Ein Meta-Risiko-Datenmodell für IKT

Martin Latzenhofer

Austrian Institute of Technology
Digital Safety & Security Department

Universität Wien – Fakultät für Informatik
Forschungsgruppe Multimedia Information Systems
martin.latzenhofer@ait.ac.at

Zusammenfassung

Risikomanagement in der Informations- und Kommunikationstechnologie (IKT) ist geprägt durch eine Vielzahl unterschiedlicher Methoden und Modelle, die durch ähnliche Aspekte, aber dennoch im Detail differierende Strukturen und Vorgehensweisen gekennzeichnet sind. Dies führt dazu, dass Organisationen, wenn sie IKT-Risikomanagement betreiben möchten oder müssen, zunächst einen hohen Initialaufwand zu investieren haben, um überhaupt die Voraussetzungen in Form von anwendbaren Risikomodellen, Risikoprozessen und Setups für ihre aktuell zu bewertende Situation inklusive der Datenaufbereitung und Verarbeitung mit IKT-Tools zu schaffen. Um diesen Initialaufwand entgegen zu wirken, nimmt dieser Beitrag einen Metamodellierungsansatz aus dem Umfeld von Disaster Recovery als Anregung und postuliert ein Meta-Datenmodell für IKT-Risikomanagement. Ausgehend von den gängigen Frameworks und Standards aus dem Bereich Risikomanagement werden Forschungsansätze und ein erster Entwurf eines Unified-Modeling-Language-Schemas (UML) für das Meta-Risiko-Datenmodell vorgestellt. Eine Beschreibung der geplanten weiteren Aktivitäten zur Ausformulierung und Verfeinerung des hier vorgestellten Meta-Risiko-Datenmodells schließen den Beitrag ab.

1 Einleitung

1.1 Ausgangssituation und grundlegende Begriffe

Risiko bezeichnet die „Auswirkungen von Unsicherheit auf Ziele, Tätigkeiten und Anforderungen“ [Aust14], wobei diese Auswirkungen grundsätzlich zumeist negativ angesehen werden und die Unsicherheit bezüglich ihres Eintretens mit einer entsprechenden Wahrscheinlichkeit eingeschätzt wird. Risiko versteht sich daher als Folge von Ereignissen oder Entwicklungen [Aust14, Inte09].

Risikomanagement hat das Ziel, eine Organisation im Umgang mit Risiken zu koordinieren und zu steuern, wobei im Rahmen des zugehörigen Risikomanagement-Prozesses konkrete Risiken identifiziert, analysiert, bewertet, bewältigt sowie aufgezeigt, verfolgt, kommuniziert und überwacht werden [Aust14]. Risikomanagement als prozessualer, einzelorganisationsspezifischer Ansatz hat somit die strukturelle Behandlung des wahrscheinlichen Eintritts und die damit zusammenhängende ex ante Ausarbeitung und Vorbereitung von wirkungsvollen Maßnahmen zur Minimierung eines Risikos respektive eines kompletten Risikobildes zum Ziel.

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 161-173.

Diese Einforderung einer intensivierten Betrachtung von Risikomanagement wirkt sich auch auf IKT und damit ebenso auf die erbringenden IKT-Organisationen aus. Aufgrund ihrer angenommenen inhärenten Charakteristik – Einsatz komplexer Technologien, Blackbox-Tendenz, spezifisches Knowhow, hoher Grad an Abhängigkeit für andere Geschäftsbereiche, welche diese IKT-Services nutzen und ihre Entscheidungen auf diesen aufbauen – entsteht ein signifikantes Gefährdungspotential. Die Möglichkeit des Versagens von IKT – sei es willentlich oder unwillentlich herbeigeführt – und die damit einhergehenden weitreichenden negativen Folgen treten als konkretes Risiko stark in den Vordergrund. Extensive organisationsübergreifende Risikobetrachtungen erfolgen für spezifische Branchen oder Themen (z.B. Finanzwirtschaft, Energiewirtschaft, kritische Infrastrukturen, etc.). Diese sind jedoch erfahrungsgemäß weder rein auf IKT bezogen, noch wird eine Gesamtsicht unter Einbeziehung mehrerer IKT-Organisationen entwickelt. Diese nicht organisationsübergreifende Ausrichtung mag sich zwar mit der typischen Querschnittsfunktion von IKT argumentieren lassen (IKT fungiert als ein Enabler für andere, höhere Zwecke), sie wirkt jedoch zu einschränkend. Rein praktisch ist eine solche Ausrichtung aufgrund der individuellen Risikomanagement-Ansätze der einzelnen IKT-Organisationen und des Generierens von somit nicht vergleichbaren Basisdaten schwer zu überwinden. Dementsprechend spezifisch und differenziert ist die jeweils angewendete Methodik, die dann in weiterer Folge zu einer großen Zahl an unterschiedlichen Modellen führt. Signifikant ins Gewicht fällt auch, dass Organisationen beim Aufbau von Risikomanagementstrukturen einen hohen Initialaufwand zu leisten haben, das Prinzip der Wiederverwendbarkeit von bereits bewährt eingesetzten Teilen – etwa aus anderen Organisationen – nicht erschöpfend zur Anwendung kommt. Eine Vergleichbarkeit der Vorgehensweisen und der Ergebnisse über die engen Grenzen einer einzelnen IKT-Organisation hinweg ist nicht hinreichend gegeben.

1.2 Integrationsbedarf

Die vorhandenen Methoden und Modelle werden in der wirtschaftlichen Praxis je nach dem Grad der zumeist extrinsischen Motivation der Organisation angewendet und innerhalb der Organisationsgrenzen verwertet. Jedoch werden diese Methoden und Modelle anschließend weder zusammengeführt noch wird eine übergeordnete Sichtweise etabliert. Die Konfiguration, das Setup und die Nutzbarmachung der Modelle sind für die Organisationen nicht wiederholbar, also nicht prozesshaft einsetzbar. Was in der momentanen Praxis und der Forschung fehlt, ist ein übergeordnetes, gemeinsames und möglichst generisch formuliertes Meta-Risiko-Modell, das eine Zusammenführung – und somit eine Vergleichbarkeit – aller risiko-relevanten und IKT-bezogenen Informationen inklusive bisher rein organisationsspezifischer Ergebnisse zulässt. Ein konsistentes Meta-Risiko-Modell für den IKT-Bereich in Kombination mit einer unmittelbar anwendbaren Datenstruktur ermöglicht diesen geforderten Datentransfer, eine Datenzusammenführung sowie Vergleiche auf übergeordneter Ebene. Die explizite Darstellung des Meta-Risiko-Modells als Datenmodell wird hier in weiterer Folge als Meta-Risiko-Datenmodell bezeichnet.

