Ein informationssicherheitsoptimiertes Geschäftsprozessmanagement-Rahmenwerk für föderierte Organisationsstrukturen

Dissertation

zur Erlangung des akademischen Grades
Doktor-Ingenieur (Dr.-Ing.)

angenommen durch die
Fakultät für Informatik der
Otto-von-Guericke-Universität Magdeburg

vorgelegt von
Erik Neitzel, Master of Science
geb. am 18.03.1986 in Potsdam

Gutachter:
Prof. Dr. Dipl. Wi.-Ing. Klaus Turowski
Prof. Dr. Dipl. Inf. Kai Rannenberg
Prof. Dr. Dipl. Phys. Robert Udo Franz

Magdeburg, 20. Februar 2015

Otto-von-Guericke-Universität Magdeburg

Erik Neitzel

Ein informationssicherheitsoptimiertes Geschäftsprozessmanagement-Rahmenwerk für föderierte Organisationsstrukturen

Ehrenerklärung

Ich versichere hiermit, dass ich die vorliegende Arbeit ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe; verwendete fremde und eigene Quellen sind als solche kenntlich gemacht. Insbesondere habe ich nicht die Hilfe eines kommerziellen Promotionsberaters in Anspruch genommen. Dritte haben von mir weder unmittelbar noch mittelbar geldwerte Leistungen für Arbeiten erhalten, die im Zusammenhang mit dem Inhalt der vorgelegten Dissertation stehen.

Ich habe insbesondere nicht wissentlich:

- Ergebnisse erfunden oder widersprüchliche Ergebnisse verschwiegen,
- statistische Verfahren absichtlich missbraucht, um Daten in ungerechtfertigter Weise zu interpretieren,
- fremde Ergebnisse oder Veröffentlichungen plagiiert,
- fremde Forschungsergebnisse verzerrt wiedergegeben.

Mir ist bekannt, dass Verstöße gegen das Urheberrecht Unterlassungs- und Schadensersatzansprüche des Urhebers sowie eine strafrechtliche Ahndung durch die Strafverfolgungsbehörden begründen kann.

Die Arbeit wurde bisher weder im Inland noch im Ausland in gleicher oder ähnlicher Form als Dissertation eingereicht und ist als Ganzes auch noch nicht veröffentlicht.

Magdeburg, den 25. Juli 2014

Erik Neitzel

Danksagung

Substanziell danke ich meinen Gutachtern Klaus Turowski, Kai Rannenberg und Robert Franz für ihre persönliche, fachliche und formale Unterstützung meines Promotionsvorhabens. Bei einer externen Promotion ist dies nicht selbstverständlich, und die Suche nach einer Betreuung meines sehr speziellen Themas war entsprechend lang.

Robert Franz und Michael Höding gilt darüber hinaus mein großer Dank für die umfassende Unterstützung seit Beginn meines Bachelor-Studiums, über das Master-Studium bis zum heutigen Tag. Rückblickend brachte diese Zeit viel Wandel mit sich, sodass ich für jede Konstante nur dankbar sein kann.

Ein großes Danke richtet sich auch an Sachar Paulus und Knud Brandis für die vielen fachlichen und persönlichen Runden der Konsultation. Zu Beginn meines Master-Studiums wurde hierdurch nicht nur mein Interesse am Thema Governance, Risk und Compliance geweckt. Ich erhielt auch wertvolle Eindrücke in die Praxis, sachdienliche Kritik, vielseitige Unterstützung sowie einen weiträumigen Einblick in das Potenzial meines Promotionsthemas.

Letztlich möchte ich mich bei verschiedenen Personen bedanken, die meinen beruflichen und akademischen Lebensweg positiv beeinflusst haben. Zu nennen sind Andreas Johannsen für die Einblicke in das Beratungswesen, Dietmar Wikarski für die Lehrveranstaltung Systemanalyse, die mir systematisches Laufen beibrachte, Thomas Frambach für den frühen Einblick in die Welt der SAP, Benjamin Schmidt für die vielen unterhaltsamen Stunden der gemeinsamen Lehre und viele weitere Personen, auch in meinem privaten Umfeld, die mich trotz der hohen Auslastung ertragen und mental stabil gehalten haben.

Zusammenfassung

In der vorliegenden Dissertation wird eine Methodik zur Unterstützung der Etablierung und Aufrechterhaltung von Informationssicherheit für föderierte Geschäftsprozesslandschaften entwickelt und evaluiert. Vorhandene relevante Rahmenwerke werden analysiert und dienen als Grundlage zur Erweiterung. Es wird versucht, die organisatorischen Grenzen traditioneller Ansätze zu entfernen, indem ein neues Rahmenwerk entwickelt wird, welches die Geschäftsprozesse und die darin transportierten Informationen vor den mit den Aufgaben in Verbindung stehenden Ressourcen zentralisiert und somit zur Ursachenbehandlung von Sicherheitsvorfällen beiträgt.

Betrachtet man Föderierungen, beispielsweise Unternehmenskooperationen oder langfristige Kunden-Lieferanten-Beziehungen, so stellt sich die Frage nach dem Element, welches als Referenz für den Erhalt eines einheitlichen, d.h. organisationsübergreifenden, Verständnisses des Schutzbedarfs führen kann. Hier manifestiert sich die Kritikalität der zu einem bestimmten Arbeitsschritt gehörenden, transportierten Informationen. Der Schutzbedarf dieser Informationen ist für jede an der Föderation beteiligten Organisation unterschiedlich. Um ein für das Gesamtsystem konsistentes Schutzniveau zu ermöglichen, müssen diese abgeglichen und bestimmte Entscheidungen und Maßnahmen vor Beginn der Etablierung der Zusammenarbeit getroffen und realisiert werden. Entsprechend wird vorliegend ein Modell anvisiert, welches die Entwicklung gemeinsamer Geschäftsprozesskonfigurationen unterstützt.

