegeben werden nützliche Funktionen bei Bedarf hinzufügen zu können. Die *inversen Relationen* und die Funktionen *Suche* und *Anfrage* sind besonders wichtig mit Blick auf die in Kapitel 3 modellierte Ontologie. Diese beiden Anforderungen sind vor allem wichtig, um aus der Ontologie die Informationen erhalten zu können, für die diese entwickelt wurde.
Im nächsten Abschnitt soll nun die Bewertung der vier Tools bezüglich ihrer Erfüllung der Anforderungen stattfinden.

Anforderungen
Dokumentation
Benutzerfreundlichkeit
Erweiterbarkeit
Inverse Relationen
Suche/Anfrage

Abbildung 4.3: Übersicht über die wichtigen Anforderungen

4.5 Dritte Phase: Toolauswahl

In diesem Abschnitt werden zu jedem Tool die wesentlichen Fakten zusammengestellt und eine Zusammenfassung der Bewertung gegeben. Die Fakten beziehen sich auf die folgenden Punkte:

- **Entwickler:** Wo und von wem wurde das Tool entwickelt?
- **Lizenz:** Unter welcher Lizenz wird das Tool zur Verfügung gestellt und welche Daten müssen gegebenenfalls beim Download angegeben werden?
- **Webseite:** Auf welcher Webseite sind das Tool und dazugehörige Informationen zu finden?
- **Systemanforderungen:** Auf welchen Betriebssystemen läuft das Tool und welche sonstigen Anforderungen werden an das System gestellt?
- **Zweck:** Für welchen Zweck wurde das Tool entwickelt?
- **Formate:** In welchen Formaten können Ontologien gespeichert, exportiert und importiert werden?

Die Bewertung der Anforderungen wird anhand der vorhandenen Dokumentation und der Installation der vier Tools inklusive dem Testen eines kleinen Beispiels vorgenommen. Das Beispiel besteht immer aus ein paar einfachen Konzepten und Instanzen (*Regelwerk*, *Gesetz*, *Standard*, *BDSG*, *ISO27001*, *BSI100-1*) sowie des Testens einer Relation. Für die Bewertung der Darstellung wird für jedes Tool dieses Beispiel sowie ein größeres Beispiel einer anderen Ontologie getestet. Die endgültige Bewertung der Tools wird in Abschnitt 4.5.2 zusammengefasst dargestellt.

4.5.1 Tools

Amine

- **Tool:** Amine Platform
- **Entwickler:** Master- und Doktorarbeit von Pr. Adil Kabbaj, ergänzt durch weitere Arbeiten
- **Lizenz:** Open Source (GNU Library/Lesser General Public License)
- **Version:** Amine 7 (veröffentlicht 14.3.2011)
- **Webseite:** http://amine-platform.sourceforge.net
- **Systemanforderungen:** Keine genauen Angaben, Java benötigt
- **Zweck:** Plattform zur Entwicklung von intelligenten Systemen/Multiagentensystemen (inklusive der Entwicklung von Ontologien und Wissensbasen)
- **Formate:** ont, XML, OWL

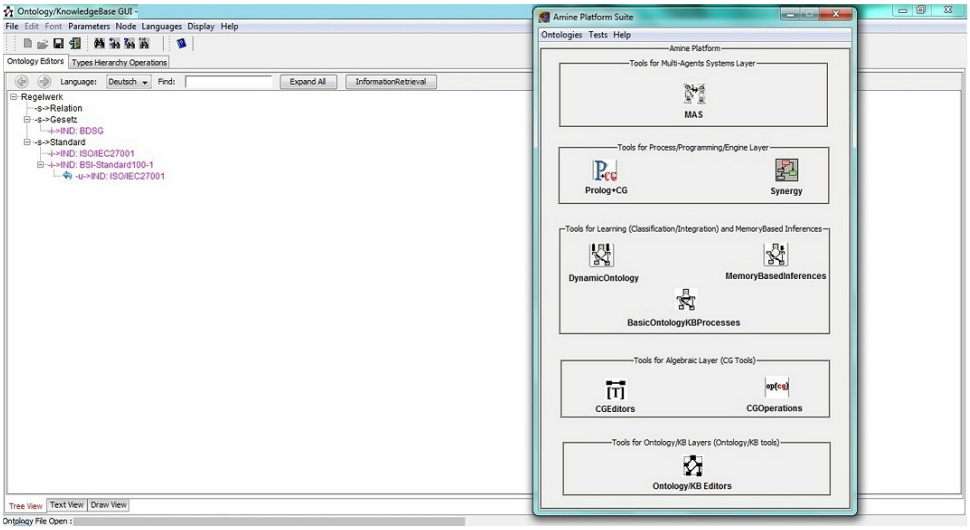

Abbildung 4.4: Amine Baumansicht

Zur Bewertung von Amine werden die Informationen auf der Webseite von Amine verwendet. Es lassen sich keine genauen Angaben finden, auf welchem System das Tool läuft. Da es sich bei Amine um eine Plattform zur Entwicklung von kompletten Wissenssystemen handelt, ist die Entwicklung von Ontologien nur eine Teilfunktion des Tools. Die Strukturen der Ontologien in Amine wurden so entwickelt, dass sie möglichst unabhängig von spezifischen Konstrukten einer Ontologiesprache sind. Deshalb ist es nötig sich in die konzeptionellen Grundlagen von Amine einzuarbeiten, um vernünftig mit dem Tool arbeiten und z.B. die Anfragemöglichkeit in Form von *Information Retrieval* bei Amine nutzen zu können. Das Tool bietet drei verschiedene Ansichten zur Anzeige und Erstellung oder Veränderung einer Ontologie. Diese sind eine einfache Textansicht, eine Baumansicht (Abbildung 4.4) und eine grafische Darstellung (Abbildung 4.5). Die Möglichkeit zur Definition von inversen Relationen und zur Erweiterbarkeit werden nicht explizit angeboten.

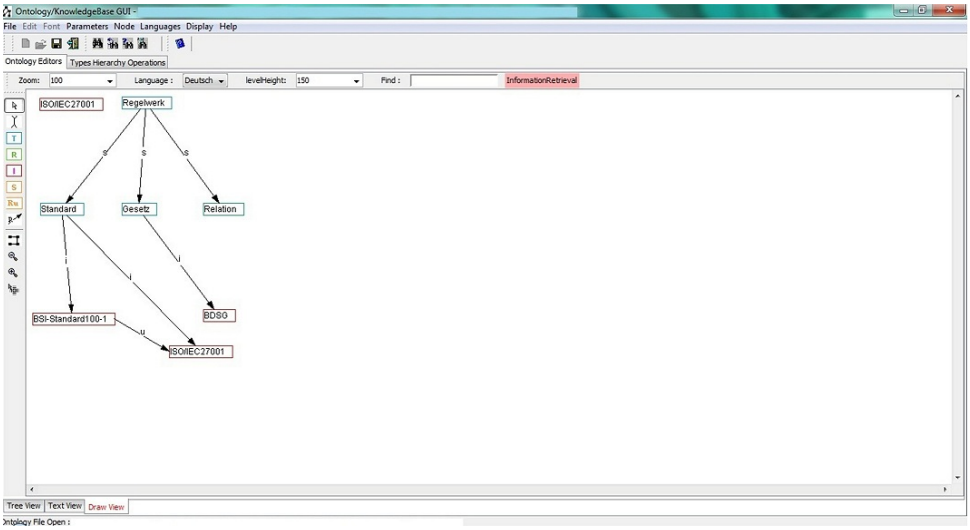

Abbildung 4.5: Amine Grafikansicht

Hozo

- **Tool:** Hozo
- **Entwickler:** The Institute of Scientific and Industrial Research, Osaka University
- **Lizenz:** Nach Registrierung (mit Name, E-Mail und Passwort) frei verfügbar
- **Version:** 5.2.35 (englische Version vom 5.8.2011)
- **Webseite:** http://www.hozo.jp
- **Systemanforderungen:** Windows 2000 oder höher, Mac OS X 10.4 oder höher, JRE/JDK 1.5.0_10 oder höher
- **Zweck:** Ontologie-Editor (Umgebung zur Entwicklung/Nutzung von Ontologien)
- **Formate:** ont, OWL, Text, XML-DTD, DAML+OIL, RDF(S)

Die Bewertung von *Hozo* basiert neben den Informationen auf der Webseite und dem Benutzerhandbuch auf den Artikeln [KKIM02] und [KSKM05]. In diesen wird das Rollenkonzept erläutert, auf dem das Tool aufbaut. Das erfordert eine vorherige Einarbeitung, um das Tool effektiv nutzen zu können. Hozo besteht aus vier Komponenten: Ontologie-Editor, Ontologie-Manager, *Onto-Studio* (spezielle methodische Unterstützung bei der Modellierung) und Ontologie-Server. Das Tool wurde ursprünglich nur in einer japanischen Version entwickelt, verfügt aber inzwischen auch über eine englische Übersetzung. Die Benutzeroberfläche weist allerdings etliche syntaktische Fehler bei der englischen Übersetzung auf. Die Dokumentation ist in Englisch verfügbar, aber nicht mehr aktuell und mit Grafiken aus der japanischen Version des Tools (mit japanischen Schriftzeichen). Neben der Vielzahl an möglichen Formaten für Ontologien, fällt besonders die übersichtliche grafische Darstellung der Ontologien positiv auf. Die Darstellung der Ontologie kann als Baum und als Grafik erfolgen, wobei beide Darstellungen das Einfügen von Elementen ermöglichen. Das Tool ist nicht durch *Plug-Ins* erweiterbar, macht keine Eingabeüberprüfung (doppelte Elemente sowie Leerzeichen und Sonderzeichen sind möglich) und hat auch keine Möglichkeit inverse Relationen anzugeben. Die Abbildung 4.6 zeigt eine Ansicht des Tools.

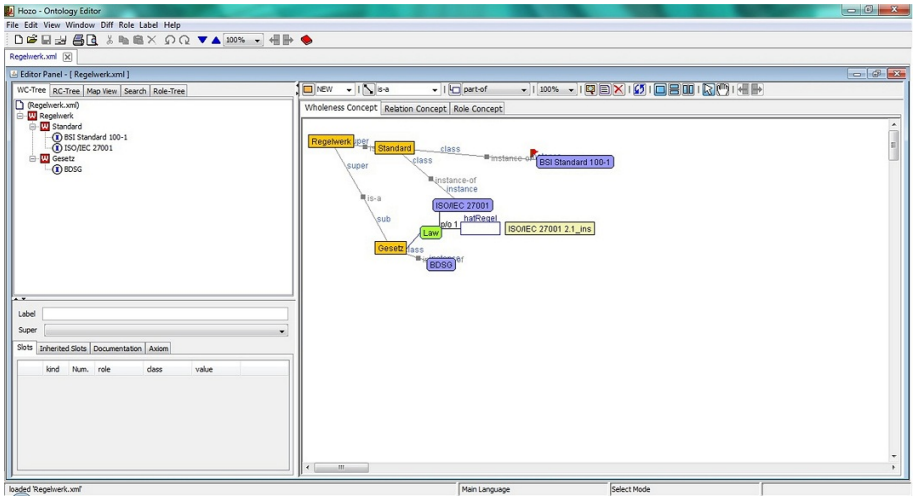

Abbildung 4.6: Hozo

NeOn Toolkit

- **Tool:** NeOn Toolkit
- **Entwickler:** NeOn Project (Projekt bestehend aus 14 europäischen Partnern (akademisch und industriell), Start: März 2006, Dauer: 4 Jahre)
- **Lizenz:**
  - *Basiskonfiguration:* Open Source (Eclipse Public License (EPL)), Angabe von Name, Organisation und E-Mail erforderlich
  - *Erweiterte Konfiguration:* Evaluation License (für 3 Monate) von *Ontoprise*
- **Version:** 2.5 (veröffentlicht am 15.4.2011), 32-Bit-Variante
- **Webseite:** http://neon-toolkit.org/wiki/
- **Systemanforderungen:** Windows 2000 oder höher, Linux, Mac OS X 10.5 oder höher; möglichst aktuellste Version von Java
- **Zweck:** Ontologie-Entwicklungsumgebung (Schwerpunkt: Große semantische Anwendungen in verteilten Organisationen)
- **Formate:** OWL2, FLogic, RDF(S)

Das *NeOn Toolkit* funktioniert mit den gängigen Betriebssystemen und verfügt über drei Versionen. Neben einer *Source-Code*-Version für Entwickler, gibt es zwei Konfigurationen für Endbenutzer, von denen nur die Basiskonfiguration frei verfügbar ist. Die Versionen sind durch *Plug-Ins* erweiterbar, wobei die erweiterte Konfiguration zusätzlich die Nutzung kommerzieller *Plug-Ins* einiger Projektteilnehmer erlaubt. Die Oberfläche des NeOn Toolkit baut auf der Oberfläche von *Eclipse* auf. Das Hinzufügen von Elementen ist nur in der Baumansicht möglich, das Reaktionsverhalten war dabei allerdings sehr träge. Die grafische Darstellung der Ontologie war bereits bei dem kleinen Beispiel unübersichtlich und schlecht zu navigieren. Die Abbildung 4.7 zeigt einen Ausschnitt aus dem Tool.