Im Rahmen des im österreichischen Sicherheitsforschungsprogramm KIRAS durchgeführten Projekts „MetaRisk“ [Bund00] wurde bereits versucht, eine sensorunterstützte Risikoanalyse inklusive -managementsystem zu entwerfen. Ziel war es, ein workflow-unterstütztes, operatives Lagebild darzustellen und so Entscheidungsunterstützung für Organisationen zu bieten. Im Gegensatz zum Projekt „MetaRisk“ bezieht sich der hier verfolgte Ansatz rein auf IKT-Risikomanagement. Das entwickelte Meta-Risiko-Modell bleibt dabei nicht ausschließlich auf generischer Ebene, sondern fokussiert auf die Entwicklung und Darstellung eines UML-Datenmodells, um so eine unmittelbare IKT-Anwendung zu ermöglichen.

1.3 Voraussetzungen für effektive Lösungsansätze

Zunächst ist zu verifizieren, ob und in welcher Weise von den bestehenden Voraussetzungen in der IKT ausgehend ein übergeordnetes Meta-Risiko-Datenmodell entworfen werden kann, das in der Lage ist, weitgehend flexibel die Spezifika der zugrunde liegenden IKT-Risikomanagementmethoden aufzunehmen und nichtsdestotrotz hinreichend abstrahiert und generisch formuliert ist, um schließlich eine konsistente Einbettung in den Kontext bestehender Risikomanagementmodelle zu gewährleisten.

Die aktuell in der IKT angewendeten Frameworks und Standards bilden die grundlegende Basis für die Entwicklung des Meta-Risiko-Datenmodells. Dieses hat den Anspruch, die jeweils ähnlichen Schlüsselaspekte und Zusammenhänge dergestalt generisch zu formulieren, dass die bestimmten Risikomodelle, welche durch die oben erwähnten Frameworks und Standards propagiert werden, als konkrete Instanzen dieses Meta-Risiko-Datenmodells für IKT-Risikomanagement dargestellt werden können. Dazu bedient es sich eines Metamodellierungsansatzes, um über die Einführung einer übergeordneten Abstraktionsebene eine gemeinsame Datenbasis zu schaffen. Die Auswahl der betrachteten IKT-Risikomodelle orientiert sich dabei an deren Relevanz in der Praxis und soll die am häufigsten in der IKT angewendeten Modelle umfassen. Nachdem die im wirtschaftlichen Umfeld eingesetzten Risikomanagement-Modelle für IKT stark etabliert sind, ist eine Ablösung durch ein neues, umfassendes Modell weder realistisch noch zielführend, was den hier verfolgten Ansatz vielversprechend und praxisorientiert erscheinen lässt. Der Beitrag schlägt ein Meta-Risiko-Datenmodell vor, das prinzipiell auf viele bekannte Risikomanagementframeworks anwendbar sein soll. Dadurch wird – falls sich das Vorgehen als praxistauglich erweist – ein erheblicher Mehrwert geschaffen, da nun die Modellierung der Risiken unabhängig von der Kenntnis der einzelnen Frameworks erfolgen kann.

Ein kritischer Erfolgsfaktor ist die Wahl der Detailebenen bei der Modellierung, da durch die Abstraktion mitunter Informationsverlust einhergeht. Trotzdem muss sichergestellt werden, dass alle relevanten Daten im übergeordneten Modell enthalten und semantisch korrekt verknüpft sind. Für den betrachteten IKT-Bereich soll explizit eine IKT-orientierte Lösung erarbeitet werden. Das Meta-Risiko-Modell wird somit konsequenterweise unmittelbar als Datenmodell dargestellt. Durch diesen Ansatz erfolgt ein integrativer Brückenschlag von den spezifischen IKT-Risikomanagement-Modell(en) in ein übergeordnetes Meta-Risiko-Datenmodell. Die unmittelbare Darstellung als Datenmodell differenziert sich von anderen Metamodellierungsansätzen und soll zusätzlich die unmittelbare IKT-Anwendung in der Praxis sicherstellen. Eine Validierung mit IKT-Mitteln erscheint so einfach und transparent machbar.

Der vorliegende Artikel gliedert sich nach dieser Themeneinführung in einem zweiten Kapitel in eine Diskussion der IKT-Perspektiven, eine Kurzvorstellung der in der IKT gängigen Risikomanagementframeworks und schließt mit einem möglichen Lösungsansatz über Metamodellierung ab. Im dritten Kapitel wird nach der Formulierung der grundsätzlichen Anforderungen an das Datenmodell das initiale Meta-Risiko-Modell vorgestellt und die Hauptkomponenten beschrieben. Der Beitrag endet mit einem Ausblick auf die unmittelbar bevorstehenden nächsten Schritte, um diesen Ansatz weiter zu vertiefen.

2 State of the Art

2.1 IKT-orientierte Perspektiven

Die im Meta-Risiko-Modell verwendete Perspektive beschränkt sich auf den Anwendungsbereich IKT, was eine deutliche Komplexitätsreduktion bedeutet. Die etablierten und anerkannten Frameworks und Standards, die im IKT-Umfeld eingesetzt werden, wurden explizit für die Anwendung in diesem Bereich entwickelt und betrachten typische IKT-Bedrohungsbilder und somit zu einem großen Teil reine IKT-Risiken. Diese Frameworks und Standards stellen unterschiedliche Methoden vor, die wiederum zu verschiedenen Modellen führen. Im Rahmen der vorzunehmenden Analyse werden diese Modelle auf mögliche gemeinsame Schlüsselaspekte hin untersucht. Durch diese Bottom-Up-Herangehensweise wird sukzessive ein Meta-Risiko-Modell aufgebaut, das durch die Objekte dieser Modelle und deren Beziehungen untereinander beschrieben wird.