Traditionelle Ansätze zur Ausrichtung der IT an den Geschäftszielen (wie COBIT), für das IT-Management (wie ITIL) und/oder die Etablierung und Aufrechterhaltung von Informationssicherheit (wie die ISO 27001) adressieren die Entwicklung von Geschäftsprozessen nicht. Gleichzeitig ist die Adressierung von informationssicherheitstechnischen Anforderungen von traditionellen Rahmenwerken zum Geschäftsprozessmanagement (wie ARIS) ebenfalls nicht hinreichend gegeben.

Das resultierende Rahmenwerk etabliert eine Erweiterung der traditionellen Geschäftsprozess-Sichten (auf Ressourcen, Geschäftsinformationen, Geschäftsfunktionen, resultierende Prozesse und erhaltbare Dienstleistungen und Produkte) um informationssicherheitstechnische Informationen, Funktionen und Prozesse, welche als Input für die Entwicklung und/oder der informationssicherheitstechnischen Optimierung von Geschäftsprozessen dienen können. Es entstehen Phasen zur Analyse, der Konzeption, der Implementierung, dem Monitoring und der fortwährenden Verbesserung der resultierenden Geschäftsprozesse, inklusive der eingesetzten technischen Komponenten. Dabei werden Aussagen über zu realisierende Maßnahmen an beteiligten Ressourcen auf Basis der identifizierten Schutzbedarfe der Informationen der beteiligten Kooperationspartner möglich. Hierbei wird Wert darauf gelegt, die Verwendbarkeit verschiedener bestehender Rahmenwerke zu ermöglichen.

Das Modell wird an einem konkreten Anwendungsfall, aufgrund von Komplexität und Verbreitung dem Order-to-Cash Ende-zu-Ende Geschäftsprozess, mit einer konkreten technischen Instanziierung, einer teilweisen mobilen Unterstützung, validiert. Hierbei wird einerseits gezeigt, dass auch die Behandlung nicht föderierter Szenarien deckungsgleiche Ergebnisse zu denen der ISO 27001 liefert. Andererseits wird gezeigt, dass das Problem unterschiedlicher Schutzbedarfe, und somit inkompatibler Schutzniveaus der in der Föderation transportierten Informationen, unter Anwendung des entwickelten Rahmenwerks nicht mehr auftreten. Abschließend wird das Modell einer Akzeptanzprüfung unterzogen.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACL ..... Access Control Lists
ASP ..... Active Server Pages
BPEL ..... Business Process Execution Language
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
BSM ..... Business Service Management
CEO ..... Chief Executive Officer
CMDB ..... Configuration Management Database
COBIT ..... Control Objectives in Information and related Technology
CSA ..... Cloud Security Alliance
ERP ..... Enterprise Resource Planning
GRC ..... Governance Risk Compliance
IaaS ..... Infrastructure as a Service
IS ..... Informationssicherheit
ISACA ..... Information Systems Audit and Control Association
ISM ..... Informationssicherheitsmanagement
ISMS ..... Informationssicherheitsmanagementsystem(e)
ISO ..... International Organization for Standardization
IT ..... Informationsttechnik
ITIL ..... IT Infrastructure Library
ITPM ..... IT Process Quality Management
ITS ..... Informationstechniksicherheit
ITSM ..... IT Service Management

JSP ..... Java Server Pages
KPI ..... Key Performance Indicator(s)
MAT ..... Mensch(en) Aufgabe(n) Technik
MOF ..... Microsoft Operations Framework 4.0
OGSA ..... Open Grid Services Architecture
OO ..... Objektorientierung
OTC ..... Order-to-Cash Geschäftsprozess
PaaS ..... Platform as a Service
PDCA ..... Plan Do Check Act
RACI ..... Responsible Accountable Communicated Informed
SaaS ..... Software as a Service
SCM ..... Supply Chain Management
SLA ..... Service Level Agreement
SOA ..... Service Oriented Architecture
SOAP ..... Simple Object Access Protocol
UCF ..... Unified Compliance Framework
UML ..... Unified Modeling Language
VLBA ..... Very Large Business Application(s)
WKWI ..... Wissenschaftliche Kommission Wirtschaftsinformatik
WSDL ..... Web Service Definition Language
WSLA ..... Web Service Level Agreement
XML ..... Extensible Markup Language

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Dieses Kapitel dient sowohl der Beschreibung der Motivation des vorliegenden Themas, als auch zur Erläuterung von Zielen, Beiträgen und des Vorgehens innerhalb dieser Dissertation.

1.1 Situation

Organisationen sind seit längerer Zeit existenziell abhängig von Informationssystemen, das heißt einer Einheit aus Menschen, Aufgaben und Technik welche Informationen verarbeiten, die für die Instanziierung von Geschäftsprozessen notwendig sind.

Geschäftsprozesse sind eine Folge logisch zusammenhängender Aktivitäten zur Erstellung einer Leistung oder Veränderung eines Objektes. Das Ziel von Prozessen ist die mittel- oder unmittelbare Wertsteigerung und Wertschöpfung. Neben den Aktivitäten müssen die Reihenfolge der Aktivitäten, die die Aktivitäten beeinflussenden Ereignisse, Datenobjekte zur Abwicklung von Aktivitäten sowie Bearbeitungsrollen und Qualitätskriterien definiert sein.

Die für die Unterstützung der Prozesse nötigen Ressourcen, aber auch die Prozesse selbst, unterliegen zusätzlich einer Vielzahl extern und intern definierter Anforderungen. Dies können beispielsweise gesetzliche Auflagen oder Schutzbedarfe für wertvolle Informationen sein, die im Unternehmen verarbeitet werden. Entsprechend müssen diese Anforderungen durch adäquate Maßnahmen adressiert werden. Dieses Problem ist bereits innerhalb

einer einzelnen Organisation äußerst komplex, kann dort jedoch mit den heute vorrätigen Methodiken effizient gelöst werden. Durch das Zusammenspiel externer und interner Prozesse zwischen mehreren Organisationen stellt sich jedoch ein Geflecht weit höherer Komplexität ein.