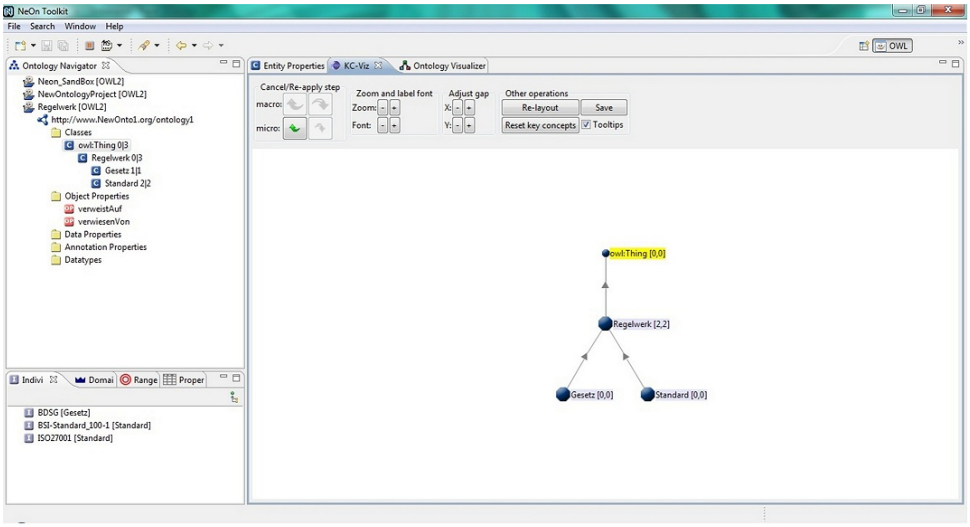

Abbildung 4.7: NeOn Toolkit

Protégé

- **Tool:** Protégé
- **Entwickler:** Stanford Center for Biomedical Informatics Research (Stanford University School of Medicine)
- **Lizenz:** Open Source (Mozilla Public License (MPL)), Registrierung mit Name und E-Mail
- **Version:** 3.4.7 (veröffentlicht: 15.7.2011), 4.1 (veröffentlicht: 26.7.2011)
- **Webseite:** http://protege.stanford.edu/
- **Systemanforderungen:** Windows, Unix, Mac OS X, mindestens JDK 1.5
- **Zweck:** Entwicklung, Visualisierung und Manipulation von Ontologien
- **Formate:** Standard Text Files (CLIPS), RDF(S), XML Schema, OWL (Version 3.4.7), OWL2 (Version 4.1), JDBC database

Protégé ist das meist benutzte Tool für Ontologien. Es unterstützt die gängigen Betriebssysteme und verfügt über eine umfangreiche Dokumentation sowie eine aktive *Community*. Seit Juli 2011 ist die Version 4.1 verfügbar. Da diese allerdings viele Funktionen noch nicht unterstützt (keine Unterstützung der Anfragesprache SPARQL; keine Unterstützung der Frames-Variante, nur OWL2), wird zur Bewertung die Version 3.4.7 benutzt, die ebenfalls im Juli 2011 erschienen ist. Protégé kann durch eine Vielzahl von *Plug-Ins*, um Funktionen erweitert werden. Die Benutzeroberfläche erfordert vor der Benutzung eine Einarbeitung in den Aufbau des Tools, was durch die umfangreiche Dokumentation erleichtert werden kann. Bei der Eingabe von Elementen gibt es Unterstützung durch sogenannte *Wizards*. Das Hinzufügen der Elemente erfolgt in der Baumdarstellung und kann durch die *Wizards* teilweise automatisiert gemacht werden. Durch *Plug-Ins* kann die Ontologie auch grafisch angezeigt werden (je nach Installationsauswahl sind *Plug-Ins* teilweise schon vorinstalliert). Abbildung 4.8 zeigt die grafische Darstellung des Beispiels mit dem *Plug-In Jambalaya*.

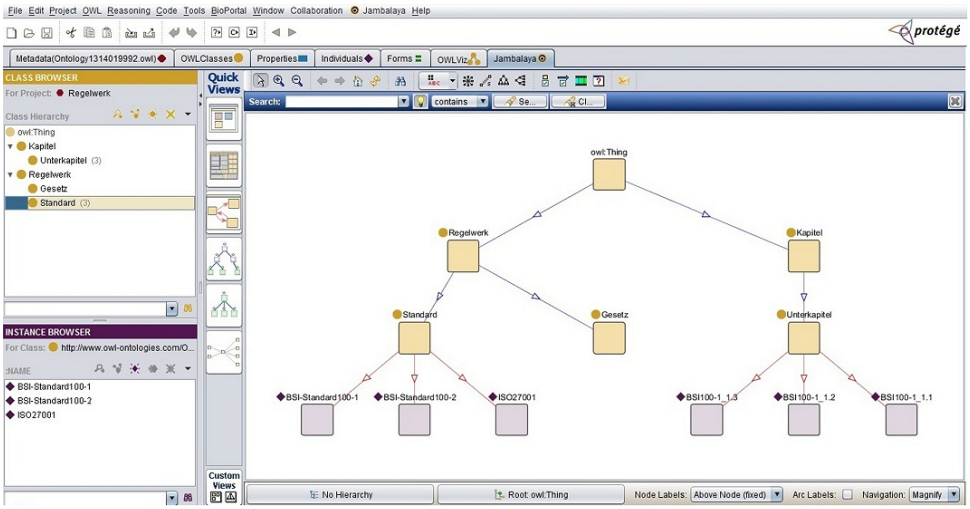

Abbildung 4.8: Protégé mit Plugin Jambalaya

Kriterien/Tools	Amine	Hozo	NeOn	Protégé	Art	Gewichtung
Sprache						
- Mehrsprachenunterstützung	2	1	2	2		
- Synonyme	1	1	1	1	J/N	
Formate	1	2	2	2		
Dokumentation	1 (2)	1 (2)	1 (2)	2 (4)		x2
Support	1	1	2	2		
Benutzerfreundlichkeit	(4)	(4)	(4)	(6)		x2
- Bedienung allgemein	1	1	1	1		
- Eingabe/Verwaltung	1	1	1	2		
Grafische Darstellung						
- Übersichtlichkeit	2	2	1	2		
- Zoom	1	1	1	1	J/N	
Eingabeüberprüfung						
- Sprache	2	1	1	2		
- Validierung/Reasoning	1	1	1	1	J/N	
Erweiterbarkeit	0 (0)	0 (0)	1 (2)	1 (2)	J/N	x2
Systemanforderungen	1	1	2	2		
Inverse Relationen	0 (0)	0 (0)	1 (2)	1 (2)	J/N	x2
Suche/Anfrage	2 (4)	1 (2)	2 (4)	2 (4)		x2
Relationen zwischen Instanzen	1	0	1	1	J/N	
Gesamt	23	19	28	34		

Abbildung 4.9: Bewertung der Tools

4.5.2 Bewertung

Nach der Vorstellung der Tools und erster Eindrücke bezüglich der Anforderungen werden diese bewertet. Die Tabelle in Abbildung 4.9 zeigt die Bewertung der vier Tools anhand der vorher definierten Anforderungen. Zur besseren Übersicht ist in der vorletzten Spalte nochmal angegeben, wenn es sich bei der Anforderung um eine Ja/Nein-Anforderung handelt. Die restlichen Anforderungen gehören zu den qualitativ bewerteten Anforderungen. Die letzte Spalte kennzeichnet die Anforderungen, die als besonders wichtig eingestuft wurden und daher doppelt gewichtet werden. Die Werte in Klammern sind die gewichteten Werte, die anstelle der einfachen Wertung in die Bewertung mit einfließen.
Die größte Summe erzielt das Tool Protégé und wird daher zur Modellierung der Ontologie benutzt.

4.6 Protégé

Aus der Entscheidung für das Tool *Protégé* ergeben sich weitere Entscheidungen, die vor der Umsetzung der Ontologie getroffen werden müssen. Im Rahmen der Toolbewertung wurde bereits entschieden, dass die Version 3.4.7 benutzt wird, da die aktuellere Version 4.1 sich noch in der Entwicklung befindet und deswegen einige Funktionen der älteren Version nicht anbietet. Die weiteren Entscheidungen mussten über die Variante und die Ontologiesprache getroffen werden.

4.6.1 Variantenauswahl

Protégé ist in zwei Varianten verfügbar: der Protégé-Frames-Editor und der Protégé-OWL-Editor[1]. Die beiden Varianten haben in Protégé unterschiedliche Benutzeroberflächen und arbeiten mit unterschiedlichen Begrifflichkeiten.

Der Protégé-Frames-Editor ist Frame-basiert und orientiert sich an der Spezifikation des *Open Knowledge Base Connectivity Protocol (OKBC)*[2]. Eine Frame-basierte Ontologie besteht aus:

- einer Menge von Klassen, die in einer Hierarchie eingeordnet sind und die Konzepte einer Domäne repräsentieren,
- einer Menge von *Slots* und
- einer Menge von Instanzen dieser Klassen.

Slots sind mit den Klassen verbunden und beschreiben deren Eigenschaften und Beziehungen. Die Instanzen sind individuelle Objekte der Konzepte und haben Werte bezüglich der Eigenschaften. Das Konzept der Repräsentation ist objekt-orientiert ([Neb99]). Im Protégé-Frames-Editor lassen sich die Ontologien in den Formaten RDF, XML oder HTML speichern.

Der Protégé-OWL-Editor ist für Ontologien im *Semantic Web* gedacht. Im OWL-Editor werden Ontologien durch die Beschreibung von Klassen, *Properties* und Instanzen der Klassen dargestellt. Durch die formale Semantik von OWL, die an Beschreibungslogiken orientiert ist, wird spezifiziert wie logisch gefolgert werden kann. Der Protégé-OWL-Editor ermöglicht Ontologien in RDF und OWL.

In [WNR+06] werden die Unterschiede zwischen Protégé-Frames und Protégé-OWL anhand mehrerer Kriterien aufgezeigt. Die ausschlaggebenden Kriterien in diesem Fall sind:

- *Closed World Assumption - Open World Assumption*:
  In Protégé-Frames wird von einer abgeschlossenen Welt ausgegangen, d.h. alles ist verboten bis es explizit erlaubt ist. In Protégé-OWL gilt die Annahme der offenen Welt, wo alles erlaubt ist, solange es nicht verboten ist.

- *Assertion - Classification*:
  In Protégé-Frames können nur notwendige Bedingungen angegeben werden, die für alle Instanzen einer Klasse gelten. In Protégé-OWL können ebenfalls notwendige Bedingungen definiert werden, zudem gibt es noch die Möglichkeit notwendige und hinreichende Bedingungen zu definieren. Anhand derer ist es möglich Elemente einer Klasse zu identifizieren, wodurch andere Möglichkeiten für Folgerungen geboten werden.

- *Constraint checking - Consistency checking*:
  In Protégé-OWL ist es durch einen *Reasoner* möglich einer Instanz neue Typen zuzuweisen, in Protégé-Frames ist dies nicht möglich.

[1] http://protege.stanford.edu/
[2] http://www.ai.sri.com/~okbc/

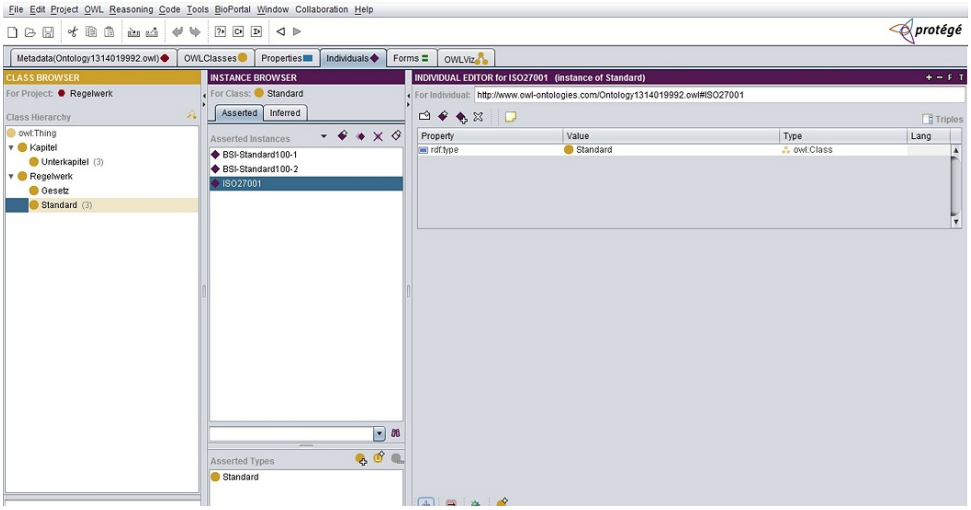

Abbildung 4.10: Oberfläche von Protégé-OWL

- *Slots - Properties*:
  In Protégé-Frames muss ein *Slot* erst zu einer Klasse hinzugefügt werden, bevor *Slot*-Werte zu Instanzen der Klasse hinzugefügt werden können. In Protégé-OWL können *Properties* mit jeder Klasse oder Instanz benutzt werden, solange der Bereich der *Property* nicht explizit eingeschränkt wird (*Open World Assumption*).
  Die *Properties* in Protégé-OWL können zudem die Eigenschaft der Transitivität besitzen.

Die größere Flexibilität und die Möglichkeiten der *Properties* in Protégé-OWL sind die Vorteile, die dazu führen, dass Protégé-OWL für die Umsetzung der Ontologiemodellierung gewählt wird. Abbildung 4.10 zeigt die Benutzeroberfläche von Protégé-OWL.

4.6.2 Sprachenauswahl

Durch die Entscheidung für Protégé-OWL muss vor der Umsetzung der Ontologie auch eine Wahl für eine der OWL-Varianten getroffen werden. OWL hat drei Untersprachen: *OWL Lite*, *OWL DL* und *OWL Full* (Übersicht in [MVH+04]). OWL besteht aus einer Menge von logischen Konstrukten, die zur Beschreibung der Ontologie verwendet werden können. Die Sprachen unterscheiden sich durch die Anzahl der Konstrukte, die verwendet werden können, sowie den Einschränkungen bezüglich dieser Konstrukte.
OWL Lite verwendet nur eine kleine Auswahl an Sprachfunktionalitäten von OWL. Daher eignet sich *OWL Lite* nur für einfache Klassifikationshierarchien.
OWL DL enthält alle OWL-Sprachkonstrukte, die aber nur unter bestimmten Bedingungen und mit Einschränkungen genutzt werden können. Dadurch bietet *OWL DL* eine relativ hohe Ausdrucksfähigkeit und bleibt maschinell berechen- und entscheidbar.
OWL Full enthält ebenfalls alle Sprachkonstrukte, aber schränkt diese nicht ein, so dass viele syntaktische Möglichkeiten vorhanden und z.B. Meta-Modelle möglich sind. Deswegen gibt es aber keine Garantien bezüglich der Berechenbarkeit.
OWL Lite ist aufgrund der starken Beschränkungen der Ausdrucksfähigkeit eher weniger geeignet zur Darstellung der Ontologie und wird deswegen nicht benutzt. Für die Ontologie wird die Ausdrucksfähigkeit von *OWL DL* und *OWL Full* benötigt. Weil *OWL Full* keine Garantie der Berechenbarkeit hat, wird *OWL DL* als Sprache gewählt.