Im wirtschaftlichen Umfeld werden vielfach externe Berater, die aus mehreren vergangenen Projekten und Aufträgen persönliches Wissen aufgebaut haben, engagiert, um ein Risikomanagement für IKT aufzusetzen, zu erweitern oder anzupassen. Ein Berater setzt dann die Methode situationsangepasst für den Kunden individuell auf und kann so – aus methodischer Sicht – den ressourcenintensiven Setup-Aufwand de facto nicht reduzieren. Im Gegensatz dazu ermöglicht der Einsatz eines Meta-Risiko-Modells durch ein klares und robustes Vorgehen, dass Organisationen, ausgehend von ihrem aktuell angewendeten IKT-Risikomodell, den vorgeschlagenen Lösungsweg mit verringertem Ressourcenaufwand rekapitulieren und so das Meta-Risiko-Modell für ihre spezifischen Risiken effizient anwenden können. Dazu wird vom Datenmodell die erforderliche individuelle Datenstruktur abgeleitet und befüllt.

Inhaltlich deckt das Vorhaben somit den gesamten Prozess des IKT-Risikomanagements ab, d.h., die strukturierte Erfassung der Input-Komponenten (Werte, Gefährdungen, Bedrohungen, Verwundbarkeiten, Eintrittswahrscheinlichkeiten), der Durchführungsaktivitäten (Risikobewertung, die anschließende Risikobehandlung und konkrete Risikoadressierung, das übergeordnete unternehmerische Handeln), der Output-Aspekte (Ereignisse, Kennzahlen, Risikomanagement-Berichte) und deren Zusammenspiel. Eine iterative Prozessperspektive betont den wiederholenden Charakter für einen in der Praxis aufzusetzenden IKT-Risikomanagement-Prozess, um die Annahmen für erwartete Risikoereignisse immer regelmäßig mit den tatsächlichen Vorkommnissen abgleichen zu können. Die dabei erforderlichen Informationen für den Prozessablauf sollen sich generisch im Datenmodell wiederfinden.

2.2 Zentrale Frameworks und Standards

Die IKT-Prozesslandschaft ist geprägt durch verschiedene Frameworks mit unterschiedlichen Ausrichtungen, die eine Vielzahl von Methoden und ihrerseits jeweils eigenständigen Modellen propagieren sowie spezifische Werkzeuge für die Umsetzung vorschlagen. Hierbei sind als etablierte, anerkannte Frameworks und Standards vor allem ISO 3100x [Inte09], ONR 4900x [Aust14], COSO ERM [Comm04a], COBIT for Risk [Info13], NIST [Nati12, Nati10, Nati11], M_o_R [Stat10] und OCTAVE [AlDo01] zu nennen. Die Stoßrichtung dieser Frameworks differiert grundsätzlich und dementsprechend wird auch deren IKT-Risikomanagement-Aspekt mehr oder weniger betont. Jedoch stellen sie allesamt unter anderem rasch anwendbare Risikomanagement-Methoden vor.

Die ISO 3100x [Inte09] der International Organization for Standardization (ISO) [Inte00] hat sich mittlerweile zum weithin akzeptierten globalen Leitnorm für Risikomanagement entwickelt. Durch ihre generische Formulierung ist sie in jeder Organisation, unabhängig von ihrer Art, Ausrichtung oder Größe, universell einsetzbar. Der bipolare Aufbau adressiert einerseits die Schaffung eines iterativen, am Qualitätsmanagementzyklus Plan-Do-Check-Act orientierten, Risikomanagementrahmens. Andererseits wird die operative Umsetzung des Risikomanagementprozesses, welcher die konkreten Risiken in den organisatorischen Kontext setzt, beurteilt und bewältigt. Über den gesamten Prozesslebenszyklus erfolgt Kommunikation und Überwachung[SPLS15, S.12, 18f].

Die ONR 4900x [Aust14] ist die österreichische Variante von Austrian Standards [Aust00], deren inhaltliche Aspekte aus der ersten Edition zunächst bei der Entwicklung des internationalen Standards ISO 3100x eingeflossen sind, und sich in weiterer Folge in der aktuell gültigen Ausgabe als erweitertes Instrument zur Umsetzung der ISO 3100x-Aspekte in der Praxis versteht. Weite Strecken dieser Norm sind die deutschsprachige Übersetzung der ISO 3100x. Die zweigeteilte Diversifikation in eine operative und strategisch-taktische Ebene ist hier ebenso evident. Im Gegensatz zur ISO 3100x gibt die ONR 4900x konkrete Implementierungsvorschläge für das Risikomanagementsystem, aber auch für den Risikomanagementprozess und seine Subprozesse [Aust08].

Die Publikation des Committee of Sponsoring Organizations of the Treadway Commission (COSO) [Comm00] „Enterprise Risk Management – Integrated Framework“ [Comm04a] ist eine Ergänzung zum ursprünglichen „Internal Control – Integrated Framework“ [Comm12] und trägt der expliziten Ausrichtung auf die Bestimmung, Bewertung und Steuerung von Risiken im Rahmen des Internen Kontrollsystems (IKS) Rechnung. Es behandelt somit die explizite Ausrichtung des IKS auf ein unternehmensweites Risikomanagement. Es besteht aus acht verknüpften interdependenten Komponenten, die für ein vollständiges Funktionieren von Risikomanagement in der Organisation vorhanden sein müssen, und verfolgt einen iterativen Ansatz zur Schaffung von Risikomanagementstrukturen. Auch hier kommen Abstraktionsebenen zur Anwendung. Der erste Teil, das Rahmenwerk, beschreibt Prinzipien und Konzepte, und enthält Guidelines für Führungskräfte in der Organisation, um eine kontinuierliche Verbesserung der Risikomanagementstrukturen zu erreichen. Die konkreten Umsetzungsmethoden im zweiten Teil diskutieren notwendige Implementierungsaspekte [Comm04b].