Dem Problem der effizienten Verarbeitung von Geschäftsprozessen über mehrere Organisation wird zunehmend mit einer föderativen Strategie begegnet. Hierbei werden eigene Prozesse in lokaler Autonomie entwickelt und abgearbeitet. Das globale Zusammenspiel wird auf die notwendige, zu spezifizierende Kommunikation zwischen den beteiligten Organisationen beschränkt. Dies senkt unmittelbar die Komplexität, da die einzelne Organisation stets nur noch die Grenze zur nächsten Organisation beachten muss, jedoch nicht deren interne Einzelprozesse. Dies ist analog zur Prämisse der Kapselung in der Softwareentwicklung.

Geschäftsprozesse haben sich aufgrund dieser Vorteile inzwischen von organisationsspezifischen Prozessen zu organisationsübergreifenden, föderierten Prozessstrukturen entwickelt [Est03] [Sey02], Abbildung 1.1 visualisiert diesen Gedanken.

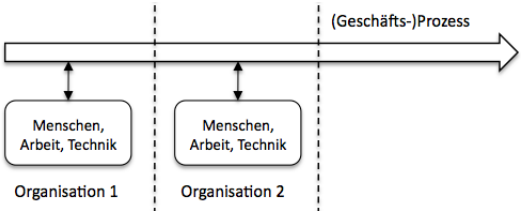

Abbildung 1.1: Föderierte Geschäftsprozesse

Föderative Organisationen teilen das Interesse an einem gemeinsamen Wertschöpfungsnetz, welches den einzelnen Mitgliedern jedoch weitreichende Unabhängigkeit gewährt. Die verbundenen Unternehmen müssen sich jedoch in einem gemeinsamen Raum definierter Standards, Richtlinien und

gegebenenfalls technischen Vorgaben bewegen – insbesondere zur Gewährleistung von Sicherheitsanforderungen.

Die an einer Föderation beteiligten Organisationen müssen nun jedoch nicht nur für sich selbst, sondern bezogen auf die Wertschöpfungsgemeinschaft, d.h. organisationsübergreifend sicherstellen, dass ihre IT zwar angemessene Wertbeiträge liefert, hierbei jedoch interne und externe Anforderungen hinreichend erfüllt werden. Es muss die Qualität von Anwendungssystemen sichergestellt werden. Hierunter fallen Kriterien ökonomischer Natur (Kosten) und funktionale/nicht-funktionale Kriterien (Features, Usability, Security). Einige dieser Kriterien sind komplementär. Hervorzuheben ist die Informationssicherheit, da sie nicht nur ein alleinstehendes Qualitätsmerkmal ist, sondern gleichzeitig auch die Erreichung der Unternehmensziele, d.h. Wertschöpfung, sicherstellt.

Zur Sicherstellung der Wertbeitragslieferung existieren Referenzmodelle herstellerunabhängiger Natur (ITIL, COBIT) und proprietäre Referenzmodelle (MOF, ITSM, ITPM). Sie beschreiben Ziele, Aufgaben, organisatorische Aspekte und konkrete Ergebnisse der IT-Steuerung und Kontrolle [Goe06b]. Sie bieten somit Verfahren zur Implementierung allgemeiner, sogenannter „IT-Governance“, für einzelne Organisationen. Innerhalb dieser IT-Governance-Rahmenwerke sind teils auch Sicherheitsaspekte inbegriffen.

Für IT-Goverance existieren verschiedene Blickwinkel. Die strategische Sicht sieht darin eine Führungsleitlinie für zentrale und dezentrale IT, das IT-Management sieht ein Rahmenwerk zur Definition von Zielen, an denen sich die Ausgestaltung der IT messen lassen muss, die Produktion sieht eine formale Implementierung von Methoden zur Steuerung des operativen Betriebs [MF07]. Vorliegend wird unter IT-Governance eine Mischform aus der taktischen und der operativen Sicht verstanden.

Ferner existieren einerseits Ansätze für Entwicklung und Betrieb von Geschäftsprozessen sowie andererseits Informationssicherheitsmanagementsysteme (ISMS) wie der BSI IT-Grundschutz und die ISO 27001 zur Gewähr-

leistung der Einführung und Unterhaltung eines angemessenen Schutzbedarfs für eine spezifische Organisation. In dieser Richtung existieren auch erste Denkansätze für systematische, modellgestützte Vorgehensmodelle, wie in [SS06] vorgestellt, sowie Vorschläge zur Messbarkeit der Sicherheitsqualität bei betrieblichen Anwendungssystemen [HR06]. Ebenso entstehen Projekte zur rein technischen Absicherung föderierter VLBA [AA06] [WA11].

Die neue Herausforderung ist hierbei, IT-Governance betreiben zu können (das heißt die IT wertbeitragsfähig zu halten, und somit weniger als „Cost Center“ sondern eher als „Value Center“ zu verstehen [Goe06a]) und dabei gleichzeitig Qualitätsanforderungen wie Sicherheit im geforderten Maß einzuhalten. Obgleich hier stets ein Kompromiss zwischen vielen (potenziell gegenläufigen) Anforderungen gefahren werden muss (Beispiel: Usability vs. Security), sollten die Qualitätsanforderungen bestenfalls Teil der IT-Governance werden und ganzheitlich Betrachtung finden. Unter zusätzlicher Berücksichtigung regulatorischer Anforderungen geschieht dies unter Verwendung zuvor erwähnter Rahmenwerke wie COBIT, welche sich auch unter dem namentlich etablierten Begriff „GRC“ (Governance, Risk, Compliance) finden lassen.