4.7 Zusammenfassung

In diesem Kapitel wurde in drei Phasen die Entscheidung über ein Tool zur Umsetzung der Ontologie getroffen. Zunächst wurde anhand von fünf K.O.-Kriterien eine Vorauswahl getroffen, um die Anzahl der Tools auf ein angemessenes Maß zu reduzieren. Dann wurden Anforderungen an ein Tool identifiziert und ein Bewertungsschema entwickelt. Anhand dieser Anforderungen wurden die vier, nach der Vorauswahl, verbliebenen Tools bewertet. Die Entscheidung fiel dabei auf *Protégé*. Als Variante wurde der *Protégé-OWL-Editor* gewählt und *OWL DL* als Untersprache für die Ontologie.

Kapitel 5

Umsetzung und Evaluierung

In diesem Kapitel wird im ersten Abschnitt auf Anpassungen der modellierten Ontologie in Protégé eingegangen. Im zweiten Abschnitt wird die Ontologie anhand verschiedener Beispielszenarien evaluiert. Dazu wird die Anfragesprache SPARQL benutzt, die vorher kurz vorgestellt wird.

5.1 Umsetzung der Ontologie in Protégé

In diesem Abschnitt werden Anmerkungen zu Besonderheiten der Umsetzung der Ontologie in Protégé gemacht, insbesondere zu Anpassungen bezüglich der Namensgebung.

5.1.1 Konventionen

Die Namen der Konzepte und Relationen werden ohne Umlaute und „ß“ dargestellt. Einer der Gründe ist die bessere Kompatibilität, um so Konflikte bei der Nutzung von anderen Programmen oder Systemen von vornherein auszuschließen. Ein weiterer Grund ist die Einschränkung von Protégé bei der Eingabe von Elementen, dass keine Umlaute als Anfangsbuchstabe zugelassen werden. Die umgewandelten Zeichen sind in Tabelle 5.1 dargestellt.

Eine weitere Anpassung ist nötig, da keine Leerzeichen in einem Konzept erlaubt sind. So werden Konzepte, die aus zwei Worten bestehen, zu einem Wort zusammengefügt. Zur besseren Abgrenzung fängt das zweite Wort mit einem Großbuchstaben an.

5.1.1 Beispiel (Leerzeichen).
Das Konzept *Natürliche Person* wird wegen des Umlauts und der zwei Wörter zu *NatuerlichePerson*.

Zeichen	Anpassung in Protégé
ä	ae
ö	oe
ü	ue
ß	ss

Tabelle 5.1: Umwandlung der Umlaute und „ß“

Regelwerk	Abkürzung	Beispiel für die Instanzen
Mindestanforderungen an das Risikomanagement (Versicherungen)	MaRiskVA	*MaRiskVA_Kap7, MaRiskVA_Kap7.2.2.2*
Bundesdatenschutzgesetz	BDSG	*BDSG_Abschnitt1, BDSG_Abschnitt2.2, BDSG_P14*
ISO/IEC 27001:2005	ISO27001	*ISO27001_Kap3, ISO27001_Kap4.2.2*
ISO/IEC 27002:2005	ISO27002	*ISO27002_Kap10, ISO27002_Kap10.1*
ISO/IEC 27005:2008	ISO27005	*ISO27005_Kap8, ISO27005_Kap8.2.1*
BSI IT-Grundschutz-Kataloge	BSIGrundschutz	*BSIGrundschutz_Kap3, BSIGrundschutz_B1.1, BSIGrundschutz_M2.2, BSIGrundschutz_G3.8*
BSI-Standard 100-1	BSI100-1	*BSI100-1_Kap2, BSI100-1_Kap2.1*
BSI-Standard 100-2	BSI100-2	*BSI100-2_Kap4.5, BSI100-2_Kap4.5.1*
BSI-Standard 100-3	BSI100-3	*BSI100-3_Kap2, BSI100-3_Kap2.3*
BSI-Standard 100-4	BSI100-4	*BSI100-4_Kap4, BSI100-4_Kap4.5*

Abbildung 5.1: Benennung der Instanzen der Regeln

Bei Instanzen der Regelelemente wird zur Trennung von mehreren Wörtern ein *Unterstrich* verwendet.

5.1.2 Beispiel (Mehrere Worte bei Instanzen).
Die Instanz *Windows Vista* wird in der Ontologie zu *Windows_ Vista*

Instanzen der Regeln

Für die Instanzen der Regeln gelten andere Konventionen bei der Benennung. Die Bezeichnung setzt sich aus den folgenden Elementen zusammen:

- Kürzel des entsprechenden Regelwerks (erste Spalte in Abbildung 5.1)
- *Unterstrich*
- Kürzel *Kap* bei Kapiteln oder *Abschnitt* bei Gesetzen
- Nummer der Regel

Für die Paragraphen des *Bundesdatenschutzgesetzes* und die Gefährdungen und Maßnahmen der *IT-Grundschutz-Kataloge* gilt eine Sonderregel:
Anstelle von *Kap* oder *Abschnitt* wird ein *P*, *G* oder *M* angehängt.
In Abbildung 5.1 sind die Abkürzungen der Regelwerke und Beispiele für die Benennung der Instanzen aufgeführt.

5.1.2 Relationen in Protégé

Relationen werden in Protégé als *Properties* bezeichnet. Es können damit auch Eigenschaften zu Konzepten und Instanzen hinzugefügt werden. Es gibt drei verschiedene Arten von *Properties* in Protégé:

- *Object Property*: Verbindungen zwischen Konzepten und Instanzen
- *Datatype Property*: Verbindungen von Konzepten/Instanzen mit einem Datentyp (z.B. Integer, Boolean)
- *Annotation Property*: Verbindungen von Konzepten/Instanzen/*Object Properties*/*Datatype Properties* mit Metadaten

Relation	Inverse Relation	Eigenschaft
hatTeilelement	istTeilelementVon	transitiv
istKomplementärZu	istKomplementärZu	symmetrisch
hatTeilprozess	istTeilprozessVon	transitiv
hatTeil	istEinTeilVon	transitiv

Abbildung 5.2: Relationen mit weiteren Eigenschaften

In der modellierten Ontologie werden nur die *Object Properties* für die Relationen benutzt. In diesem Kapitel wird weiterhin Relation als Bezeichnung für *Property* benutzt.
Neben den in Kapitel 3 selbst definierten Relationen, sind folgende Elemente aus der OWL-Spezifikation bei der Darstellung der Ontologie besonders wichtig:

- *rdfs:subClassOf*: Gibt das Konzept an, von der das Element das Unterkonzept ist.
- *rdfs:label*: Ermöglicht die Zuordnung eines Namens zu einem Element.
- *owl:inverseOf*: Gibt die inverse Relation einer Relation an.

Die Relationen in Protégé können noch weitere Merkmale haben, wobei die folgenden Merkmale für die selbst definierten Relationen wichtig sind (siehe auch [TT07]):

- Symmetrisch (*owl:SymmetricProperty*):
  Eine Relation R ist symmetrisch, wenn für alle $(a, b) \in R$ gilt, dass $(b, a) \in R$ ist.
- Transitiv (*owl:TransitiveProperty*):
  Eine Relation R ist transitiv, wenn für alle $(a, b) \in R$ und $(b, c) \in R$ gilt, dass auch $(a, c) \in R$ ist.

Abbildung 5.2 zeigt die Relationen aus Kapitel 3, denen diese Merkmale zugeordnet werden.

5.2 Evaluierung

In diesem Abschnitt soll die Ontologie anhand mehrerer Szenarien evaluiert werden. Dafür wird die Anfragesprache SPARQL benutzt. Die Szenarien werden kurz dargestellt, die entsprechenden Anfragen an die Ontologie in SPARQL formuliert und die Ergebnisse der Anfragen aufgezeigt. Da die Anfragen oft ähnlich sind und die Ergebnisse viel Platz einnehmen, sind der Großteil der Anfragen und die Ergebnisse im Anhang zu finden.
Es soll gezeigt werden, dass die Ontologie für bestimmte Begriffe oder bestimmte Regeln relevante Regeln oder Regelwerke liefern kann.

5.2.1 SPARQL

SPARQL ist eine Anfragesprache, die vom *W3C*[1] als Standard für RDF-Ontologien entwickelt wurde. Da jedes OWL-Dokument ein RDF-Dokument ist (siehe [MVH+04]), kann SPARQL auch für OWL-Ontologien genutzt werden. Protégé bietet eine integrierte Möglichkeit Anfragen mit SPARQL an die Ontologie zu stellen. Die Ergebnisse werden in Protégé in Form von Tabellen angezeigt. Ein Tutorial zur Einführung in SPARQL findet sich in [Dod05].

[1] http://www.w3.org/

Die Syntax der SPARQL-Anfragen ist grundsätzlich der Syntax von SQL-Anfragen ähnlich. Die Anfragen werden aus einer *SELECT*-, einer *FROM*- und einer *WHERE*-Anweisung zusammengesetzt. Die *FROM*-Anweisung zur Angabe der Quelle der Ontologie kann in Protégé weggelassen werden, weil automatisch die geöffnete Ontologie als Quelle identifiziert wird. Die *SELECT*-Anweisung gibt an, welche Anfrageelemente in der Ergebnistabelle dargestellt werden sollen. Die Elemente der *WHERE*-Anweisung bestehen aus Tripeln der Form:

Subjekt Relation Objekt.

Für die Elemente der Tripel können entweder Werte oder Variablen angegeben werden.

5.2.1 Beispiel (Werte).
Bei einem Tripel mit konkreten Werten wird vor die Werte ein Doppelpunkt gesetzt, so dass das Tripel folgendermaßen aussehen würde:

:Subjekt :Relation :Objekt

5.2.2 Beispiel (Variablen).
Die Variante mit Variablen enthält anstelle des Doppelpunktes ein Fragezeichen, wird also so dargestellt:

?Subjekt ?Relation ?Objekt

Werte und Variablen können in den Tripeln beliebig kombiniert werden.
Neben diesen Grundelementen einer Anfrage, bietet SPARQL noch weitere Konstrukte für den Aufbau einer Anfrage. An dieser Stelle werden die Elemente vorgestellt, die später auch in den Beispielszenarien verwendet werden.

- *UNION*:
  Dieses Element vereinigt zwei Mengen. Die Mengen können aus ein oder mehr Tripeln bestehen.

- *OPTIONAL*:
  Optionale Argumente werden in der Ergebnistabelle angezeigt, wenn ein Tripel der darin angegebenen Form existiert. Dieses Konstrukt ist wichtig, da es bei der Kombination von zwei oder mehr Bedingungen passieren kann, dass für eine der Bedingungen ein Element die Bedingung nicht vollständig erfüllt, weil kein Wert angegeben wurde. Das Element würde daraufhin gar nicht im Ergebnis angezeigt werden, weil es die Anfrage nicht erfüllt. Unter Umständen ist gewollt, dass das Ergebnis trotzdem angezeigt wird, weil die Bedingung nicht entscheidendes Kriterium sein soll. Diese Bedingungen können deshalb mit dem *OPTIONAL*-Argument versehen werden, um das Filtern der Ergebnisse zu verhindern.

- *ORDER BY*:
  Mit diesem Argument können die Ergebnisse nach einem angegebenem Kriterium geordnet werden.

5.2.3 Beispiel (*OPTIONAL*).
Es sollen ausgehend von *Regel1* die Regeln angezeigt werden, die in einer bestimmten *Relation* zu dieser *Regel1* stehen. Zu diesen Regeln soll auch der *Name* der Regeln angegeben werden. Die *WHERE*-Anweisung sieht folgendermaßen aus:

:Regel1 :Relation ?Regeln.
?Regeln :hatName :Name.

Sollte für eine der Regeln, die durch die *Relation* gefunden werden, kein *Name* angegeben worden sein, so würde diese Regel nicht im Ergebnis angezeigt werden, weil der Wert fehlt. Wird das zweite Tripel allerdings in eine *OPTIONAL*-Anweisung gesetzt, dann würde diese Regel trotzdem angezeigt.

SPARQL ist in der Form, wie es in Protégé zur Verfügung gestellt wird, limitiert:

- SPARQL kann mit der Semantik der transitiven *Properties* nicht automatisch umgehen und
- das Ergebnis einer Anfrage kann nicht einfach gespeichert und weiterverarbeitet werden.

Protégé bietet aber eine API, über die andere *Reasoner* genutzt werden können, mit denen diese Probleme gelöst werden können. Für die Evaluierung der Ontologie ist SPARQL aber an dieser Stelle ausreichend.

5.2.2 Beispielszenario 1: Vertraulichkeit

Beschreibung

Ausgangspunkt für dieses Szenario ist die Eigenschaft *Vertraulichkeit*. Es sollen Regeln gefunden werden, die für *Vertraulichkeit* wichtig sind. Es stellen sich z.B. folgende Fragen:

- Was ist *Vertraulichkeit*?
- Was kann die *Vertraulichkeit* gefährden und welche Maßnahmen helfen *Vertraulichkeit* sicherzustellen?
- In welchen Regeln ist *Vertraulichkeit* relevant?

Anfragen

Für den ersten Schritt wird angenommen, dass nach einer Definition von *Vertraulichkeit* gesucht wird. Folgende Frage soll beantwortet werden:

- In welchen Regeln kann eine Definition von *Vertraulichkeit* gefunden werden?

Die Anfrage für diese Frage sieht folgendermaßen aus:

```
SELECT   ?Regel ?Name
WHERE    { :Vertraulichkeit :istDefiniertIn ?Regel.
           OPTIONAL { ?Regel rdfs:label ?Name.}}
```

Regel	Name
ISO27001_Kap3	Terms and definitions
BSIGrundschutz_Kap4	Glossar

Tabelle 5.2: Regeln mit Definition für Vertraulichkeit

Das Ergebnis der Anfrage befindet sich in Tabelle 5.2. Es wurden zwei Regeln gefunden, die eine Definition für *Vertraulichkeit* enthalten.

Im nächsten Schritt geht es um die Frage:

- Welche Gefährdungen gibt es für *Vertraulichkeit*?

Die Anfrage und die Tabelle mit dem Ergebnis befinden sich im Anhang A.1.1 und in den Tabellen A.1 und A.2.

Die Gefährdungen führen zu der nächsten Frage:

- Welche Maßnahmen gibt es, die helfen können *Vertraulichkeit* zu gewährleisten?

Die Anfrage und die Ergebnisse befinden sich in Anhang A.1.2 und der Tabelle A.3.

Nachdem bereits Gefährdungen und Maßnahmen für *Vertraulichkeit* gefunden wurden, stellt sich noch die Frage:

- Welche Regeln müssen generell bei Vertraulichkeit beachtet werden?