„COBIT for Risk“ [Info13] ist eine spezifische auf Risikomanagement ausgerichtete Publikation der Information Systems Audit and Control Association (ISACA) [Info00]. Ausgehend von der Standardedition von COBIT 5 [Isac12] – dem weitgehend anerkannten Framework für Governance und Management einer Enterprise-IKT mit dem Fokus auf ein funktionierendes Zusammenspiel zwischen IKT- und den klassischen Unternehmenszielen – werden die dort postulierten fünf Prinzipien auf Risiko-Anforderungen ausrichtet und jene für Risikomanagement relevanten Enabler (Prozesse) identifiziert. Erweitert wird dieses Konstrukt um eine Sammlung von 111 IKT-Risiko-Szenarien, die sowohl top-down von den Geschäftszielen als auch bottom-up von generischen Szenarienbeschreibungen entwickelt werden und dafür Response-Maßnahmen vorschlägt. Auch hier findet sich eine Zweiteilung zwischen der Risikomanagementperspektive (strategisch-taktisch) und der Risikomanagementfunktion (operativ) [Info13].

Das US-amerikanische National Institute of Standards and Technology (NIST) [Nati00] beschreibt in deren Special Publications (SP) 800-30 [Nati12], 800-37 [Nati10] und 800-39

[Nati11] die Risikoanalyse und Aktivitäten zur Vorbereitung und Durchführung von Risikoanalysen und berücksichtigt dabei ebenso die laufende Kommunikation der Ergebnisse und der Aufrechterhaltung des Risikoanalyseprozesses. Inhaltlich werden Referenzen und Beispiele für Gefährdungsquellen und Gefährdungsereignisse, Schwachstellen und begünstigende Bedingungen für Risikoereignisse, Kriterien für die Schätzung von Eintrittswahrscheinlichkeiten und Auswirkungen, Berechnungsmatrizen sowie Entscheidungshilfen für die Evaluierung von Risiken und die Bereitstellung von Reports behandelt. Bei der Umsetzung der Risikoanalyse durch eine Organisation muss sichergestellt sein, dass die Aktivitäten in den übergeordneten Risikomanagementprozess integriert werden können. Dieser prozessorientierte US-Standard (mit konkreten Prozess-Schritten, Aufgaben und Aktivitäten) ist weniger generisch formuliert und liefert konkrete Spezifikationen für den Aufbau von Risikomanagementstrukturen [Nati12, Nati10, Nati11].

Die Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [AlDo01] ist eine restriktive prozessorientierte Risikomanagementmethode, die vom Software Engineering Institute (SEI) der Carnegie Mellon University [SoCa00] entwickelt wurde. Jeweils drei unterschiedliche Methoden OCTAVE-Method, OCTAVE-S und als jüngste Entwicklung seit 2007 OCTAVE-Allegro [CSYW07] nehmen Rücksicht auf Zielsetzung, Themenbreite und Organisationsgrößen. Das Framework definiert eine umfassende Bewertungsmethode auf Basis einer Risikoanalyse. So werden Schwachstellen und Bedrohungen, die auf die IKT-Infrastruktur wirken, erkannt und die Organisation kann Schutzstrategien entwickeln und Gegenmaßnahmen setzen, um das Gesamtrisiko zu reduzieren. Die drei OCTAVE-Phasen werden je nach Organisationsgröße in fünf bis acht Prozesse unterteilt und von Teams, welche aus Organisationsmitgliedern mit sehr breit ausgelegten Verantwortungen und Kompetenzen bestehen, im Rahmen von Workshops durchgeführt. Ziele, Strukturen und sogar Workshopunterlagen sind vorgegeben [AlDo01, CSYW07].

Das Management of Risk (M_o_R) Framework [Stat10] des ehemaligen britischen Office of Government Commerce (OGC) stellt über sogenannte Prinzipien einen Risikomanagementrahmen auf, der Organisationen helfen soll, ihre Projekte, Programme und Dienstleistungen zu verwalten. Die Hauptstoßrichtung liegt dabei auf der Risikoidentifikation und bei der Entwicklung von Entscheidungshilfen für den Umgang einer Organisation mit Risiken. Aus den Prinzipien wird ein individueller Ansatz entwickelt, der dann mit vier umfangreich beschriebenen Prozessen, welche sich an den Grundprinzipien des Orange Books [Trea04] orientieren, umgesetzt wird [Stat10].

Wiewohl sich die ISO 31000 langsam als führender internationaler Standard für Risikomanagement etabliert, bleiben erfahrungsgemäß in den Organisationen im wirtschaftlichen Umfeld die einmal eingesetzten Methoden aus Praktikabilitätsüberlegungen heraus nachhaltig bestehen. Damit wird die evolutionäre, aus ganzheitlicher Sicht gegenwärtige Sackgasse prolongiert. Es ist evident, dass bei den verschiedenen Frameworks und Standards gemeinsame Schlüsselelemente identifizierbar sind, welche semantisch konsolidiert und danach verallgemeinert auf eine generische Ebene transferiert werden können. Durch das hier vorgestellte Meta-Risiko-Datenmodell soll dies für den Teilbereich IKT geleistet werden.

2.3 Die Notwendigkeit der Metamodellierung

Metamodellierung ist ein flexibler Ansatz, um über die Einführung einer zusätzlichen Abstraktionsebene verschiedenartige Problemstellungen effektiv in Modellen abbilden zu können

[KaKü02, KFHN08]. Dieser Ansatz kommt in IKT insbesondere bei der Entwicklung von Modellierungssprachen sowie im Zusammenhang mit Semantic Web und Business Engineering zur Anwendung. Daraus werden die Voraussetzung für die Interoperabilität und Integration verschiedenartiger domainspezifischer Methoden geschaffen [KaVi11]. Die in den bisherigen Anwendungsbereichen erzielten Vorteile sollen für IKT-Risikomanagement nutzbar gemacht werden, um einerseits die verschiedenen Methoden und Modelle miteinander zusammenzuführen sowie einen gewinnbringenden Informationsaustausch zu gewährleisten und andererseits, um IKT-Risikomanagement unabhängig von spezifischen Einzelmethoden betreiben zu können.