1.2 Problem

Die Realisierung der Informationssicherheit muss aufgrund der Komplexität der Anwendungslandschaft methodisch gestützt werden, einerseits bei der (Software-)Entwicklung, jedoch auch beim Betrieb der Anwendungssysteme. Die Literatur fokussiert sich auf die Entwicklungssicht (Vorgehensmodelle, Methoden, etc.), nicht den Betrieb. Der Betrieb ist jedoch in der Praxis das verbreitetere Problem (Beispiel Banken: 70% der Aufwendungen sind dem Betrieb zu schulden [Goe06b]). Die praktische Relevanz des Problems ist somit sehr groß, die wissenschaftlichen Beiträge hierzu gleichzeitig sehr gering.

Grundsätzlich beschäftigt sich Informationssicherheitsmanagement mit dem Prozess der nachhaltigen Risikoreduktion in Bezug auf verschiedene Gefährdungen gegen die drei Hauptkriterien der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität [ISO13]. Diese Kriterien ändern sich nicht, wenn sich Prozesse über mehrere Organisationen erstrecken. Ebenso bleiben die Gefährdungen erhalten. Das Risiko hingegen wächst signifikant, und somit die Notwendigkeit der Implementierung effektiver Maßnahmen für relevante IT-Objekte.

Die erwähnten Lösungsansätze zum Erfüllen der beschriebenen Anforderungen sind jedoch auf System- und Organisationsapspekte sowie -kompetenzen ausgelegt. Daher ist es verständlich, dass die Bearbeitung dieser Anforderungen mit den traditionellen Mitteln (beispielsweise der ISO 27001) sehr viel Aufwand erfordert. Um beispielsweise eine kontextunabhängige Sicherheit bei Cloud-basierten Geschäftsprozessen zu realisieren, müssten alle beteiligten Stellen (insbesondere der Cloud Provider) von maximalen Risiken ausgehen, das heißt alle denkbaren Maßnahmen an den jeweiligen Ressourcen umsetzen.

Bislang existiert kein Rahmenwerk, welches die wachsende Notwendigkeit der IT-Governance über mehrere Organisationen, insbesondere der nachhaltigen Unterstützung eines konsistenten Informationssicherheitsmanagements für föderierte Geschäftsprozesse, auf effiziente Weise (das heißt mit schmalen Prozessen, nur den nötigsten Maßnahmen, geringen Kosten und klaren organisationsübergreifenden Verantwortlichkeiten) adressiert. Dies stellt den zentralen Betrachtungsgegenstand innerhalb dieser Arbeit dar. Eine detailliertere Problembeschreibung erfolgt zu einem späteren Zeitpunkt.

1.3 Ziele, Beiträge und Vorgehen

In [Hev04] werden Kriterien zur Evaluation von gestaltungsorientierten Forschungsvorhaben definiert, welche nun an das vorliegende Forschungsvor-

haben angelegt werden sollen.

Guideline 1: Design as Artifact - beschreibt die Identifikation eines Artefaktes, welches effektiv beschrieben werden und sich in eine bestehende Domäne integrieren lassen muss. Dieses Artefakt ist vorliegend das zu entwickelnde Rahmenwerk, welches unter Wahrung des (unter anderem von der ISO 27001 erfüllten) PDCA[1]-Zyklus [Wal88] die Geschäftsebene, die IT-/Ressourcen-Ebene sowie die Ebene der GRC-Anforderungen integrieren muss.

Unter diesem Rahmenwerk versteht sich die Entwicklung einer gesamtbildhaften Methodik zur Etablierung und Erhaltung eines angemessenen Schutzbedarfs von verarbeiteten Informationen in einer föderierten Prozessumgebung zwischen mehreren Organisationen, ausgehend von der Perspektive des Geschäftsprozesses.

Guideline 2: Problem Relevance - fordert das Vorhandensein eines relevanten Problems, welches das Artefakt adressiert. Vorliegend wäre die Relevanz gegeben, sobald (a) nachgewiesen ist, dass Organisationen tatsächlich zunehmend föderierte Geschäftsprozesse abbilden (demonstriert in [Est03] und [Sey02]) und (b) die vorhandenen Informationssicherheitsmanagementstandards diesen Fall nicht effizient verarbeiten können.

Letzteres haben die ISMS-Standards nicht in der Weise zum Anspruch, wie es für Fälle starker Föderierung von Prozessen motiviert wurde. Sie sehen sowohl in der Betrachtung der relevanten IT-Objekte als auch der relevanten Verantwortlichkeitszuordnung lediglich organisationseigene Personen/Mitarbeiter an. Eine Sicht auf den Geschäftsprozess wird nicht zwingend notwendig, wodurch u.a. potenziell unwichtige IT-Objekte mit Maßnahmen behandelt werden, wodurch hohe Kosten entstehen, die nicht notwendig sind.

[1] Plan, do, check, act

Gleichzeitig wird in der Literatur (wie beispielsweise von Senk und Bartmann [CS11]) demonstriert, wie aufwändig u.a. Authentifizierungs- und verwandte Sicherheitsmechanismen in Föderationen zu implementieren sind. Dies verdeutlicht beispielhaft, dass eine effiziente Methodik einen großen Unterschied hinsichtlich der Kosten im Zuge der Maßnahmenrealisierung bieten kann.

Eine prozessorientierte Sicht wird für föderative Szenarien entsprechend zwingend erforderlich, da nicht die IT-Objekte, sondern der Lebenszyklus der Prozesse in Bezug auf die Relevanz abzusichernder IT-Objekte im Vordergrund steht. Der Prozess stellt jenes Element dar, welches die beteiligten Organisationen über den zielgerichteten Austausch von Informationen miteinander verbindet. Gleichzeitig liegt eben in dieser Verbindung die potenzielle Gefährdung der Sicherheitsanforderungen des Prozesses, insbesondere bei stark abstrahierten IT-Systemen. Der Schutzbedarf eines Prozesses richtet sich nach der Art der verarbeiteten Informationen, das heißt der Zielsetzung des Prozesses.