Dafür wird folgende Anfrage gestellt:

```
SELECT          ?Regel ?Name
WHERE           { :Vertraulichkeit :istEigenschaftIn ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}
ORDER BY ASC    (?Regel)
```

Das Ergebnis dieser Anfrage befindet sich in Tabelle 5.3.
Die Anfragen können grundsätzlich auch in einer Anfrage gestellt werden, indem statt der Namen der Relationen eine Variable benutzt wird oder die Anfrage aus den einzelnen Abfragen zusammengestellt und die Ergebnisse vereinigt werden.
Bisher wurden die Anfragen nur für *Vertraulichkeit* gestellt. Es ist auch möglich die Ergebnisse je nach Situation einzugrenzen, z.B. in Bezug auf bestimmte Objekte. Die folgende Anfrage liefert Regeln für *Vertraulichkeit* in Bezug auf *Daten*:

Regel	Name
BSI100-3_Kap4	Ermittlung zusätzlicher Gefährdungen
BSI100-4_Kap5.5.1	Feinkonzeption, Sicherheit und Kontrollen
BSIGrundschutz_B1.7	Kryptokonzept
MaRiskVA_Kap7.2.2.2	Betriebliche Anreizsysteme und Ressourcen

Tabelle 5.3: Regeln für Vertraulichkeit

```
SELECT          ?Regel ?Name
WHERE           { :Vertraulichkeit ?Relation ?Regel.
                  :Daten ?Relation ?Regel.
                  OPTIONAL { ?Regel rdfs:label ?Name.}}
ORDER BY ASC    (?Regel)
```

Regel	**Name**
BSIGrundschutz_G2.111	Kompromittierung von Anmeldedaten bei Dienstleisterwechsel
BSIGrundschutz_G2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
BSIGrundschutz_G2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
BSIGrundschutz_G3.1	Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
BSIGrundschutz_G5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten

Tabelle 5.4: Regeln für Vertraulichkeit bei Daten

Das Ergebnis in Tabelle 5.4 enthält fünf Gefährdungen. Das sind wesentlich weniger Gefährdungen als die Gefährdungen nur für *Vertraulichkeit* in den Tabellen A.1 und A.2. Wenn das Ziel ist nur die Regeln zu erhalten, die Vertraulichkeit in Bezug auf die Daten behandeln, dann kann diese Eingrenzung der Anfrage also helfen die relevanten Ergebnisse zu erhalten.
Bei der Eingrenzung der Ergebnisse durch Kombination von Elementen muss aufgepasst werden, dass Regeln gefiltert werden könnten, weil eines der Elemente nicht mit einer Regel assoziiert wurde. Bei der Benutzung der Vereinigung von mehreren Elementen in der Anfrage, können in der Ergebnismenge mehr Ergebnisse geliefert werden.

5.2.3 Beispielszenario 2: Risikomanagement

Beschreibung

Ein gemeinsames Thema der Regelwerke ist das *Risikomanagement*. In der Richtlinie *MaRiskVA* werden die allgemeinen Anforderungen an das *Risikomanagement* in Versicherungen behandelt. In den ISO- und BSI-Standards wird *Risikomanagement* auf dem Gebiet der Informationssicherheit als ein Teilelement behandelt.
In diesem Szenario soll im ersten Abschnitt gezeigt werden, wie Informationen über das *Risikomanagement* sowie Regeln für das *Risikomanagement* gefunden werden können. Im zweite Abschnitt wird gezeigt, wie ausgehend von einer bestimmten Regel weitere Regeln gefunden werden können.

Risikomanagement

Der erste Schritt beschäftigt sich mit der Klärung der Fragen:

- Was ist *Risikomanagement* und wo kann eine Definition für *Risikomanagement* gefunden werden?

Die Anfragen mit SPARQL sind folgende:

```
SELECT   ?Konzept
WHERE    { :Risikomanagement rdfs:subClassOf ?Konzept.}

SELECT   ?Regel
WHERE    { :Risikomanagement :istDefiniertIn ?Regel. }
```

Die Ergebnisse dieser Anfragen enthalten die Informationen, dass *Risikomanagement* ein *Prozess* ist und dass Definitionen für *Risikomanagement* in den Regeln *MaRiskVA_Kap1* und *MaRiskVA_Kap7* zu finden sind.
Die Anfrage nach Unterkonzepten von *Risikomanagement* liefert keine Ergebnisse. Da ein Prozess aus einzelnen Aktivitäten besteht, soll im nächsten Schritt herausgefunden werden, welche Teilprozesse zu dem Prozess *Risikomanagement* gehören und ob diese weitere Unterkonzepte haben. Dafür wird folgende Anfrage ausgeführt:

```
SELECT          ?Teilprozess ?Unterkonzept
WHERE           { :Risikomanagement :hatTeilprozess ?Teilprozess.
                OPTIONAL { ?Unterkonzept rdfs:subClassOf ?Teilprozess.}}
ORDER BY ASC    (?Teilprozess)
```

Das Ergebnis sind die Aktivitäten in Tabelle 5.5.

Nachdem die Teilprozesse des Risikomanagements bekannt sind, sollen im nächsten Schritt nun die Regeln für *Risikomanagement* und dessen Teilprozesse gefunden werden. Für Prozesse und Aktivitäten gibt es für die Verbindung zu Regeln und Regelwerken drei Relationen: *istAktivitaetIn*, *hatGefaehrdung* und *hatMassnahme*. Die Anfrage für Regeln im Zusammenhang mit dem *Risikomanagement* wird aus den einzelnen Tripeln mit diesen drei Relationen zusammengesetzt.

Teilprozess	**Unterkonzept**
AblauforganisationRisikomanagement	
AufbauorganisationRisikomanagement	
Risikoakzeptanz	
Risikoanalyse	
Risikobehandlung	Risikoannahme
Risikobehandlung	Risikoreduktion
Risikobehandlung	Risikotransfer
Risikobehandlung	Risikovermeidung
Risikobewertung	
Risikoidentifikation	
Risikokommunikation	
Risikoueberwachung	

Tabelle 5.5: Teilprozesse vom Prozess *Risikomanagement*

```
SELECT   ?Regel
WHERE    {{ :Risikomanagement :istAktivitaetIn ?Regel.}
         UNION {{ :Risikomanagement :hatGefaehrdung ?Regel.}
         UNION { :Risikomanagement :hatMassnahme ?Regel.}}}
```

Regel
MaRiskVA
ISO27005_Kap6

Tabelle 5.6: Regeln für *Risikomanagement*

Das Ergebnis ist in Tabelle 5.6 dargestellt und enthält ein Regelwerk (*MaRiskVA*) und eine Regel aus *ISO27005*.
Um Regeln für die Teilprozesse vom *Risikomanagement* und die Unterkonzepte der *Risikobehandlung* zu erhalten, werden noch zwei weitere Anfragen gestellt, die sich in Anhang A.2.1 (mit Tabellen A.4 und A.5) und A.2.2 (mit Tabelle A.6) befinden. Wenn Regeln mit mehreren Risikomanagement-Aktivitäten verbunden sind, so werden die Regeln bei dieser Anfrage für jede dieser Aktivitäten angezeigt und tauchen deswegen mehrmals in der Ergebnistabelle auf.

MaRisk VA - Kapitel 7

Kapitel 7 der MaRisk VA beschäftigt sich mit den Elementen des Risikomanagements. In diesem Szenario geht es um die Instanz *MaRiskVA_Kap7*. Die Frage ist, welche Regeln für diese Instanz beachtet werden müssen. In den Tabellen mit den Ergebnissen werden im Folgenden nur die wichtigen und für das weitere Vorgehen relevanten Ergebnisse dargestellt. Wichtige Ergebnisse bedeutet hier, dass es sich entweder um Beziehungen zu anderen Regeln handelt oder um den Namen der Regel.
Die erste Anfrage wird benutzt, um grundsätzliche Informationen über die Regel oder auch erste weiterführende Regeln zu erhalten. Dafür wird folgende Anfrage gestellt:

```
SELECT   ?Relation ?Objekt
WHERE    { :MaRiskVA_Kap7 ?Relation ?Objekt.}
```

An dem Ergebnis in Tabelle 5.7 kann erkannt werden, dass *MaRiskVA_Kap7* aus weiteren Teilelementen besteht. Der nächste Schritt besteht deshalb darin Regeln für diese

Relation	**Objekt**
hatTeilelement	MaRiskVA_Kap7.2
hatTeilelement	MaRiskVA_Kap7.1
hatTeilelement	MaRiskVA_Kap7.5
hatTeilelement	MaRiskVA_Kap7.4
hatTeilelement	MaRiskVA_Kap7.3
rdfs:label	Elemente eines angemessenen Risikomanagements

Tabelle 5.7: Teilelemente von *MaRiskVA_Kap7*

Teilelemente zu erhalten, die aufgrund der Teilmengenbeziehung auch für *MaRisk_Kap7* gelten. Außerdem können noch weitere Teilelemente existieren.
Die Anfrage befindet sich in Anhang A.2.3. In der Tabelle A.7 mit den Ergebnissen der Anfrage erfährt man neben der Information, dass es noch weitere Teilelemente gibt, auch die ersten Regeln. Dabei tauchen spezialisierende, verallgemeinernde und unterstützende Regeln auf.
Für die weiteren Teilelemente wird erneut eine Anfrage gestellt (siehe Anhang A.2.4). Im Ergebnis in Tabelle A.8 findet sich diesmal nur eine weitere Spezialisierung in einer anderen Regel, aber es existieren weitere Teilelemente. Für diese wird die Prozedur wiederholt. Im Anhang finden sich unter A.2.5 und A.2.6 die dazugehörigen Anfragen. In den Ergebnistabellen A.9 und A.10 befinden sich noch Relationen zu weiteren Regeln. Neben spezialisierenden und unterstützenden Regeln gehören auch Verweise auf Regelwerke sowie eine zu beachtende Regel des *BDSG* dazu. Weitere Teilelemente gibt es an dieser Stelle nicht mehr.
Je nachdem welcher Grund für die Anfrage vorliegt, können auch andere Elemente, wie Aktivitäten, Objekte, Personen oder Eigenschaften, interessant sein.

5.2.4 Beispielszenario 3: Geschäftsprozess

Beschreibung

Ausgangspunkt für dieses Szenario ist ein Geschäftsprozess. Es sollen die Regeln gefunden werden, die in dem Geschäftsprozess beachtet werden müssen. Der betrachtete Geschäftsprozess in Abbildung 5.3 stammt aus [Bos11]. Dabei handelt es sich um den Lebenszyklus eines Dokumentes. Der Geschäftsprozess wurde auf die wesentlichen Elemente reduziert, da diese für das Vorgehen in diesem Szenario ausreichend sind.
Der erste Schritt des Prozesses ist das Verfassen eines Dokumentes. Im nächsten Schritt wird das Dokument gespeichert. Zur Aufbewahrung kann das Dokument entweder ausgedruckt oder gesichert werden. Bei der ausgedruckten Aufbewahrungsform wird das Dokument entweder irgendwann vernichtet oder wieder digitalisiert und gesichert werden. In der Form der elektronischen Aufbewahrung muss das Dokument irgendwann gelöscht werden oder es wird wieder geöffnet und kann bearbeitet und wieder gespeichert werden.

Vorarbeiten

In den Aktivitäten des Geschäftsprozesses gibt es Elemente, die für die Anfrage an die Ontologie von Bedeutung sind. In diesem Szenario sind erstmal nur Objekte und Aktivitäten im Fokus. Elementares Objekt ist das Dokument selbst. In spezifischeren Prozessen können je nach der Modellierung des Geschäftsprozesses noch weitere Objekte wie Computer oder auch Personen mit den Aktivitäten des Prozesses verbunden sein. Mit dem Dokument können verschiedene Aktivitäten im Laufe des Prozesses durchgeführt werden, die im vorherigen Abschnitt beschrieben wurden.
Für die Anfrage müssen die Aktivitäten aus dem Geschäftsprozess noch Aktivitäten aus der Ontologie zugeordnet werden, da es sprachliche Unterschiede bezüglich der Bezeichnungen gibt. Die zugehörigen Aktivitäten werden in Abbildung 5.4 dargestellt. Für die Aktivität *Dokument digitalisieren* aus dem Geschäftsprozess wird die Aktivität *Scan* als mögliche Methode zur Ausführung gewählt.
Zur besseren Übersichtlichkeit wird eine Anfrage für jedes Element einzeln gestellt. In den Anfragen der Aktivitäten sind die folgenden Relationen von Bedeutung:

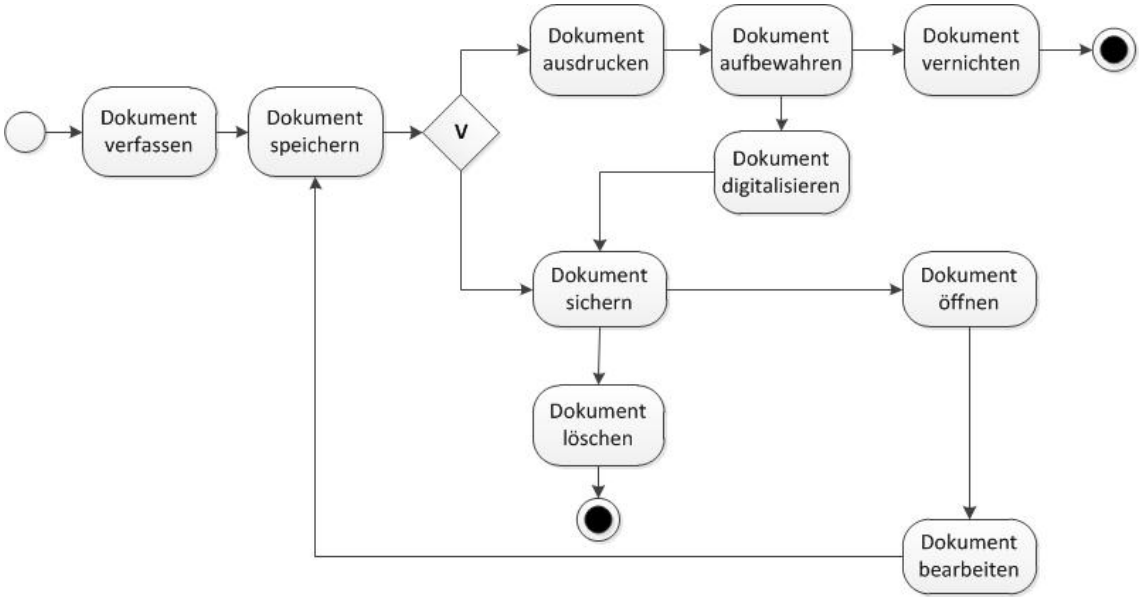

Abbildung 5.3: Geschäftsprozess Dokumentieren

- *istAktivitaetIn*
- *hatGefaehrdung*
- *hatMassnahme*
- *benutztObjekt* und die Regeln für das Objekt

Die Ergebnisse können durch das Verknüpfen mehrerer Stichworte eingegrenzt werden wie z.B. die Kombination einer Aktivität und eines Objektes.
Im nächsten Abschnitt werden die Anfrage und Ergebnisse zu dem Objekt *Dokument* dokumentiert. Ergebnisse, die für den angestrebten Zweck dieser Anfrage unwichtig sind, werden zur besseren Übersichtlichkeit aus der Tabelle entfernt. Wichtig sind für dieses Szenario nur die Regeln. Die Anfragen für die Aktivitäten und die Tabellen mit deren Ergebnissen befinden sich im Anhang A.3.