Im Kontext einer Metamodellierungshierarchie [KaKü02] nach [Stra96] und[GeKP98], wie in Abbildung 1 dargestellt, kann das Meta-Risiko-Datenmodell auf Level 2 eingeordnet und über eine Metamodellierungssprache, in diesem Fall UML, beschrieben werden. Die Metamodellierungssprache UML bezieht sich in der Hierarchie in Ebene 3 in weiterer Folge auf das Meta-Model von UML, das selbst über eine korrespondierende Modellierungssprache beschrieben wird; hier somit die Beschreibungssprache für das UML-Metamodell selbst. Am unteren Ende des Konstrukts auf Level 1 wird ein konkretes Framework, etwa COBIT for Risk, dabei als das Modell bezeichnet, die Modellierungssprache ist in dem Fall eine semi-narrative Beschreibung (im Sinne der Framework-Publikationen). Das Original kann nun als eigentlicher Anwendungsfall (den Use Cases) interpretiert werden, also etwa die Risikobetrachtung eines Telekommunikationsnetzwerkes durch einen Betreiber, der das Risikomodell von COBIT for Risk anwendet. Die Abstraktion erfolgt über einen Klassifikationsprozess, die Verringerung der Modellierungsebene leistet Instanziierung. Die Modellebene auf Level 1 soll austauschbar sein – also andere Frameworks und Standards (z.B. COSO oder ISO 31000) dafür eingesetzt werden, wobei gemäß der Zielsetzung die Metamodellebene auf Level 2 unverändert bleiben soll.

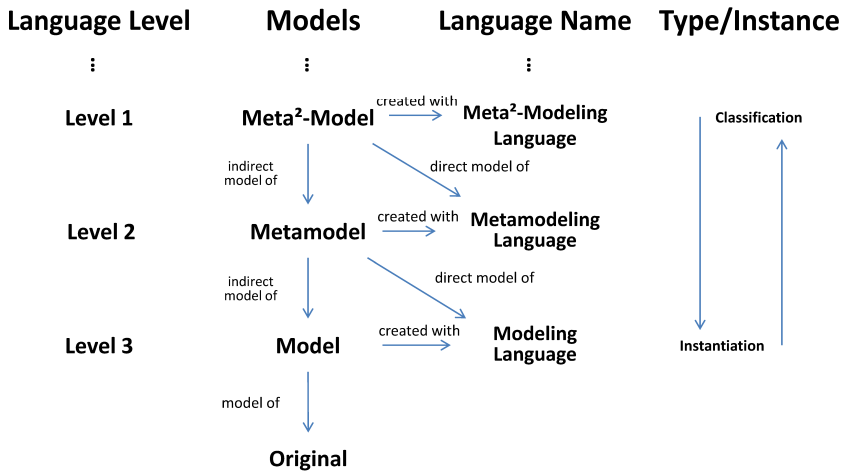

Abb. 1: Metamodellierungshierarchien [KaKü02, S.174]

Der Metamodellierungsansatz wurde bereits durch Othman und Beydoun in [OtBe10] für den Bereich Disaster Recovery aufgegriffen. Darin wurde ein Metamodell entworfen, für spezielle Katastrophensituationen (Erdbeben, Nuklearvorfall) abgeleitet und auf zwei verschiedene praktische Anwendungsfälle (Christchurch-Erdbeben 2010, Fukushima/Tsunamibedrohung 2011) hin verifiziert [OtBe10]. Diese Leitidee wird im vorliegenden Ansatz übernommen, um spezielle Gegebenheiten im IKT-Risikomanagement und die verfügbaren Modelle aus den bereits in IKT in Verwendung befindlichen Frameworks und Standards in einem Meta-Risiko-Datenmo-

dell zu repräsentieren. Die praktischen Anwendungsfälle, welche über die Meta-Ebene dargestellt werden sollen, sind spezifische Use Cases aus dem IKT-Risikomanagement von Unternehmen. Gelingt dieser Ansatz, wird eine gemeinsame Informationsbasis geschaffen und eine organisationsübergreifende Perspektive kann eingenommen werden, ohne die in der Praxis etablierten Methoden und Modelle radikal ersetzen zu müssen.

Das Meta-Risiko-Datenmodell soll in weiterer Folge gegenwärtig etablierte Risikomodelle generisch darstellen können – im angestrebten Idealfall bilden sie Instanzen des Meta-Risiko-Datenmodells. Die Sicherstellung eines konsistenten Strukturaufbaus, einerseits zwischen den bereits bestehenden Modellen und dem zu formulierenden Meta-Risiko-Modell, andererseits zwischen dem korrespondierenden logischen Strang vom generischen Datenmodell zur konkreten Datenstruktur für das Ablegen der Daten aus dem konkreten Risikomanagementmodell, steht im primären Fokus des Ansatzes, da dies die Voraussetzung für eine ganzheitliche (Meta-)Sicht darstellt und so die geforderte Integration der Modelle umsetzt.

3 Anforderungen an das Meta-Risiko-Datenmodell

3.1 Generelle Anforderungen

Die Formulierung des Meta-Risiko-Modells als Datenmodell muss zusammengefasst fundamentalen Anforderungen genügen. Zum einen sollen die wichtigsten IKT-Risikomanagement-Frameworks (wie unter Abschnitt 2.2 vorgestellt) als Instanzen abgebildet werden können. Somit ist sichergestellt, dass die bereits in der Organisation etablierten Risikomanagementmodelle und die davon abgeleiteten Methoden weiter angewendet werden können. Durch die Verifikation der Abbildungsfähigkeit konkreter Risikomanagementmodelle und Anwendung für ausgewählte Use Cases wird wiederum die Tragfähigkeit des angestrebten Meta-Risiko-Modells erhöht. Die Schlüsseldaten für das Risikomanagement werden in das Meta-Risiko-Modell abstrahiert, um dort mit anderen Daten – mitunter aus anderen Risikomanagementmodellen – zusammengeführt oder verglichen zu werden.