In der Literatur existieren zwar Ansätze für das Management von Prozessen, genau wie für das Management von Informationssicherheit für Einzelorganisation und ihre IT-Objekte. Es existiert jedoch kein konsistent integriertes Rahmenwerk für das Sicherheitsmanagement föderierter Geschäftsprozesse.

Guideline 3: Design Evaluation - fordert die Messbarkeit des Nutzens, der Qualität und der Wirksamkeit eines Artefaktes. Eine Evaluation des Rahmenwerks unterliegt verschiedenen Erschwernissen. Zunächst lassen sich Methodiken aufgrund mangelnder Vergleichsobjekte grundsätzlich schwer evaluieren. Im Bereich der Informationssicherheit ist es zusätzlich unmöglich nachzuweisen, welche Vorfälle nicht eingetreten sind. Auch lassen sich unternehmenskritische Daten realer Organisationen nicht verwenden. Schließlich liefern Befragungen stets nur Aussagen zur Akzeptanz, weniger zur Effektivität von Methodiken.

Aufgrund dieser Erschwernisse wird vorliegend zunächst geprüft, ob sich mit dem entwickelten Rahmenwerk klassische, nicht föderierte Szenarien adressieren lassen, konkret dass die Ergebnisse vergleichbar zu denen der ISO 27001 sind. Dies leistet einen ersten Nachweis zur Effektivität des Rahmenwerks.

Anschließend wird geprüft, dass darüber hinaus auch föderierte Szenarien adressierbar sind. Dazu wird mit dem Order-to-Cash-Prozess (OTC) ein Geschäftsprozess ausgewählt, welcher sowohl hohe Verbreitung, als auch hohe Komplexität aufweist. Für dieses Szenario lässt sich annehmen, dass bei erfolgreicher Evaluation die entwickelte Methodik auch bei weniger komplexen Geschäftsprozessen effektiv ist.

Schließlich wird über eine Befragung eine Akzeptanzprüfung durchgeführt, welche Nutzen und Anwendbarkeit des Rahmenwerks greifbarer macht.

Guideline 4: Research Contributions - fordert klar definierte und überprüfbare Beiträge zu vorhandenen Artefakten, Grundlagen oder Methodologien. Das vorliegend entwickelte Rahmenwerk könnte der tatsächlichen Erreichung eines revisionssicheren, angemessenen Schutzniveaus einer Föderation im Kernbereich ihrer übergeordneten Tätigkeit (der Abwicklung des Kerngeschäftsprozesses der marktnahen Organisation, welche Bestandteil der Föderation ist) dienlich sein, was gleichzeitig zur Sicherstellung der Wertschöpfung der IT beiträgt, da alle beteiligten Systeme weniger anfällig gegen Vertraulichkeits- und Integritätsverletzungen und vor allem höher verfügbar sind. Gleichzeitig kann mit der Vereinheitlichung der Gedankengebäude von Prozess-, IT- und Sicherheitsbelangen ein potenzieller Mehrwert für künftige, artverwandte Forschungsvorhaben geliefert werden.

Guideline 5: Research Rigor - fordert die Einbeziehung von klaren Methoden in sowohl der Konstruktion als auch der Evaluation von Artefakten. Vorliegend werden Literaturrecherchen, Business Case Analysen, Be-

fragungen sowie die anonymisierte Auswertung empirischer Daten (Abfolge von Schritten und Bewertung der Kritikalität von Informationen im OTC) von Organisationen verwendet, um die adressierten Teilschritte zur Lösung des Problems, der Durchsuchung des Lösungsraumes, verwendet. Zur Beschreibung von Abhängigkeiten wird UML verwendet. Es wird angestrebt, das beschriebene Artefakt hierdurch greifbarer und nützlicher zu gestalten.

Guideline 6: Design as a Search Process - fordert die klar definierte Suche eines effektiven Artefaktes durch Verwendung vorhandener Möglichkeiten zur Erreichung des gewünschten Zweckes unter gleichzeitiger Berücksichtigung der Gesetzmäßigkeiten der Problemumgebung.

Vorliegend werden verschiedene Themen adressiert, die dieser Guideline Rechnung tragen. Es werden Konzepte evaluiert, die versprechen, die genannten Probleme (teilweise) zu lösen. Diese Konzepte stammen aus den Bereichen des Geschäftsprozessmanagements und des Informationssicherheitsmanagements. Die Betrachtung von Rahmenwerken zur Behandlung nicht-informationssicherheitsrelevanter Probleme kann Hinweise geben, wie artverwandte Probleme gelöst und eigene adressiert werden können.

Grundsätzlich wird auch versucht, vorhandene Probleme bei der Sicht auf föderative Geschäftsprozesse zu vereinfachen und/oder diese Probleme in kleinere Teilprobleme zu zerlegen. Ferner wird analysiert, ob das entwickelte Rahmenwerk sich nur auf föderierte oder nach wie vor auch auf nichtföderierte Geschäftsprozesse anwenden lässt. In letzterem Fall würden sich traditionelle Ansätze inhaltlich ablösen lassen.

Guideline 7: Research Communication - fordert die effektive Präsentation des Forschungsstandes gegenüber technologisch- und managementorientiertem Publikum. Dies wird vorliegend durch verschiedene geplante

Publikationen und die Einbeziehung praktischer Beispiele, die in der Literatur bereits genannt werden, sowie beispielhaft erstellte Abbildungen zur Visualisierung von Problemen und Lösungen versucht zu erreichen.