Prozessaktion	Objekt	Aktivität
Dokument verfassen	Dokument	Dokumentation
Dokument speichern	Dokument	Speicherung
Dokument ausdrucken	Dokument	Drucken
Dokument aufbewahren	Dokument	Archivierung
Dokument vernichten	Dokument	Vernichtung
Dokument digitalisieren	Dokument	Scan
Dokument sichern	Dokument	Sicherung
Dokument löschen	Dokument	Löschung
Dokument öffnen	Dokument	
Dokument bearbeiten	Dokument	Dokumentation

Abbildung 5.4: Zuordnung der Aktivitäten

Dokument

Für das Objekt *Dokument* wird die folgende Anfrage gestellt:

```
SELECT          ?Regel ?Name
WHERE           {{ :Dokument :istObjektIn ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}
                UNION {{ :Dokument :hatGefaehrdung ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}
                UNION { :Dokument :hatMassnahme ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}}
ORDER BY ASC    (?Regel)
```

Tabelle 5.8 zeigt die Regeln für das Objekt *Dokument*.

Für jeder der Aktivitäten wird eine ähnliche Anfrage gestellt. Ziel der Anfragen ist die Ermittlung der Regeln, die für die Aktivitäten beachtet werden müssen. Dabei ist im Fokus, mit welchen Regeln die Aktivität verbunden sind und welche Gefährdungen und Maßnahmen es für die Aktivität gibt. In den Ergebnistabellen werden in der Spalte *Regel* angezeigt. Die Spalte *Name* enthält den Namen der Regel. Zusätzlich wird auch nach Objekten gefragt, die mit den Aktivitäten verbunden sind, und nach Regeln, die für diese beachtet werden müssen. Wenn eine Regel zu einem Objekt gehört, dann wird in der Spalte *Objekt* das Objekt angezeigt.
In den Ergebnistabellen im Anhang wurden wie schon beim Objekt *Dokument* unrelevante Ergebnisse entfernt (z.B. der Typ von Objekten, den man durch die Variable *?Relation* in den Anfragen auch erhält). Die einzelnen Anfragen für die Aktivitäten können auch in einer Anfrage gestellt werden. So können doppelte Regeln, die eventuell durch die einzelnen Anfragen für die Aktivitäten geliefert werden, gefiltert werden. Aus Gründen der besseren Übersichtlichkeit der Ergebnisse wurde darauf aber verzichtet. Die Anfragen befinden sich ebenfalls im Anhang. Die Tabelle 5.9 zeigt die Aktivitäten mit dem zugehörigen Abschnitt im Anhang für Anfrage und Ergebnis.

Regel	**Name**
BSI100-4_Kap3	Der Notfallmanagement-Prozess
BSIGrundschutz_G2.48	Ungeeignete Entsorgung der Datenträger und Dokumente
BSIGrundschutz_M4.170	Auswahl geeigneter Datenformate für die Archivierung von Dokumenten
MaRiskVA_Kap10	Information und Dokumentation
MaRiskVA_Kap7.2	Organisatorische Maßnahmen

Tabelle 5.8: Regeln für das Objekt *Dokument*

Aktivität	Abschnitt	Ergebnistabelle
Dokumentation	A.3.1	A.11 und A.12
Speicherung	A.3.2	A.13
Drucken	A.3.3	A.14
Archivierung	A.3.4	A.15
Vernichtung	A.3.5	A.16
Scan	A.3.6	A.17
Sicherung	A.3.7	A.18 und A.19
Löschung	A.3.8	A.20

Tabelle 5.9: Aktivitäten im Anhang

5.3 Zusammenfassung

In diesem Kapitel wurde anhand von drei Beispielszenarien die Ontologie evaluiert. Dafür wurde die Funktion für SPARQL-Anfragen in Protégé genutzt. Die Möglichkeiten mit SPARQL sind eingeschränkt, jedoch konnte mit den Anfragemöglichkeiten zumindest grundlegend gezeigt werden, wie die Ontologie eingesetzt werden kann.
Dabei konnten sowohl Verbindungen zu anderen Regelwerken gefunden werden, als auch Regeln für die Aktivitäten eines Geschäftsprozesses. Bei der Formulierung der Anfrage muss genau überlegt werden, auf welchen Aspekt bei den Ergebnissen mehr Wert gelegt werden soll:

- Sollen möglichst genaue und passende Ergebnisse und damit auch tendenziell weniger Ergebnisse gefunden werden?

  oder

- Soll nach möglichst vielen Ergebnissen gesucht werden, wo eventuell nicht relevante Ergebnisse manuell aussortiert werden müssen?

Im nächsten Kapitel soll eine Zusammenfassung dieser Arbeit vorgenommen und Überlegungen zu Verbesserungen und weitergehenden Arbeiten angestellt werden.

Kapitel 6

Zusammenfassung und Ausblick

Das Ziel der Diplomarbeit war die Modellierung einer Ontologie und darauf aufbauend eine Anforderungserhebung zur Auswahl eines Tools für die Umsetzung dieser Ontologie. Die Ontologie sollte so modelliert werden, dass sie Unternehmen bei ihrer Compliance unterstützen kann, indem Verbindungen zwischen unterschiedlichen Regelwerken aufgezeigt und Regeln zu Geschäftsprozessen gefunden werden können.

6.1 Zusammenfassung

Eine Ontologie besteht aus Konzepten, Instanzen und Relationen, die eine Domäne beschreiben. In dieser Arbeit sollten unterschiedliche Regelwerke in einer Ontologie modelliert werden. Es wurden zunächst Konzepte modelliert, um die Arten und die Struktur der Regelwerke und Regeln allgemein zu beschreiben. Die Instanzen dieser Konzepte bestehen aus den betrachteten Regelwerken und ihren Regeln. Um die Konzepte und Instanzen der verschiedenen Regelwerke miteinander zu verbinden, wurden Relationen anhand der Regelwerke identifiziert und modelliert.
In einem weiteren Schritt wurden Elemente in den Regeln identifiziert. Mit diesen Elementen ist es möglich für Geschäftsprozesse relevante Regeln zu finden, die in den Schritten des Prozesses beachtet werden müssen. Diese Elemente werden in die Kategorien *Aktivität*, *Prozess*, *Person*, *Objekt* und *Eigenschaft* unterteilt. Die Elemente sind auch in Geschäftsprozessen zu finden oder lassen sich aus diesen ableiten und ermöglichen daher eine Verbindung mit der Ontologie.
Ausgehend von der Modellierung wurden Anforderungen an ein Tool identifiziert, die dieses zur Darstellung und Benutzung der Ontologie erfüllen sollte. Zu diesen Anforderungen zählten zum einen Aspekte bezüglich der Bedienung der Tools und zum anderen Ontologiespezifische Anforderungen, die sich aus der Modellierung der Ontologie ergaben. Anhand dieser Anforderungen wurde eine Auswahl von Ontologie-Tools bewertet. Nach dieser Bewertung wurde das Tool *Protégé* ausgewählt, um die modellierte Ontologie beispielhaft umzusetzen und zu evaluieren.
Zur Evaluierung der Ontologie wurde die Anfragesprache SPARQL benutzt, mit der die Funktionalität der Ontologie anhand von drei Beispielszenarien näher betrachtet wurde. Dabei wurde gezeigt, wie ausgehend von Elementen, Regeln oder einem Geschäftsprozess mit Hilfe der Ontologie relevante Regeln gefunden werden können.

6.2 Bewertung

Im Verlauf der Analyse der Regelwerke und der Modellierung der Ontologie ergaben sich Schwierigkeiten, aber auch Potenziale bei der Nutzung der Ontologie.
Die ausgewählten Regelwerke kamen aus unterschiedlichen Bereichen. Bei der Identifikation der Verbindungen zwischen den Regelwerken ergab sich, dass die Verbindungen meist auf nur wenige Themenbereiche wie Risikomanagement, Notfallmanagement, etc. begrenzt waren. Nach der Definition der Relationen zwischen den Regelwerken wurde zudem deutlich, dass die Zuordnung der Regeln bei einigen der Relationen nicht immer eindeutig durchführbar war. Dieses Problem trat oft bei der Unterscheidung zwischen den Relationen *unterstütztVon* und *istSpezialisiertIn* auf, wo bei der Zuordnung der Regeln nicht eindeutig klar war, welche der Relationen besser geeignet ist.
Eine weitere Schwierigkeit ergab sich durch den Ansatz bei der Modellierung der Ontologie die unterschiedlichen Regelwerke in eine gemeinsame Ontologie zu bringen. Die Modellierung wurde deswegen stark an die ausgewählten Regelwerke angepasst. Z.B. behandelt diese Arbeit von den beiden *MaRisk* nur die Variante für die Versicherungen. Durch die Art der Modellierung ist die *MaRisk VA* stark in die Ontologiestruktur integriert. Der Austausch der *MaRisk VA* durch die *MaRisk BA* wäre daher sehr aufwändig.
Potenzial in der Ontologie bietet dagegen die Verbindung der Regeln zu Geschäftsprozessen. Neben der Funktionalität zur Identifizierung von Regeln für Geschäftsprozesse können diese auch die Möglichkeit bieten mit Hilfe der Elemente in den Regeln ähnliche und sich unterstützende Regeln zu identifizieren.

Im nächsten Abschnitt sollen mögliche Lösungen für diese Schwierigkeiten und Weiterentwicklungsmöglichkeiten für die Ontologie aufgezeigt werden.

6.3 Ausblick

Dieser Abschnitt wird in zwei Unterabschnitte unterteilt. Im ersten Abschnitt werden Verbesserungen der Ontologie aufgezeigt. Der zweite Abschnitt beschäftigt sich mit möglichen Erweiterungen für den Einsatz der Ontologie.

Verbesserungen

Um die Schwierigkeiten mit den Relationen in der Ontologie zu lösen, sollten diese überarbeitet werden, indem sie zusammengefasst oder mehr abgegrenzt werden. Für eine eindeutigere Identifikation der Verbindungen zwischen Regelwerken sollten grundsätzlich Experten der einzelnen Bereiche herangezogen werden. Für die betrachteten Regelwerke wären das insbesondere Experten der Bereiche Risikomanagement, Datenschutz und Informationssicherheit. Da dieses Vorgehen zu einem relativ hohen Aufwand führt, sollte für diesen Bereich abgewägt werden, ob das Potenzial der Relationen zwischen den Regelwerken diesen Aufwand rechtfertigt. Alternativ oder ergänzend könnte diese Funktionalität über die gemeinsamen Elemente in den Regeln erhalten werden.
Für eine bessere Nutzbarkeit der Ontologie bezüglich der Geschäftsprozesse sollte die Einordnung und Benennung der Konzepte für die Elemente überarbeitet werden. Die Relationen für die Verbindung der Regeln mit den Elementen sollten differenzierter benannt werden, so dass mehr kontextspezifische Informationen durch die Benennung der Relationen bekannt sind. Protégé bietet die Möglichkeit von *Subproperties*, womit eine Relation in spezifischere Relationen unterteilt werden kann.

6.3.1 Beispiel (Subproperties).
Für die Relation *hatPerson* könnten z.B. folgende spezifischeren Relationen definiert werden:

- erfordertMitwirkungVon
  - erfordertEntscheidungVon
- istMaßnahmeFür (nur auf Personen bezogen)

Bei dem Ansatz für die Modellierung der Ontologie wäre eine andere Vorgehensweise eventuell vielversprechender. So könnte zunächst jedes Regelwerk in einer eigenen Ontologie modelliert werden. Diese Ontologien könnten dann nach Bedarf zusammengeführt werden. Dabei können gleiche Begriffe z.B. über das OWL-Element *owl:sameAs* miteinander verbunden oder dieselben Begriffe als Schnittpunkte verschmolzen werden. Ein Hauptvorteil dieser Vorgehensweise wäre die einfachere Austauschbarkeit von Regelwerken wie im Fall mit den beiden *MaRisk*.

Erweiterungen

Eine inhaltliche Möglichkeit zur Erweiterung besteht in der Einbeziehung und Umsetzung weiterer Regelwerke. Die betrachteten Regelwerke stellen nur eine kleine Teilmenge möglicher Regelwerke dar. Da die betrachteten Regelwerke nur in Auszügen umgesetzt wurde, gibt es auch bei diesen Potenzial für weitere Ergänzungen.
Des Weiteren wurden bei der Umsetzung nur die grundlegenden Ontologieelemente und -eigenschaften von Protégé benutzt. Eine Erweiterung könnte in der Formulierung von Bedingungen für Konzepte bestehen, die z.B. Möglichkeiten für die automatische Klassifizierung von Elementen bieten könnten.

In Kapitel 5.2.1 wurde bereits auf die limitierten Möglichkeiten von Anfragen mit SPARQL innerhalb von Protégé hingewiesen. Mit der Nutzung von anderen *Reasonern* könnten potenziell mehr Möglichkeiten zur automatischen Anfrage und Weiterverarbeitung der Ergebnisse geboten werden. Möglich wäre das über die Nutzung der *Protégé-API*.

Die Umwandlung der Elemente von Geschäftsprozessen zu Anfragen für die Ontologie wurde in Kapitel 5.2.4 noch manuell vorgenommen. Dieser Prozess könnte automatisiert umgesetzt werden. Die Elemente der Geschäftsprozesse könnten mit einer entsprechenden Schnittstelle automatisiert identifiziert und in Anfragen für die Ontologie umgesetzt werden.