Die Funktion des Datentransfers vom instanziierten Modell zum Meta-Risiko-Modell ist die zweite wesentliche Anforderung an das Datenmodell. Dies kann durch jeweils für die einzelnen Risikomanagementmodelle formulierte Transformationsvorschriften erfolgen und wird nicht ohne Informationsverlust ablaufen. Als kritischer Erfolgsfaktor ist dabei die richtig justierte Wahl der Informationsweitergabe zu sehen, die so viel wie nötig und so hinreichend wie möglich Informationen in das Meta-Risiko-Modell speist. Das Austarieren des optimalen Detaillierungsgrades wird dadurch erreicht, dass eine Auswahl von (zunächst drei bis vier) wichtigsten in der IKT eingesetzten Risikomanagementmodellen als konkrete Modellausprägungen herangezogen und verifiziert wird. Dabei gilt zu zeigen, ob das Meta-Risiko-Datenmodell grundsätzlich in der Lage ist, den im Modell geforderten Informationsgehalt als eine Instanz des Meta-Risiko-Modells darzustellen. Durch diese mehrfache Verfeinerung wird die Tragfähigkeit und Robustheit des Meta-Risiko-Datenmodells sukzessive verbessert.

Die unmittelbare Implementierung des Meta-Risiko-Modells als Datenmodell generiert praxisrelevante Vorteile. Der Lösungsansatz und das Datenmodell können umgehend von den Organisationen praktisch angewendet werden, zumal sowohl das Datenmodell vorgegeben und Transformationsvorschriften für das in der Organisation angewendete Risikomanagementmodell formuliert wurden. Diese IKT-Lösung ist auch sofort in der IKT anwendbar, da das Datenmodell direkt vom Meta-Risiko-Modell ableitbar ist, oder vielmehr durch das Datenmodell

selbst dargestellt wird. Die IKT-Risikomanagementaktivitäten können organisationsunabhängig und ressourceneffizient formuliert, ver- und abgeglichen werden. Das Meta-Risiko-Datenmodell selbst fungiert somit als unmittelbare praxisorientierte IKT-Anwendung.

3.2 Initiales Modell

Ein erster Vorschlag für ein Meta-Risiko-Datenmodell ist in Abbildung 2 als Klassendiagramm in UML dargestellt, wobei die *Klassen* kursiv und die Beziehungen zwischen den Komponenten unterstrichen sind. Im Folgenden werden die Klassen und Beziehungen diskutiert und grob in Ebenen kategorisiert.

Das Datenmodell sieht auf der Ebene der Metastruktur sämtliche Objekte als Element *Organisation* und unterteilt diese weiter in *Input*, *Prozess*, *Output* und *Akteure*. Letztere repräsentieren Verantwortlichkeiten und Intervention und das Setzen von Aktivitäten durch Rollen, etwa durch den Risikomanager. Dadurch lassen sich über Generalisierung einheitliche Attribute weitervererben, zudem geben die allgemeinen abstrakten Oberklassen dem Datenmodell eine zusätzliche Struktur.

Die inhaltlich orientierten Klassen auf der Ebene der Einflussfaktoren beziehen sich auf die Abbildung der operativen IKT-Risikomanagement-Inhalte. Eine *Gefährdung* bedroht zunächst eine *Verwundbarkeit* und wird so zur *Bedrohung*, hier als Assoziationsklasse realisiert. Die *Bedrohung* wirkt sich aus auf die Klasse *Wert*, worauf sich die weitere Assoziationsklasse *Auswirkung* bezieht. In Kombination mit der *Eintrittswahrscheinlichkeit* entsteht das *Risiko*. Das *Risiko* muss im Zuge der Prozessablauf-Ebene jedenfalls einer *Bewertung* unterzogen werden. De facto werden die identifizierten Roh-Risiken mit einer subjektiven Bewertung konnotiert, d.h. in *Bewertung* finden sich die bewerteten Risiken dann in Relation zu der gegebenen Einflussfaktoren (Organisation, Unternehmenssteuerung, Risikoeinstellung). Eine etwaige *Maßnahme* behandelt die *Bewertung* (also die zuvor bewerteten Risiken), welche die dritte Assoziationsklasse *Behandlung* hervorbringt. Somit werden ausgehend von den Risiken über die Bewertung hin zur Behandlung Filter gesetzt, die immer überschaubarere Submengen bilden und am Ende nur jene Risiken darstellen, die in weiterer Folge durch den Risikomanagementprozess kontinuierlich behandelt werden. Dadurch soll die Anwendung in der Praxis transparenter und mit geringerer Komplexität dargestellt werden. Die Behandlung wird durch die Klasse *MitigationManagement* beobachtet. Zusätzlich wird durch die Klasse *Ausnutzung* eine Feedbackschleife als Komposition von *Auswirkung* realisiert, welche zusätzlich diese auch noch abstuft und die *Verwundbarkeit* berücksichtigt. Die Klasse *Metrik* aggregiert *Berechnungskomponente* und versucht so, die unterschiedlich angewendeten Metriken abzubilden. Des Weiteren hilft eine Klasse *Kategorisierung*, die diversen Inputobjekte und deren Einteilungen einzubinden. Auch Mehrfachklassifizierungen oder mehrdimensionale Kategorisierungen sollen über eine selbstreferenzierende Beziehung und weiteren Verschachtelungen darstellbar sein. Zusätzlich sind bei den Klassen *Auswirkung*, *Bewertung*, *Behandlung* selbst-referenzierende Beziehungen möglich, um substantielle Auswirkungs-, Risiko- und Maßnahmenanalysen ebenfalls zu berücksichtigen.

Auf der letzten Ebene erfolgen Evaluierungen. Hier beinhaltet die Klasse *Dokumentation* die Klasse *Bericht*, dieser enthält (mehrere) *Kennzahl*(en). Der zweite Aspekt des Berichts erfasst Ereignisse im Zuge der Klasse Risikoereignis. Alle dieser erfassenden, messenden Komponenten sind mit der *CorporateGovernance* verbunden, welchen steuernden Einfluss auf Schlüsselobjekte hat, hier *Bewertung* und *Behandlung* und *MitigationManagement*. Dadurch werden die (Risiko-)Managementaktivitäten ins Datenmodell integriert.