Technische Beteiligte sollen ein Verständnis für Zielsetzung und teils auch Notwendigkeit föderierter Prozessstrukturen erhalten. Hierbei sollen technische Details wie die Beschreibung nutzbarer Technologien wie Middleware und Cloud-Dienste erläutert werden. Managementorierte Beteiligte sollen hinsichtlich der Wichtigkeit des Problems sowie des Neuigkeitsgehaltes der vorgestellten Lösung und ihrer Anwendbarkeit sensibilisiert werden, indem hinreichend Motivationen verwendet und Beispiele sowie Nachweise für Problemreduktionen durch Einsatz des Artefaktes gegeben werden.

1.4 Aufbau der Arbeit

Die vorliegende Arbeit gliedert sich in insgesamt fünf Teile. In Teil I werden elementare Konzepte des Föderalismus, beteiligter Technologien, der Sicherheit und des Sicherheitsmanagements von und in Organisationen erläutert.

Hierzu wird in Kapitel 2 zunächst beschrieben, welche Begrifflichkeiten im Umfeld der Unternehmensprozesse vorliegend Verwendung finden sollen und wie die Einheit von Menschen, Prozessen und Technik verstanden wird. Kapitel 3 beschäftigt sich mit relevanten Konzepten der Sicherheit in Organisationen. In Kapitel 4 werden Begriffe, Voraussetzungen, Herangehensweisen und in Kapitel 5 die dazugehörigen Technologien in Föderationen geklärt. Ein darin enthaltener Blick auf das Sicherheitsmanagement in föderierten Umgebungen und sein Einfluss auf Prozesse, Menschen und Technik rundet diesen Teil ab.

In Teil II werden die bislang vorhandenen Konzepte zum methodisch gestützten Sicherheitsmanagement von Informationen in Organisationen identifiziert, erläutert und klassifiziert. Kapitel 6 liefert eine Übersicht über Rah-

menwerke, welche hierfür relevant sind. In Kapitel 7 werden Kriterien zur Klassifizierung dieser Rahmenwerke abgeleitet und die Klassifizierung durchgeführt.

In Teil III wird die sich aus den vorherigen Teilen ergebende Lücke benannt und der für die Realisierung anvisierte Betrachtungsgegenstand beschrieben, d.h. Anforderungen für das zu entwickelnde Rahmenwerk für Föderationen erhoben. In Kapitel 8 wird ein typisches Föderierungsszenario benannt. Kapitel 9 beschäftigt sich mit der Isolierung des Problemfeldes.

Teil IV schließt die zuvor ausdefinierte Lücke durch die Entwicklung des Rahmenwerks und validiert die Erfüllung der zuvor beschriebenen Anforderungen. Die notwendigen Anforderungen an ein neues GRC-optimiertes Geschäftsprozessrahmenwerk werden in Kapitel 10 erhoben. Kapitel 11 beschreibt die Konstruktion des Rahmenwerks unter Berücksichtigung der Anforderungen. Kapitel 12 schließt mit einer Evaluierung samt Akzeptanzprüfung des entwickelten Rahmenwerks.

Teil I

Grundlagen

Überblick Teil I

Nachdem in der Einleitung sowohl die Motivation für föderatives Informationssicherheitsmanagement als auch die Ziele dieser Arbeit dargelegt wurden, sollen nachfolgend elementare Konzepte des Föderalismus, beteiligter Technologien, der Sicherheit und des Sicherheitsmanagements von und in Organisationen erläutert werden.

Hierzu wird in Kapitel 2 zunächst beschrieben, welche Begrifflichkeiten im Umfeld der Unternehmensprozesse vorliegend Verwendung finden sollen und wie die Einheit von Menschen, Prozessen und Technik verstanden wird. Kapitel 3 beschäftigt sich mit relevanten Konzepten der Sicherheit in Organisationen. In Kapitel 4 werden Begriffe, Voraussetzungen, Herangehensweisen und in Kapitel 5 die dazugehörigen Technologien in Föderationen geklärt. Ein darin enthaltener Blick auf das Sicherheitsmanagement in föderierten Umgebungen und sein Einfluss auf Prozesse, Menschen und Technik rundet diesen Teil ab.

Für die Erstellung der Teile I und II wurde zunächst sämtliche Literatur gesammelt, welche für das Themenfeld weiträumig relevant schien. Hierbei wurde mit einer strukturierten Literaturanalyse gearbeitet, in welcher für Bücher, Journalbeiträge, Whitepaper und online verfügbare Fachbeiträge zunächst die Attribute Titel, Autor, Verlag, Erscheinungsjahr, ggf. ISBN-Nummer sowie ein eigener Kommentar erfasst wurden.

Im Anschluss wurden jedem Eintrag eingängige Schlagwörter vergeben, darunter beispielsweise Architektur, Auditing, Föderierung, Governance,

Rahmenwerk und/oder SOA. Später wurden die für das jeweilige Themenfeld passendsten Einträge diagonal gelesen und einer qualitativen Bewertung hinsichtlich ihrer Wissenschaftlichkeit unterzogen. Die inhaltlich passendsten und für wissenschaftliche Zwecke geeignetsten Beiträge wurden vorliegend verwendet, die übrigen lediglich zur Validierung für potenzielle Widersprüche verwendet.

Schließlich wurden konkrete Themen und Definitionen ausgewählt, die zum wechselseitigen Verständnis der Stakeholdergruppen Geschäftsführung, Informationssicherheitsmanagement und IT-Management beitragen können. Auf Basis der aus der Literaturanalyse resultierenden Beiträge wurden schließlich die nachfolgenden Kapitel zusammengestellt.

2 Informationen und Prozesse

Die Wirtschaftsinformatik – als die Disziplin, zu welcher sich die Untersuchungen in dieser Dissertation zuordnen lassen – ist eine Schnittstellenwissenschaft im Zentrum vieler Nachbarwissenschaften. Sie besitzt neben einem weiträumigen Methodenpluralismus auch eine Vielzahl verschiedener Definitionen für vermeintlich einheitlich verwendete Begrifflichkeiten. Dieses Kapitel dient daher der Erfassung und der Diskussion von in der Literatur verwendeten Begriffen, die für die späteren Untersuchungen relevant sind.