Anhang A

Anhang

Der Anhang enthält die Anfragen und die zugehörigen Ergebnisse zu den Beispielszenarien aus Kapitel 5.

A.1 Beispielszenario: Vertraulichkeit

A.1.1 Gefährdungen für Vertraulichkeit

```
SELECT          ?Regel ?Name
WHERE           { :Vertraulichkeit :hatGefaehrdung ?Regel.
                  OPTIONAL { ?Regel rdfs:label ?Name.}}
ORDER BY ASC    (?Regel)
```

Regel	**Name**
BSIGrundschutz_G2.111	Kompromittierung von Anmeldedaten bei Dienstleisterwechsel
BSIGrundschutz_G2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
BSIGrundschutz_G2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
BSIGrundschutz_G2.54	Vertraulichkeitsverlust durch Restinformationen
BSIGrundschutz_G3.1	Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
BSIGrundschutz_G3.13	Weitergabe falscher oder interner Informationen
BSIGrundschutz_G3.26	Ungewollte Freigabe des Dateisystems
BSIGrundschutz_G3.44	Sorglosigkeit im Umgang mit Informationen
BSIGrundschutz_G3.45	Unzureichende Identifikationsprüfung von Kommunikationspartnern

Tabelle A.1: Regeln mit Gefährdungen für Vertraulichkeit - Teil 1

Regel	Name
BSIGrundschutz_G3.97	Vertraulichkeitsverlust trotz BitLocker Drive Encryption unter Windows Vista
BSIGrundschutz_G4.27	Unterlaufen von Zugriffskontrollen über ODBC
BSIGrundschutz_G4.34	Ausfall eines Kryptomoduls
BSIGrundschutz_G4.37	Mangelnde Authentizität und Vertraulichkeit von E-Mail
BSIGrundschutz_G5.104	Ausspähen von Informationen
BSIGrundschutz_G5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
BSIGrundschutz_G5.123	Abhören von Raumgesprächen über mobile Endgeräte
BSIGrundschutz_G5.13	Abhören von Räumen
BSIGrundschutz_G5.139	Abhören der WLAN-Komponenten
BSIGrundschutz_G5.143	Man-in-the-Middle-Angriff
BSIGrundschutz_G5.146	Vertraulichkeitsverlust durch Auslagerungsdateien
BSIGrundschutz_G5.40	Abhören von Räumen mittels Rechner mit Mikrofon
BSIGrundschutz_G5.7	Abhören von Leitungen
BSIGrundschutz_G5.71	Vertraulichkeitsverlust schützenswerter Informationen

Tabelle A.2: Regeln mit Gefährdungen für Vertraulichkeit - Teil 2

A.1.2 Maßnahmen für Vertraulichkeit

```
SELECT          ?Regel ?Name
WHERE           { :Vertraulichkeit :hatMassnahme ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}
ORDER BY ASC    (?Regel)
```

Regel	Name
BSIGrundschutz_M2.164	Auswahl eines geeigneten kryptographischen Verfahrens
BSIGrundschutz_M2.56	Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter
BSIGrundschutz_M3.18	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
BSIGrundschutz_M3.23	Einführung in kryptographische Grundbegriffe
BSIGrundschutz_M3.55	Vertraulichkeitsvereinbarungen
BSIGrundschutz_M4.22	Verhinderung des Vertraulichkeitsverlustes schutzbedürftiger Daten im Unix-System
BSIGrundschutz_M4.29	Einsatz eines Verschlüsselungsproduktes für tragbare PCs
BSIGrundschutz_M5.108	Kryptographische Absicherung von E-Mail

Tabelle A.3: Regeln mit Maßnahmen für Vertraulichkeit

A.2 Beispielszenario: Risikomanagement

A.2.1 Regeln für Teilprozesse von *Risikomanagement*

```
SELECT          ?Teilprozess ?Regel ?Name
WHERE           { :Risikomanagement :hatTeilprozess ?Teilprozess.
OPTIONAL        {{ ?Teilprozess :istAktivitaetIn ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}
                UNION {{ ?Teilprozess :hatGefaehrdung ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}
                UNION { ?Teilprozess :hatMassnahme ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}}
ORDER BY ASC    (?Teilprozess)
```

Teilprozess	**Regel**	**Name**
Ablauforganisation-Risikomanagement	MaRiskVA_Kap7.2.2	Ablauforganisation
Aufbauorganisation-Risikomanagement	MaRiskVA_Kap7.2.1	Aufbauorganisation
Risikoakzeptanz	ISO27005_Kap10	Information security risk acceptance
Risikoakzeptanz	MaRiskVA_Kap7.3.2.3	Risikosteuerung
Risikoanalyse	BSI100-4_Kap5.2	Risikoanalyse
Risikoanalyse	ISO27001_Kap4.1	General requirements
Risikoanalyse	ISO27005_Kap8.2	Risk analysis
Risikoanalyse	MaRiskVA_Kap7.3.2.2	Risikoanalyse und -bewertung
Risikoanalyse	MaRiskVA_Kap8	Funktionsausgliederung und Dienstleistungen im Sinne des §64a Abs. 4 VAG
Risikobehandlung	BSI100-3_Kap6	Behandlung von Risiken
Risikobehandlung	ISO27001_Kap4.2	Establishing and managing the ISMS
Risikobehandlung	ISO27005_Kap9	Information security risk treatment
Risikobewertung	BSI100-1_Kap8.1	Erstellung des Sicherheitskonzepts
Risikobewertung	BSI100-1_Kap9.2.1	Risikobewertung
Risikobewertung	BSI100-2_Kap5	Umsetzung der Sicherheitskonzeption
Risikobewertung	BSI100-4_Kap5.2.2	Risikobewertung
Risikobewertung	ISO27001_Kap4.1	General requirements
Risikobewertung	ISO27005_Kap8.2.2	Risk estimation
Risikobewertung	ISO27005_Kap8.3	Risk evaluation
Risikobewertung	MaRiskVA_Kap7.3.2.2	Risikoanalyse und -bewertung
Risikobewertung	MaRiskVA_Kap8	Funktionsausgliederung und Dienstleistungen im Sinne des §64a Abs. 4 VAG

Tabelle A.4: Regeln für die Teilprozesse von *Risikomanagement* - Teil 1

Teilprozess	Regel	Name
Risikoidentifikation	BSI100-3_Kap4	Ermittlung zusätzlicher Gefährdungen
Risikoidentifikation	BSI100-4_Kap5.2.1	Risikoidentifizierung
Risikoidentifikation	ISO27005_Kap8.2.1	Risk identification
Risikoidentifikation	MaRiskVA_Kap8	Funktionsausgliederung und Dienstleistungen im Sinne des §64a Abs. 4 VAG
Risikokommunikation	ISO27005_Kap11	Information security risk communication
Risikokommunikation	MaRiskVA_Kap10	Information und Dokumentation
Risikoueberwachung	BSI100-3_Kap6.2	Risiken unter Beobachtung
Risikoueberwachung	ISO27005_Kap12	Information security risk monitoring and review
Risikoueberwachung	MaRiskVA_Kap7.3.2.4	Risikoüberwachung

Tabelle A.5: Regeln für die Teilprozesse von *Risikomanagement* - Teil 2

A.2.2 Regeln für die Unterkonzepte von *Risikobehandlung*

```
SELECT          ?Unterkonzept ?Regel ?Name
WHERE           { ?Unterkonzept rdfs:subClassOf :Risikobehandlung.
OPTIONAL        {{ ?Unterkonzept :istAktivitaetIn ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}
                UNION {{ ?Unterkonzept :hatGefaehrdung ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}
                UNION { ?Unterkonzept :hatMassnahme ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}}
ORDER BY ASC    (?Unterkonzept)
```

Unterkonzept	Regel	Name
Risikoannahme	BSI100-3_Kap6.1	Handlungsalternativen
Risikoannahme	BSI100-4_Kap5.2.4	Risikostrategie-Optionen identifizieren
Risikoannahme	ISO27005_Kap9.3	Risk retention
Risikoreduktion	BSI100-3_Kap6.1	Handlungsalternativen
Risikoreduktion	BSI100-4_Kap5.2.4	Risikostrategie-Optionen identifizieren
Risikoreduktion	ISO27005_Kap9.2	Risk reduction
Risikoreduktion	MaRiskVA_Kap7.3.2.3	Risikosteuerung
Risikotransfer	BSI100-3_Kap6.1	Handlungsalternativen
Risikotransfer	BSI100-4_Kap5.2.4	Risikostrategie-Optionen identifizieren
Risikotransfer	ISO27005_Kap9.5	Risk transfer
Risikovermeidung	BSI100-3_Kap6.1	Handlungsalternativen
Risikovermeidung	BSI100-4_Kap5.2.4	Risikostrategie-Optionen identifizieren
Risikovermeidung	ISO27005_Kap9.4	Risk avoidance
Risikovermeidung	MaRiskVA_Kap7.3.2.3	Risikosteuerung

Tabelle A.6: Regeln für die Unterkonzepte von *Risikobehandlung*

A.2.3 Regeln für die Unterkapitel von *MaRiskVA_Kap7*

```
SELECT          ?Regel1 ?Relation ?Objekt
WHERE           { ?Regel1 :istTeilelementVon :MaRiskVA_Kap7.
                  ?Regel1 ?Relation ?Objekt.}
ORDER BY ASC    (?Regel1)
```

Regel1	**Relation**	**Objekt**
MaRiskVA_Kap7.1	istSpezialisiertIn	ISO27001_Kap4.2
MaRiskVA_Kap7.1	rdfs:label	Risikostrategie
MaRiskVA_Kap7.2	istVerallgemeinertIn	BDSG_P9
MaRiskVA_Kap7.2	unterstuetztVon	BSIGrundschutz_B1.1
MaRiskVA_Kap7.2	unterstuetztVon	BSIGrundschutz_B1.2
MaRiskVA_Kap7.2	hatTeilelement	MaRiskVA_Kap7.2.1
MaRiskVA_Kap7.2	hatTeilelement	MaRiskVA_Kap7.2.2
MaRiskVA_Kap7.2	rdfs:label	Organisatorische Maßnahmen
MaRiskVA_Kap7.3	istSpezialisiertIn	BSI100-2_Kap4.6.3
MaRiskVA_Kap7.3	istSpezialisiertIn	BSI100-4_Kap5.2
MaRiskVA_Kap7.3	istSpezialisiertIn	ISO27001_Kap4.2
MaRiskVA_Kap7.3	istSpezialisiertIn	ISO27005
MaRiskVA_Kap7.3	hatTeilelement	MaRiskVA_Kap7.3.1
MaRiskVA_Kap7.3	hatTeilelement	MaRiskVA_Kap7.3.2
MaRiskVA_Kap7.3	hatTeilelement	MaRiskVA_Kap7.3.3
MaRiskVA_Kap7.3	hatTeilelement	MaRiskVA_Kap7.3.4
MaRiskVA_Kap7.3	hatTeilelement	MaRiskVA_Kap7.3.5
MaRiskVA_Kap7.3	rdfs:label	Internes Steuerungs- und Kontrollsystem
MaRiskVA_Kap7.4	rdfs:label	Interne Revision
MaRiskVA_Kap7.5	rdfs:label	Interne Kontrollen

Tabelle A.7: Unterkapitel von Kapitel 7 und Relationen

A.2.4 Regeln für die Unterunterkapitel von *MaRiskVa_Kap7*

```
SELECT          ?Regel2 ?Relation ?Objekt
WHERE           { ?Regel1 :istTeilelementVon :MaRiskVA_Kap7.
                  OPTIONAL { ?Regel2 :istTeilelementVon ?Regel1.
                  ?Regel2 ?Relation ?Objekt.}}
ORDER BY ASC    (?Regel2)
```

A.2.5 Regeln für die Unterkapitel von *MaRiskVA_Kap7.2.2*

Regel1	Relation	Objekt
MaRiskVA_Kap7.2.1	rdfs:label	Aufbauorganisation
MaRiskVA_Kap7.2.2	hatTeilelement	MaRiskVA_Kap7.2.2.1
MaRiskVA_Kap7.2.2	hatTeilelement	MaRiskVA_Kap7.2.2.2
MaRiskVA_Kap7.2.2	hatTeilelement	MaRiskVA_Kap7.2.2.3
MaRiskVA_Kap7.2.2	rdfs:label	Ablauforganisation
MaRiskVA_Kap7.3.1	rdfs:label	Risikotragfähigkeitskonzept und Limitierung
MaRiskVA_Kap7.3.2	hatTeilelement	MaRiskVA_Kap7.3.2.1
MaRiskVA_Kap7.3.2	hatTeilelement	MaRiskVA_Kap7.3.2.2
MaRiskVA_Kap7.3.2	hatTeilelement	MaRiskVA_Kap7.3.2.3
MaRiskVA_Kap7.3.2	hatTeilelement	MaRiskVA_Kap7.3.2.4
MaRiskVA_Kap7.3.2	rdfs:label	Risikokontrollprozess
MaRiskVA_Kap7.3.3	istSpezialisiertIn	ISO27005_Kap11
MaRiskVA_Kap7.3.3	rdfs:label	Unternehmensinterne Kommunikation und Risikokultur
MaRiskVA_Kap7.3.4	rdfs:label	Risikoberichterstattung
MaRiskVA_Kap7.3.5	rdfs:label	Qualitätssicherung Internes Steuerungs- und Kontrollsystem

Tabelle A.8: Unterkapitel von Kapitel 7.2 und 7.3 und ihre Relationen

```
SELECT          ?Regel1 ?Relation ?Objekt
WHERE           { ?Regel1 :istTeilelementVon :MaRiskVA_Kap7.2.2.
                OPTIONAL { ?Regel1 ?Relation ?Objekt.}}
ORDER BY ASC    (?Regel1)
```

Regel1	Relation	Objekt
MaRiskVA_Kap7.2.2.1	rdfs:label	Neue Geschäftsfelder sowie Kapitalmarkt-, Versicherungs- und Rückversicherungsprodukte
MaRiskVA_Kap7.2.2.2	erfordertBeachtungVon	BDSG_P9
MaRiskVA_Kap7.2.2.2	verweistAufRegelwerk	BSIGrundschutz
MaRiskVA_Kap7.2.2.2	unterstuetztVon	BSIGrundschutz_B1.7
MaRiskVA_Kap7.2.2.2	verweistAufRegelwerk	ISO27002
MaRiskVA_Kap7.2.2.2	rdfs:label	Betriebliche Anreizsysteme und Ressourcen
MaRiskVA_Kap7.2.2.3	rdfs:label	Organisationsentwicklung