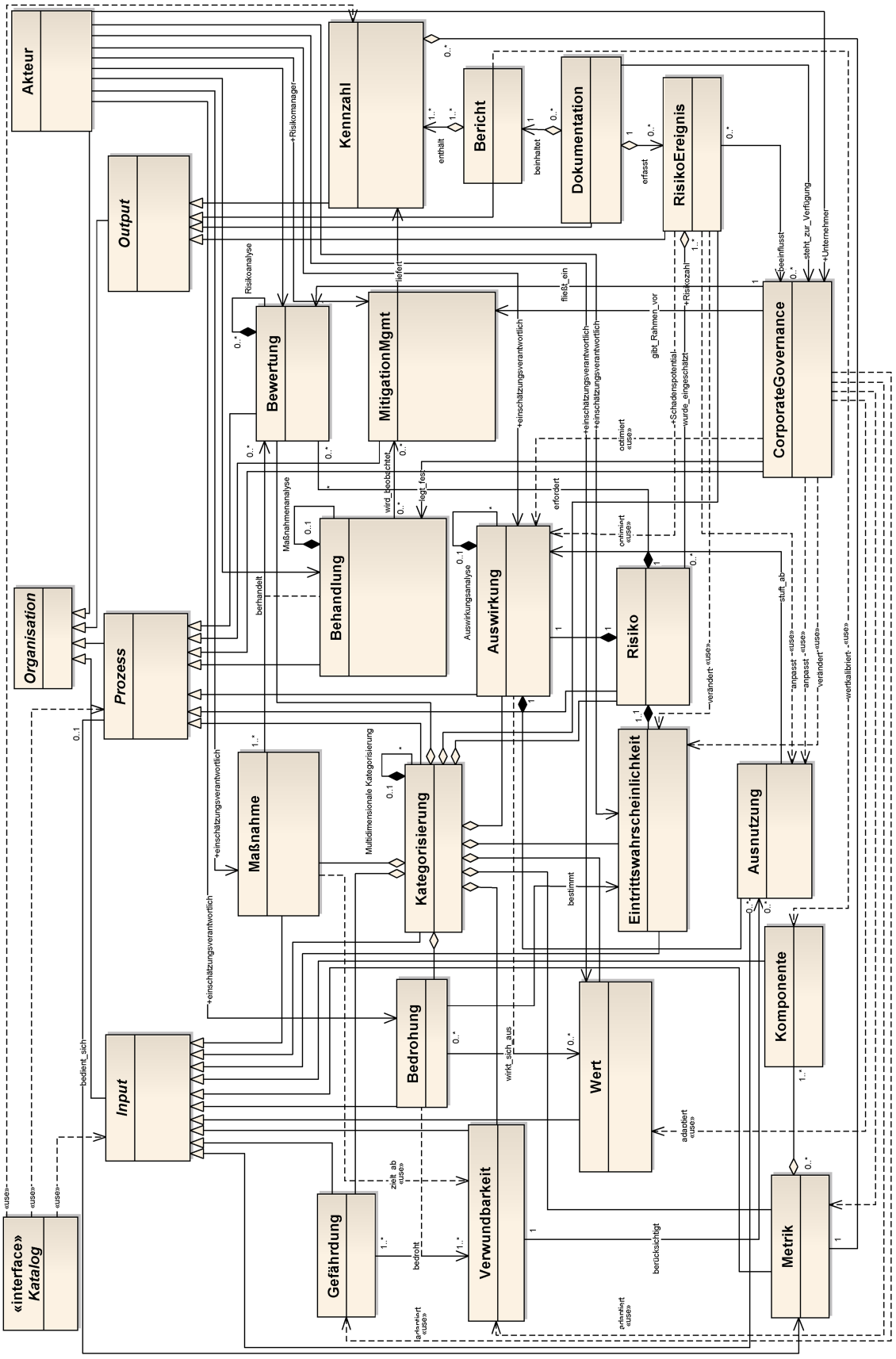

Abb. 2: Vorschlag eines Meta-Risiko-Datenmodells

4 Ausblick

Das hier erstmals postulierte Meta-Risiko-Datenmodell für IKT muss nun in einem nächsten Schritt auf die in Abschnitt 2.2 vorgestellten Frameworks und Standards abgestimmt werden. Die in Abschnitt 3.2 angegebenen Attribute und Methoden in den einzelnen Klassen sind hier ein erster Entwurf und bedürfen noch tiefgreifender Abstimmung. Es wird erwartet, dass das Meta-Risiko-Datenmodell dadurch noch verfeinert wird, insbesondere bei den Attributen und Beziehungen sind Änderungen zu erwarten. Erste konkrete Erfahrungen mit COBIT for Risk als konkretes Framework und die Darstellung des davon abgeleiteten Risikomodells durch das Datenmodell bestätigen grundsätzlich die Klassenstruktur und zeigen, dass der Metamodell-Ansatz für die weitere Forschung vielversprechend ist. Ein Mapping der risiko-spezifischen Control Objectives aus COBIT auf die Klassenstruktur des Meta-Risiko-Datenmodells konnte durchgeführt werden, ohne die inhärente Struktur des Meta-Risiko-Modells wesentlich abändern zu müssen. Weitere Aktivitäten werden zeigen, ob auch andere Risikomodelle sich in die Klassenstruktur harmonisch einfügen lassen.

Als zusätzlichen darauf aufsetzenden Proof of Concept sollen in weiterer Folge spezifische Anwendungsfälle, etwa von kritischen Infrastrukturen herangezogen werden, um die Einsetzbarkeit für die Praxis weiter zu verbessern und einen ersten Praxistest darzustellen. Nach Erreichen einer einsetzbaren Version können Schritte für eine Toolentwicklung identifiziert und die Integration mit einem Management Information System/Enterprise Information System (MIS/EIS) vorbereitet werden.