2.1 Menschen, Aufgaben, Technik

Bereits in einem Beschluss der Wissenschaftlichen Kommission Wirtschaftsinformatik (WKWI) im Jahr 1993 wurde das Ziel der Wirtschaftsinformatik durch die

> *„[…] Gewinnung von Theorien, Methoden, Werkzeugen und intersubjektiv nachprüfbaren Erkenntnissen über/zu Informations- und Kommunikationssystemen […]“ [Sch06]*

definiert.

Solche Informations- und Kommunikations- oder kurz *IKT*-Systeme befinden sich jedoch wiederum in der Schnittmenge benachbarter Disziplinen. Entsprechend sollte zunächst geklärt werden, wie einschlägige Sichten der Literatur für IKT lauten.

Die Betriebswirtschaftslehre betrachtet ein Informationssystem hierbei als formalen Teil des weiter gefassteren betrieblichen Kommunikationssystems, genauer als

> *„Summe aller geregelten betriebsinternen und -externen Informationsverbindungen sowie deren technische und organisatorische Einrichtung zur Informationsgewinnung und -verarbeitung" [Gab12].*

Die Wirtschaftsinformatik versteht ein Informationssystem als Einheit von Mensch, Aufgabe und Technik (MAT) [LJH07]. Gemäß [Wir12] spielen diese MAT-Systeme dann eine besondere Rolle, wenn der Informationszweck vordergründig und der Austausch einer Information nur ein Mittel zur Verständigung über den Inhalt der Information ist.

Entsprechend wird einerseits die Erhaltung und Verwendung, andererseits der Zweck der Informationen innerhalb einer Organisation zentralisiert. In jedem Fall wird implizit eine Wechselwirkung des Informationssystems mit seiner Umwelt vorgesehen. Hierdurch wird deutlich, dass MAT-Systeme keinem Selbstzweck dienen, sondern integrierter Bestandteil von und wichtig für die Informationswirtschaft einer Organisation sind.

2.2 Prozessverständnis

Da Informationssysteme aus Menschen, Arbeit und Technik bestehen, liegt es nah, dass diese drei Faktoren, geleitet durch eine übergeordnete Regel, miteinander interagieren müssen. Hier ist bereits wichtig zu klären, inwieweit sich ein solcher übergeordneter Prozess vom *Arbeitsprozess* innerhalb der MAT-Einheit abgrenzt.

In [LDL03] wird versucht, mit der Vielzahl verfügbarer Definitionen eine allumfassende Definition für einen Geschäftsprozess abzuleiten. Ein Geschäftsprozess ist demnach eine Sammlung von Aktivitäten, welche einen oder mehrere Eingaben erhält und eine Ausgabe liefert, welche für einen

Kunden von Wert ist. Hierbei sind die in den Aktivitäten verarbeiteten Informationen von zentraler Bedeutung.

Als Geschäftsprozess wird unterschieden in einen Typ- und einen Instanz-Begriff. Auf Ebene des Typ-Begriffs wird ein Prozess definiert, modelliert und dokumentiert, welcher einen übergeordneten wertschöpfenden oder wertsteigernden Beitrag besitzt. Ergebnis sind Folgen von Einzelaktivitäten (Arbeit) sowie eine Zuweisung von Personen (Menschen) und technologischen Unterstützungsmöglichkeiten (Technik), welche voll- und teilautomatisiert eingesetzt werden können. Die Einzelaktivitäten selbst können jedoch auch als Prozess verstanden werden. Dies ist im strengeren Sinn jedoch eine Definition über den Begriff der Prozessinstanz. Jede Aktivität, ob definiert oder undefiniert kann letztlich als Prozess verstanden werden.

Ein Geschäftsprozess soll vorliegend jedoch die übergeordnete Einheit sein, welche Konstellation und Semantik des MAT-Zusammenspiels definiert, siehe Abbildung 2.1.

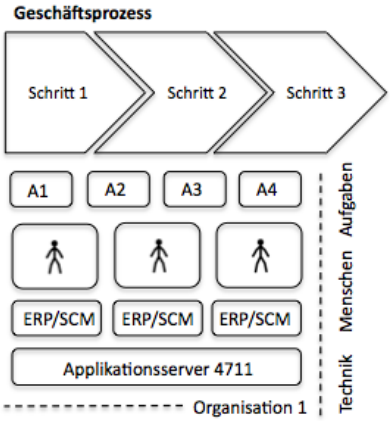

Abbildung 2.1: Prozess-MAT-Zusammenhang

Im Kontext des Föderationsgedankens ist hier insbesondere die Aufteilung der Aktivitäten des Geschäftsprozesses über mehrere Organisationen von Relevanz. Erst die letzte Ausgabe des Gesamtprozesses (des letzten Prozessbestandteils) liefert einen Mehrwert für den Kunden. Geschäftsprozesse müssen somit sinnvoll modularisiert werden können. Dieser Kerngedanke wird später wieder aufgegriffen.

Letztlich können Geschäftsprozesse unternehmensinterne und -externe Einflussfaktoren haben, die in einem Regelwerk für den Ablauf des Geschäftsprozesses enden. Dies soll später genauer erläutert werden.