Tabelle A.9: Unterkapitel von Kapitel 7.2.2 und ihre Relationen

A.2.6 Regeln für die Unterkapitel von *MaRiskVA_7.3.2*

```
SELECT          ?Regel1 ?Relation ?Objekt
WHERE           { ?Regel1 :istTeilelementVon :MaRiskVA_Kap7.3.2.
                OPTIONAL { ?Regel1 ?Relation ?Objekt?.}}
ORDER BY ASC    (?Regel1)
```

Regel1	**Relation**	**Objekt**
MaRiskVA_Kap7.3.2.1	rdfs:label	Risikoidentifikation
MaRiskVA_Kap7.3.2.2	istSpezialisiertIn	BSI100-1_Kap8.1
MaRiskVA_Kap7.3.2.2	istSpezialisiertIn	BSI100-1_Kap9.2.1
MaRiskVA_Kap7.3.2.2	istSpezialisiertIn	ISO27002_Kap4
MaRiskVA_Kap7.3.2.2	rdfs:label	Risikoanalyse und -bewertung
MaRiskVA_Kap7.3.2.3	istSpezialisiertIn	BSI100-1_Kap8.1
MaRiskVA_Kap7.3.2.3	istSpezialisiertIn	ISO27002_Kap4
MaRiskVA_Kap7.3.2.3	rdfs:label	Risikosteuerung
MaRiskVA_Kap7.3.2.4	rdfs:label	Risikoüberwachung

Tabelle A.10: Unterkapitel von Kapitel 7.3.2 und ihre Relationen

A.3 Beispielszenario: Geschäftsprozess

A.3.1 Dokumentation

```
SELECT          ?Regel ?Name ?Objekt
WHERE           {{ :Dokumentation :istAktivitaetIn ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}
                UNION {{ :Dokumentation :hatGefaehrdung ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}
                UNION {{ :Dokumentation :hatMassnahme ?Regel.
                OPTIONAL {?Regel rdfs:label ?Name.}}}
                UNION { :Dokumentation :benutztObjekt ?Objekt.
                ?Objekt ?Relation ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}
ORDER BY ASC    (?Regel)
```

Regel	Name	Objekt
BDSG_P11	Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag	
BDSG_P28b	Scoring	
BDSG_P4d	Meldepflicht	
BDSG_P4e	Inhalt der Meldepflicht	
BSI100-2_Kap4.5.3	Dokumentation der Ergebnisse	
BSI100-2_Kap6.2.2	Dokumentation im Informations-sicherheitsprozess	
BSI100-4_Kap3	Der Notfallmanagement-Prozess	Dokument
BSI100-4_Kap3.2	Dokumentation	
BSI100-4_Kap7.1.8	Dokumentation in der Notfall-bewältigung	
BSIGrundschutz_G2.27	Fehlende oder unzureichende Dokumentation	
BSIGrundschutz_G2.28	Verstöße gegen das Urheberrecht	
BSIGrundschutz_G2.48	Ungeeignete Entsorgung der Datenträger und Dokumente	Dokument
BSIGrundschutz_M2.107	Dokumentation der ISDN-Karten-Konfiguration	
BSIGrundschutz_M2.153	Dokumentation von Novell Netware 4.x Netzen	
BSIGrundschutz_M2.19	Neutrale Dokumentation in den Verteilern	
BSIGrundschutz_M2.201	Dokumentation des Sicherheits-prozesses	
BSIGrundschutz_M2.219	Kontinuierliche Dokumentation der Informationsverarbeitung	
BSIGrundschutz_M2.25	Dokumentation der System-konfiguration	
BSIGrundschutz_M2.259	Einführung eines übergeordneten Dokumentenmanagements	
BSIGrundschutz_M2.281	Dokumentation der System-konfiguration von Routern und Switches	
BSIGrundschutz_M2.31	Dokumentation der zugelassenen Benutzer und Rechteprofile	
BSIGrundschutz_M2.34	Dokumentation der Veränderungen an einem bestehenden System	

Tabelle A.11: Regeln für die Aktivität *Dokumentation* - Teil 1

Regel	Name	Objekt
BSIGrundschutz_M2.358	Dokumentation der Systemeinstellungen von Speichersystemen	
BSIGrundschutz_M2.396	Vorgaben zur Dokumentation und Kennzeichnung der IT-Verkabelung	
BSIGrundschutz_M4.170	Auswahl geeigneter Datenformate für die Archivierung von Dokumenten	Dokument
BSIGrundschutz_M5.143	Laufende Fortschreibung und Revision der Netzdokumentation	
BSIGrundschutz_M5.4	Dokumentation und Kennzeichnung der Verkabelung	
BSIGrundschutz_M6.119	Dokumentation im Notfallmanagement-Prozess	
BSIGrundschutz_M6.134	Dokumentation von Sicherheitsvorfällen	
BSIGrundschutz_M6.37	Dokumentation der Datensicherung	
ISO27001_Kap4.3	Documentation requirements	
MaRiskVA_Kap10	Information und Dokumentation	
MaRiskVA_Kap10	Information und Dokumentation	Dokument
MaRiskVA_Kap7.1	Risikostrategie	
MaRiskVA_Kap7.2	Organisatorische Maßnahmen	Dokument
MaRiskVA_Kap7.2.2.1	Neue Geschäftsfelder sowie Kapitalmarkt-, Versicherungs- und Rückversicherungsprodukte	
MaRiskVA_Kap7.2.2.2	Betriebliche Anreizsysteme und Ressourcen	
MaRiskVA_Kap7.3.1	Risikotragfähigkeitskonzept und Limitierung	
MaRiskVA_Kap7.3.2.4	Risikoüberwachung	
MaRiskVA_Kap7.3.4	Risikoberichterstattung	
MaRiskVA_Kap7.3.5	Qualitätssicherung Internes Steuerungs- und Kontrollsystem	
MaRiskVA_Kap7.4	Interne Revision	

Tabelle A.12: Regeln für die Aktivität *Dokumentation* - Teil 2

A.3.2 Speicherung

```
SELECT      ?Regel ?Name ?Objekt
WHERE       {{ :Speicherung :istAktivitaetIn ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}
            UNION {{ :Speicherung :hatGefaehrdung ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
            UNION {{ :Speicherung :hatMassnahme ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
            UNION { :Speicherung :benutztObjekt ?Objekt.
            ?Objekt ?Relation ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
ORDER BY ASC (?Regel)
```

Regel	**Name**	**Objekt**
BDSG_P14	Datenspeicherung, -veraenderung und -nutzung	
BDSG_P19	Auskunft an den Betroffenen	
BDSG_P19a	Benachrichtigung	
BDSG_P20	Berichtigung, Loeschung und Sperrung von Daten; Widerspruchsrecht	
BDSG_P28	Datenerhebung und -speicherung fuer eigene Geschaeftszwecke	
BDSG_P29	Geschaeftsmaeßige Datenerhebung und -speicherung zum Zweck der Uebermittlung	
BDSG_P30	Geschaeftsmaeßige Datenerhebung und -speicherung zum Zweck der Uebermittlung in anonymisierter Form	
BDSG_P33	Benachrichtigung des Betroffenen	
BDSG_P34	Auskunft an den Betroffenen	
BDSG_P6	Rechte des Betroffenen	

Tabelle A.13: Regeln für die Aktivität *Speicherung*

A.3.3 Drucken

```
SELECT      ?Regel ?Name ?Objekt
WHERE       {{ :Drucken :istAktivitaetIn ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}
            UNION {{ :Drucken :hatGefaehrdung ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
            UNION {{ :Drucken :hatMassnahme ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
            UNION { :Drucken :benutztObjekt ?Objekt.
            ?Objekt ?Relation ?Regel.
            OPTIONAL {?Regel rdfs:label ?Name.}}}
ORDER BY ASC (?Regel)
```

Regel	**Name**	**Objekt**
BSIGrundschutz_B3.406	Drucker, Kopierer und Multifunktionsgeräte	Drucker
BSIGrundschutz_G3.86	Ungeregelte und sorglose Nutzung von Druckern, Kopierern und Multifunktionsgeräten	Drucker
BSIGrundschutz_G4.65	Unzureichender Schutz der Kommunikation bei Druckern und Multifunktionsgeräten	Drucker

Tabelle A.14: Regeln für die Aktivität *Drucken*

A.3.4 Archivierung

```
SELECT      ?Regel ?Name ?Objekt
WHERE       {{ :Archivierung :istAktivitaetIn ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}
            UNION {{ :Archivierung :hatGefaehrdung ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
            UNION {{ :Archivierung :hatMassnahme ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
            UNION { :Archivierung :benutztObjekt ?Objekt.
            ?Objekt ?Relation ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
ORDER BY ASC (?Regel)
```

Regel	Name	Objekt
BSIGrundschutz_B1.12	Archivierung	
BSIGrundschutz_G2.75	Mangelnde Kapazität von Archiv-datenträgern	
BSIGrundschutz_G2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive	
BSIGrundschutz_G2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierung	
BSIGrundschutz_G2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung	
BSIGrundschutz_G3.54	Verwendung ungeeigneter Datenträger bei der Archivierung	
BSIGrundschutz_G5.106	Unberechtigtes Überschreiben oder Löschen von Archivmedien	
BSIGrundschutz_M4.170	Auswahl geeigneter Datenformate für die Archivierung von Dokumenten	

Tabelle A.15: Regeln für die Aktivität *Archivierung*

A.3.5 Vernichtung

```
SELECT          ?Regel ?Name ?Objekt
WHERE           {{ :Vernichtung :istAktivitaetIn ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}
                UNION {{ :Vernichtung :hatGefaehrdung ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}
                UNION {{ :Vernichtung :hatMassnahme ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}
                UNION { :Vernichtung :benutztObjekt ?Objekt.
                ?Objekt ?Relation ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}
ORDER BY ASC    (?Regel)
```

Regel	Name	Objekt
BSIGrundschutz_B1.15	Löschen und Vernichten von Daten	
BSIGrundschutz_G2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung	
BSIGrundschutz_M2.167	Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten	
BSIGrundschutz_M2.431	Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen	
BSIGrundschutz_M2.432	Richtlinie für die Löschung und Vernichtung von Informationen	
BSIGrundschutz_M2.433	Überblick über Methoden zur Löschung und Vernichtung von Daten	
BSIGrundschutz_M2.434	Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern	
BSIGrundschutz_M3.67	Einweisung aller Mitarbeiter über Methoden zur Löschung oder Vernichtung von Daten	

Tabelle A.16: Regeln für die Aktivität *Vernichtung*

A.3.6 Scan

```
SELECT          ?Regel ?Name ?Objekt
WHERE           {{ :Scan :istAktivitaetIn ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}
                UNION {{ :Scan :hatGefaehrdung ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}
                UNION {{ :Scan :hatMassnahme ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}
                UNION { :Scan :benutztObjekt ?Objekt.
                ?Objekt ?Relation ?Regel.
                OPTIONAL { ?Regel rdfs:label ?Name.}}}
ORDER BY ASC    (?Regel)
```

Regel	Name	Objekt
BSIGrundschutz_B3.406	Drucker, Kopierer und Multifunktionsgeräte	Scanner

Tabelle A.17: Regeln für die Aktivität *Scan*

A.3.7 Sicherung

```
SELECT      ?Regel ?Name ?Objekt
WHERE       {{ :Sicherung :istAktivitaetIn ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}
            UNION {{ :Sicherung :hatGefaehrdung ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
            UNION {{ :Sicherung :hatMassnahme ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
            UNION { :Sicherung :benutztObjekt ?Objekt.
            ?Objekt ?Relation ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
ORDER BY ASC (?Regel)
```

Regel	**Name**	**Objekt**
BDSG_P31	Besondere Zweckbindung	
BSIGrundschutz_B1.4	Datensicherungskonzept	
BSIGrundschutz_G2.127	Unzureichende Planung von Datensicherungs-methoden für Domänen-Controller	
BSIGrundschutz_M2.137	Beschaffung eines geeigneten Datensicherungssystems	
BSIGrundschutz_M2.41	Verpflichtung der Mitarbeiter zur Datensicherung	
BSIGrundschutz_M6.101	Datensicherung bei VoIP	
BSIGrundschutz_M6.107	Erstellung von Datensicherungen für Verzeichnisdienste	
BSIGrundschutz_M6.108	Datensicherung für Domänen-Controller	
BSIGrundschutz_M6.22	Sporadische Überprüfung auf Wiederherstell-barkeit von Datensicherungen	
BSIGrundschutz_M6.26	Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten	
BSIGrundschutz_M6.32	Regelmäßige Datensicherung	
BSIGrundschutz_M6.33	Entwicklung eines Datensicherungskonzepts	
BSIGrundschutz_M6.34	Erhebung der Einflussfaktoren der Datensicherung	
BSIGrundschutz_M6.35	Festlegung der Verfahrensweise für die Datensicherung	
BSIGrundschutz_M6.36	Festlegung des Minimaldatensicherungs-konzeptes	

Tabelle A.18: Regeln für die Aktivität *Sicherung* - Teil 1

Regel	Name	Objekt
BSIGrundschutz_M6.37	Dokumentation der Datensicherung	
BSIGrundschutz_M6.47	Datensicherung bei der Telearbeit	
BSIGrundschutz_M6.49	Datensicherung einer Datenbank	
BSIGrundschutz_M6.56	Datensicherung bei Einsatz kryptographischer Verfahren	
BSIGrundschutz_M6.71	Datensicherung bei mobiler Nutzung des IT-Systems	
BSIGrundschutz_M6.78	Datensicherung unter Windows Clients	
BSIGrundschutz_M6.79	Datensicherung beim Einsatz von Internet-PCs	
BSIGrundschutz_M6.81	Erstellen von Datensicherungen für Novell eDirectory	
BSIGrundschutz_M6.84	Regelmäßige Datensicherung der System- und Archivdaten	
BSIGrundschutz_M6.87	Datensicherung auf dem IIS	
BSIGrundschutz_M6.90	Datensicherung und Archivierung von E-Mails	
BSIGrundschutz_M6.91	Datensicherung und Recovery bei Routern und Switches	
BSIGrundschutz_M6.95	Ausfallvorsorge und Datensicherung bei PDAs	