Außerdem sollen auf Basis der ersten einsetzbaren Version Transformationsvorschriften für die Weitergabe der Daten vom konkret eingesetzten an das übergeordnete Meta-Risiko-Datenmodell erarbeitet werden. Dies mündet schließlich in ein Vorgehensmodell, das es den Organisationen erlauben soll, das Meta-Risiko-Datenmodell ressourcenoptimiert aufzusetzen und die Vorteile einer Abstraktion durch ein Datenmodell – Vergleichbarkeit, Wiederverwendbarkeit, Praxisanwendung, Überwindung der Organisationsgrenzen – zu lukrieren.

Literatur

[AlDo01] C. Albert, A.J. Dorofee: OCTAVE Criteria, Version 2.0, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA (2001)

[Aust00] Austrian Standards Institute: Austrian Standards. https://www.austrian-standards.at/home (abgerufen am 2016-03-25)

[Aust08] ON Fachinformation 06: Risikomanagement für Organisationen und Systeme. In: Austrian Standards Institute – Österreichisches Normungsinstitut (Hrsg.) (2008)

[Aust14] ONR 49000 – Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen – Umsetzung von ISO 31000 in die Praxis. In: Austrian Standards Institute (Hrsg.) (2014)

[Bund00] Bundesministerium für Verkehr, Innovation und Technologie (BMVIT): KIRAS Sicherheitsforschung: MetaRisk. URL http://www.kiras.at/home/. - abgerufen am 2016-03-31

[Comm00] Committee of Sponsoring Organizations of the Treadway Commission: COSO. URL http://www.coso.org (abgerufen am 2016-03-25)

[Comm04a] Enterprise Risk Management – Integrated Framework. In: Committee of Sponsoring Organizations of the Treadway Commission (Hrsg.) (2004)

[Comm04b] Committee of Sponsoring Organizations of the Treadway Commission: Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk, Zusammenfassung (2004)

[Comm12] COSO Internal Control Framework – COSO_InternalControlExternalReporting _September2012.pdf. In: Committee of Sponsoring Organizations of the Treadway Commission (Hrsg.) , AICPA, Durham, New York (2012).

[CSYW07] R.A. Caralli, J.F. Stevens, L.R. Young, W.R. Wilson: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Carnegie Mellon University, Software Engineering Institute (2007)

[GeKP98] R. Geisler, M. Klar, C. Pons: Dimensions and dichotomy in metamodeling : Citeseer, 1998.

[Info00] Information Systems Audit and Control Association: ISACA. https://www.isaca.org/Pages/default.aspx (abgerufen am 2016-03-31)

[Info13] COBIT 5 for Risk. In: Information Systems Audit and Control Association (ISACA) (Hrsg.) , Information Systems Audit and Control Association, Rolling Meadows, IL 60008 USA (2013)

[Inte00] International Organization for Standardization: ISO. http://www.iso.org/iso/home.html (abgerufen am 2016-03-31)

[Inte09] International Organization for Standardization (ISO) (Hrsg.): ISO 31000:2009 Risk management – Principles and guidelines, ISO : ISO, Geneva, Switzerland, 2009.

[Isac12] ISACA: COBIT 5 – Enabling Processes. Rolling Meadows, Illinois, 2012

[KaKü02] D. Karagiannis, H. Kühn: Metamodelling Platforms. In: Bauknecht, K. ; Tjoa, Am. ; Quirchmayr, G. (Hrsg.): E-Commerce and Web Technologies, Lecture Notes in Computer Science. Bd. 2455 : Springer Berlin Heidelberg, 2002, ISBN 978-3-540-44137-3, S. 182.

[KaVi11] D. Karagiannis, N. Visic: Next Generation of Modelling Platforms. In: Perspectives in Business Informatics Research : Springer, 2011, ISBN 3-642-24510-2, S. 19–28.

[KFHN08] D. Karagiannis, H.-G. Fill, P. Höfferer, M. Nemetz: Metamodeling: Some Application Areas in Information Systems. In: R. Kaschek, C. Kop, C. Steinberger; Fliedl, G. (Hrsg.): Information Systems and e-Business Technologies, Lecture Notes in Business Information Processing. Bd. 5 : Springer Berlin Heidelberg, 2008, ISBN 978-3-540-78941-3, S. 175–188

[Nati00] National Institute of Standards and Technology, US Department of Commerce: NIST. URL http://www.nist.gov/. - abgerufen am 2016-03-25

[Nati10] NIST 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. In: National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Joint Task Force Transformation Initiative Information Security (Hrsg.) , Computer Security

Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, USA (2010)

[Nati11] NIST 800-39: Managing Information Security Risk – Organization, Mission, and Information System View. In: National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Joint Task Force Transformation Initiative Information Security (Hrsg.), Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, USA (2011)

[Nati12] NIST 800-30: Guide for Conducting Risk Assessments. In: National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Joint Task Force Transformation Initiative Information Security (Hrsg.) , Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, USA (2012)

[OtBe10] S.H. Othman, G. Beydoun: Metamodelling approach to support disaster management knowledge sharing. Atlanta, GA, USA : AIS Library, 2010, S. 1–10

[SoCa00] Software Engineering Institute ; Carnegie Mellon University: Software Engineering Institute. URL http://www.sei.cmu.edu/. (abgerufen am 2016-03-25)

[SPLS15] S. Schauer, B. Palensky, M. Latzenhofer, M. Stierle: GeRBA Gesamtstaatliche Risiko- und Bedrohungsanalyse, Studie im Rahmen des KIRAS-Forschungsprogrammes, FFG-Projektnummer 845470, Austrian Institute of Technology (2015)

[Stat10] Management of Risk: Guidance for Practitioners. In: The Stationary Office (TSO) (Hrsg.) (2010)

[Stra96] S. Strahringer: Metamodellierung als Instrument des Methodenvergleichs: Eine Evaluierung am Beispiel objektorientierter Analysemethoden: Darmstadt Technical University, Department of Business Administration, Economics and Law, Institute for Business Studies (BWL) (1996)

[Trea04] Her Majesty Treasury: The Orange Book: Management of Risk-Principles and Concepts. In: London: HM Treasury (2004)