Tabelle A.19: Regeln für die Aktivität *Sicherung* - Teil 2

A.3.8 Löschung

```
SELECT      ?Regel ?Name ?Objekt
WHERE       {{ :Loeschung :istAktivitaetIn ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}
            UNION {{ :Loeschung :hatGefaehrdung ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
            UNION {{ :Loeschung :hatMassnahme ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
            UNION { :Loeschung :benutztObjekt ?Objekt.
            ?Objekt ?Relation ?Regel.
            OPTIONAL { ?Regel rdfs:label ?Name.}}}
ORDER BY ASC (?Regel)
```

Regel	Name	Objekt
BDSG_P11	Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag	
BDSG_P20	Berichtigung, Loeschung und Sperrung von Daten; Widerspruchsrecht	
BDSG_P30	Geschaeftsmaeßige Datenerhebung und -speicherung zum Zweck der Uebermittlung in anonymisierter Form	
BDSG_P35	Berichtigung, Loeschung und Sperrung von Daten	
BDSG_P6	Rechte des Betroffenen	
BSIGrundschutz_B1.15	Löschen und Vernichten von Daten	
BSIGrundschutz_G3.25	Fahrlässiges Löschen von Objekten	
BSIGrundschutz_G5.106	Unberechtigtes Überschreiben oder Löschen von Archivmedien	
BSIGrundschutz_M2.167	Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten	
BSIGrundschutz_M2.431	Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen	
BSIGrundschutz_M2.432	Richtlinie für die Löschung und Vernichtung von Informationen	
BSIGrundschutz_M2.433	Überblick über Methoden zur Löschung und Vernichtung von Daten	
BSIGrundschutz_M2.434	Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern	
BSIGrundschutz_M3.67	Einweisung aller Mitarbeiter über Methoden zur Löschung oder Vernichtung von Daten	

Tabelle A.20: Regeln für die Aktivität *Löschung*

Abbildungsverzeichnis

1.1 Ausschnitt aus der *Security Ontology* . . . 4
1.2 Anwendungsszenario aus [SBO07] . . . 4
1.3 Semantische *Ereignisgesteuerte Prozesskette* [TF06b] . . . 5

2.1 Beispiel-Ontologie . . . 16
2.2 Traditionelle Ontologiesprachen aus [GPFLC04] . . . 18
2.3 Markup Languages aus [CFLGP03] . . . 19

3.1 Regelwerke . . . 23
3.2 Übersicht über die MaRisk VA . . . 25
3.3 Modellierung der Regeln . . . 26
3.4 Relationen für die Regelwerke und Regeln mit ihren inversen Relationen . . . 27
3.5 Elemente der Regelwerke . . . 33
3.6 Relationen zwischen den Regelelementen . . . 36
3.7 Relationen zwischen den Regelwerken und Regelelementen . . . 38
3.8 Relationen für Maßnahmen und Gefährdungen . . . 39
3.9 Gesamtaufbau der Ontologie . . . 44

4.1 Die vier Tools nach der Vorauswahl . . . 48
4.2 Übersicht über die Anforderungen . . . 53
4.3 Übersicht über die wichtigen Anforderungen . . . 53
4.4 Amine Baumansicht . . . 55
4.5 Amine Grafikansicht . . . 55
4.6 Hozo . . . 56
4.7 NeOn Toolkit . . . 57
4.8 Protégé mit Plugin Jambalaya . . . 58
4.9 Bewertung der Tools . . . 59
4.10 Oberfläche von Protégé-OWL . . . 61

5.1 Benennung der Instanzen der Regeln . . . 64
5.2 Relationen mit weiteren Eigenschaften . . . 65
5.3 Geschäftsprozess Dokumentieren . . . 73
5.4 Zuordnung der Aktivitäten . . . 73

Literaturverzeichnis

[BCBG05] Benjamins, V.R., P. Casanovas, J. Breuker und A. Gangemi: *Law and the Semantic Web, an Introduction.* Law and the Semantic Web, LNAI 3369:1–17, 2005.

[Ber] Bergman, M. K.: *Sweet Tools - Simple List.* http://www.mkbergman.com/sweet-tools-simple-list/. Besucht im Juli 2011.

[Ber10] Bergman, Michael K.: *The Sweet Compendium of Ontology Building Tools.* http://www.mkbergman.com/862/the-sweet-compendium-of-ontology-building-tools/, Januar 2010. Besucht im Juli 2011.

[BLHL+01] Berners-Lee, T., J. Hendler, O. Lassila et al.: *The Semantic Web.* Scientific American, 284(5):34–43, 2001.

[Bos11] Bostan, Elena-Crina: *Formale Abbildung von regulatorischer Compliance auf Security Policies.* Diplomarbeit TU Dortmund, 2011.

[Bra11] Brand, Dr. Kurt: *Internet-Sicherheit 2011: Eine Umfrage des eco Arbeitskreises Sicherheit*, Januar 2011.

[BSIa] BSI: *IT-Grundschutz-Kataloge, Standard-Sicherheitsmaßnahmen.* https://www.bsi.bund.de/gshb. Besucht am: 06.07.2011.

[BSIb] BSI: *Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz (11.EL).* https://www.bsi.bund.de/. Seit August: Nur noch Tabelle für 12.EL.

[BSI08a] BSI: *IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2.* www.bsi.bund.de, Mai 2008. Version 2.0.

[BSI08b] BSI: *Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1.* www.bsi.bund.de, Mai 2008. Version 1.5.

[BSI08c] BSI: *Notfallmanagement, BSI-Standard 100-4.* www.bsi.bund.de, November 2008. Version 1.0.

[BSI08d] BSI: *Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3.* www.bsi.bund.de, Mai 2008. Version 2.5.

[Cas08] Casellas, N.: *Modelling Legal Knowledge through Ontologies. OPJK: the Ontology of Professional Judicial Knowledge.* Doktorarbeit, Autonomous University of Barcelona, 2008.

[CFLGP03] Corcho, O., M. Fernández-López und A. Gómez-Pérez: *Methodologies, Tools and Languages for Building Ontologies. Where Is Their Meeting Point?* Data & knowledge engineering, 46(1):41–64, 2003.

[CS06] Cardoso, J. und A.P. Sheth: *Semantic Web Services, Processes and Applications*. Springer, 2006.

[dBG+07] d'Aquin, M., C. Baldassarre, L. Gridinoc, S. Angeletou, M. Sabou und E. Motta: *Characterizing Knowledge on the Semantic Web with Watson*, 2007.

[Den04] Denny, M.: *Ontology Tools Survey, Revisited*, 2004.

[Dod05] Dodds, L.: *Introducing SPARQL: Querying the Semantic Web*, 2005.

[Eik11] Eikenberg, R.: *Hacker ohne Grenzen*. c't - Magazin für Computertechnik, 16:42, 2011.

[ES07] Euzenat, J. und P. Shvaiko: *Ontology Matching*. Springer-Verlag New York Inc, 2007.

[FE09] Fenz, S. und A. Ekelhart: *Formalizing Information Security Knowledge*. In: *Proceedings of the 4th international Symposium on information, Computer, and Communications Security*, Seiten 183–194. ACM, 2009.

[GG95] Guarino, N. und P. Giaretta: *Ontologies and Knowledge Bases*, 1995.

[GPAFL+02] Gomez-Perez, A., J. Angele, M. Fernandez-Lopez, V. Christophides, A. Stutt, Y. Sure et al.: *A Survey on Ontology Tools*, 2002.

[GPFLC04] Gomez-Perez, A., M. Fernández-López und O. Corcho: *Ontological Engineering*, Band 82. Springer, 2004.

[Gru93] Gruber, T.R.: *A Translation Approach to Portable Ontology Specifications*. Knowledge acquisition, 5(2):199–220, 1993.

[Hil08] Hildebrand, Knut: *Compliance & Risk Management*. dpunkt-Verlag, 2008.

[Hur06] Hurley, J.: *The Struggle to Manage Security Compliance for Multiple Regulations*. Computer Security Journal, 22(3):42, 2006.

[Ins09] Institut für Wirtschaftsforschung Halle: *Themenheft: Weltfinanzkrise*. www.iwh-halle.de/d/publik/wiwa/1th-09.pdf, 2009.

[ISO05a] ISO/IEC JTC1/SC27: *ISO/IEC 27001:2005 „Information technology – Security techniques – Information security management systems – Requirements“*, 2005.

[ISO05b] ISO/IEC JTC1/SC27: *ISO/IEC 27002:2005 „Information technology – Security techniques – Code of practice for information security management“*, 2005.

[ISO08] ISO/IEC JTC1/SC27: *ISO/IEC 27005:2008 „Information technology – Security techniques – Information security risk management“*, 2008.

[JU99] Jasper, R. und M. Uschold: *A Framework for Understanding and Classifying Ontology Applications.* In: *Proceedings 12th Int. Workshop on Knowledge Acquisition, Modelling, and Management KAW*, Band 99, Seiten 16–21, 1999.

[Kal11] Kalenda, Florian: *Umfrage: Zwei Drittel der mittelständischen Unternehmen ohne Compliance-Konzept.* http://www.zdnet.de/news/41549037/umfrage-zwei-drittel-der-mittelstaendischen-unternehmen-ohne-compliance-konzept.htm, Februar 2011. Besucht am 11.10.11.

[KJ97a] Kitchenham, B. und L. Jones: *Evaluating Software Engineering Methods and Tools Part 7: Planning Feature Analysis Evaluation.* ACM SIGSOFT Software Engineering Notes, 22:21–24, 1997.

[KJ97b] Kitchenham, B. und L. Jones: *Evaluating Software Engineering Methods and Tools Part 8: Analyzing a Feature Analysis Evaluation.* ACM SIGSOFT Software Engineering Notes, 22:10–12, 1997.

[KJ97c] Kitchenham, B.A. und L. Jones: *Evaluating Software Engineering Methods and Tool Part 5: The Influence of Human Factors.* ACM SIGSOFT Software Engineering Notes, 22:13–15, 1997.

[KJ97d] Kitchenham, B.A. und L. Jones: *Evaluating Software Engineering Methods and Tools Part 6: Identifying and Scoring Features.* ACM SIGSOFT Software Engineering Notes, 22:16–18, 1997.

[KKIM02] Kozaki, K., Y. Kitamura, M. Ikeda und R. Mizoguchi: *Hozo: An Environment for Building/Using Ontologies Based on a Fundamental Consideration of „Role“ and „Relationship“*, 2002.

[KRS08] Kersten, H., J. Reuter und K.W. Schröder: *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz.* Vieweg+ Teubner, 2008.

[KSKM05] Kozaki, K., E. Sunagawa, Y. Kitamura und R. Mizoguchi: *Hozo: an Ontology Development Environment-Treatment of „Role Concept“ and Dependency Management.* In: *Galway, Ireland: Proc of Posters and Demos of the 4th International Semantic Web Conference.* Citeseer, 2005.

[MPSP+09] Motik, B., P.F. Patel-Schneider, B. Parsia, C. Bock, A. Fokoue, P. Haase, R. Hoekstra, I. Horrocks, A. Ruttenberg, U. Sattler et al.: *OWL 2 Web Ontology Language: Structural Specification and Functional-Style Syntax*, 2009.

[MVH+04] McGuinness, D.L., F. Van Harmelen et al.: *OWL Web Ontology Language Overview.* W3C recommendation, 10:2004–03, 2004.

[NCY] Norta, A., L. Carlson und R. Yangarber: *Utility Survey of Ontology Tools.*

[Neb99] Nebel, B.: *Frame-Based Systems*, 1999.

[NFF+91] Neches, R., R.E. Fikes, T. Finin, T. Gruber, R. Patil et al.: *Enabling Technology for Knowledge Sharing.* AI magazine, 12(3):36, 1991.

[RFP08] Rebstock, M., J. Fengel und H. Paulheim: *Ontologies-Based Business Integration.* Springer Verlag, 2008.

[SBO07] Schmidt, R., C. Bartsch und R. Oberhauser: *Ontology-based Representation of Compliance Requirements for Service Processes.* In: *Proceedings of the Workshop on Semantic Business Process and Product Lifecycle Management (SBPM 2007)*, 2007.

[Sch10] Schmidt, J.: *BaBaBanküberfall.* c't - Magazin für Computertechnik, 22:42, 2010.

[Sch11] Schmidt, J.: *Sicherheit:mangelhaft.* c't - Magazin für Computertechnik, 4:35, 2011.

[Sow91] Sowa, J.F.: *Principles of Semantic Networks*, 1991.

[Tec] Techwiki: *Ontology Tools.* http://techwiki.openstructs.org/index.php/Ontology_Tools. Besucht im Juli 2011.

[TF06a] Thomas, O. und M. Fellmann: *Semantische Ereignisgesteuerte Prozesssketten*, 2006.

[TF06b] Thomas, O. und M. Fellmann: *Semantische Integration von Ontologien und Ereignisgesteuerten Prozessketten.* In: *EPK*, Band 5, Seiten 7–23, 2006.

[TF07] Thomas, O. und M. Fellmann: *Semantic Business Process Management: Ontology-based Process Modeling Using Event-driven Process Chains.* International Journal of Interoperability in Business Information Systems, 2(1):29–43, 2007.

[TFM09] Thomas, O. und M. Fellmann MA: *Semantische Prozessmodellierung–Konzeption und informationstechnische Unterstützung einer ontologiebasierten Repräsentation von Geschäftsprozessen.* Wirtschaftsinformatik, 51(6):506–518, 2009.

[TT07] Teschl, G. und S. Teschl: *Mathematik für Informatiker: Band 1: Diskrete Mathematik und Lineare Algebra.* Springer, 2007.

[Val05] Valente, A.: *Types and Roles of Legal Ontologies.* Law and the Semantic Web, LNAI 3369:65–76, 2005.

[WNR+06] Wang, H.H., N. Noy, A. Rector, M. Musen, T. Redmond, D. Rubin, S. Tu, T. Tudorache, N. Drummond, M. Horridge et al.: *Frames and OWL Side by Side.* In: *Presentation Abstracts*, Seite 54, 2006.

Erklärung

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 24. November 2011

Einverständniserklärung des Urhebers

Hiermit erkläre ich mich einverstanden, dass meine Diplomarbeit nach §6(1) des URG der Öffentlichkeit durch die Übernahme in die Bereichsbibliothek zugänglich gemacht wird.
Damit können Leser der Bibliothek die Arbeit einsehen und zu persönlichen wissenschaftlichen Zwecken Kopien aus dieser Arbeit anfertigen. Weitere Urheberrechte werden nicht berührt.

Dortmund, den 24. November 2011