2.3 Management von Prozessen

Geschäftsprozesse unterliegen auch gemäß den Diskussionen in [LDL03] grundsätzlich Zielen. Entsprechend sind vor der Implementierung von Geschäftsprozessen strategische Überlegungen anzustellen. Im Anschluss führen verschiedene Aktivitäten des Geschäftsprozessmanagements zu einem fertigen und dokumentierten Prozess. Diese Aktivitäten umfassen:

- Planung und Modellierung
- Verifizierung
- Realisierung/Implementierung
- Kontrolle und Verbesserung

Diese Schritte sind auch in proprietären Konzeptmodellen wie dem *Process Management Lifecycle* der SAP AG vorgesehen. [SAP13] Dort werden die Phasen *Analyze*, *Design*, *Implement* und *Run/Monitor* unterschieden. Diese Phasen verlaufen iterativ. Die Iteration geht konform mit dem PDCA-Zyklus (*Plan, Do, Check, Act*) nach Deming [Wal88], welcher eine Managementmethode mit den Phasen Planung, Durchführung, Kontrolle und Korrektur des Betrachtungsgegenstandes vorsieht, siehe Abbildung 2.2.

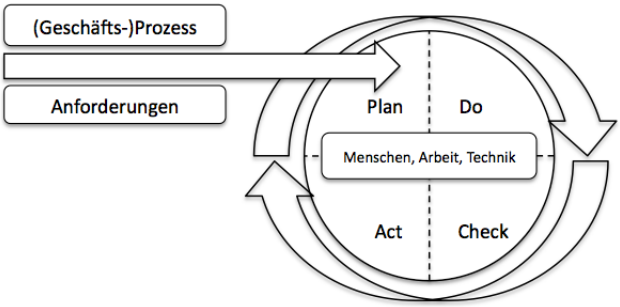

Abbildung 2.2: Plan, Do, Check, Act

Die resultierenden Prozesse unterliegen einer fortlaufenden Dokumentation von Veränderungen und Resultaten. Dem Management von Prozessen stehen schließlich verschiedene interne und externe Anforderungen gegenüber, beide Arten können dabei von internen und externen Revisoren geprüft werden. Welche Anforderungen dies im Detail sind, soll in Kapitel 3 geklärt werden. Vorliegend ist der PDCA-Zyklus von zentraler Bedeutung für die spätere Konstruktion des ISMS-Rahmenwerks, da ein konsistenter Sicherheitszustand nur erhalten werden kann, wenn die Prozesse, die diese Sicherheit beeinflussen, eine Rückkopplung besitzen. Dieser Gedanke wird ebenfalls später vertieft werden.

2.4 Prozesse und IKT

Für die Verbindung von Prozessen und IKT sind abermals verschiedene Ebenen zu unterscheiden. Die *Geschäftsprozessmodellierung* dient der Definition von Prozessen für Abläufe mit Wertschöpfungs- oder Wertbeitragsbezug, welche durch IKT Unterstützung finden. Sie ist eine Form des Prozessmanagements.

Das *IT-Service-Management (ITSM)* enthält Methoden, welche notwendig sind, um eine bestmögliche Unterstützung der IT beziehungsweise der IT-Organisation für Geschäftsprozesse zu gewährleisten. Ein De-facto-Standard für ein solches Prozessrahmenwerk ist die *IT Infrastructure Library (ITIL)*. Auf ITIL wird später in dieser Arbeit genauer Bezug genommen.

Das *Business Service Management (BSM)* bietet eine Verbindung zwischen dem Prozessmanagement und dem IT-Service-Management. *Serviceorientierte Architekturen (SOA)* bilden ein Konzept für dienstorientierte IKT-Unterstützung. BSM und SOA sollen hier keine Betrachungsgegenstände darstellen.

Erwähnt werden soll bereits an dieser Stelle, dass ein international anerkanntes Rahmenwerk mit Relevanz zum Mapping zwischen Geschäftszielen und der Ausrichtung der Wertbeiträge durch IT existiert. Das Rahmenwerk *Control Objectives in Information and related Technologie (COBIT)* dient diesem Zweck [Ins07]. Es wird später näher erläutert, soll jedoch bereits jetzt als Input für einen weiteren zentralen Definitionsbaustein dienen.

Es ist wichtig zu betrachten, welche technischen Unterstützungsmöglichkeiten für Geschäftsprozesse vorliegend von Relevanz sind. COBIT fasst hier unter dem Gesamtbegriff „Ressourcen und Services“ namentlich Informationen, Anwendungen, Infrastruktur und Personen zusammen. Hier lassen sich Anwendungen und Infrastuktur, das heißt Software und Hardware, klar der technischen Komponente der MAT-Einheit zuordnen.

2.5 Zusammenfassung

Die Wirtschaftsinformatik beschäftigt sich mit der Erschaffung von Werkzeugen und/oder der Gewinnung von Erkenntnissen für und über Informationssysteme. Diese Informationssysteme bestehen aus einem Verbund aus Menschen, Aufgaben und Technik, dessen Ausgestaltung in Abhängigkeit von einem definierten Geschäftsprozess unterschiedlich ausfallen

kann. Prozesse sind nicht zwangsläufig Geschäftsprozesse, sie können auch Einzelaktivitäten mit nur mittelbarem Wertbeitragsbezug darstellen.

Informationen dienen als Eingabe- und Ausgabewerte, die sich im Zuge der Durchführung von Aktivitäten (*Aufgaben*) durch Personen (*Menschen*) und/oder IKT (*Technik*) anreichern, woraus ein Wertbeitrag für den Adressaten des Geschäftsprozesses wächst. Die von COBIT definierten Ressourcen *Anwendungen* und *Infrastruktur* dienen vorliegend als Bestandteile der Technik der MAT-Einheit.

Es existieren verschiedene Möglichkeiten zum Management von Prozessen im Allgemeinen und der Integration in den Themenbereich der IKT im Speziellen. Rahmenwerke, welche sich ein solches Prozessmanagement zur Aufgabe stellen, sollten den PDCA-Zyklus vorsehen, welcher Planung, Durchführung, Prüfung und Optimierung des zu etablierenden Systems gewährleistet. COBIT unterstützt hier den Entwurf von Maßnahmen zur Sicherstellung des Wertbeitrags der IT zur Erfüllung von Geschäftszielen. Hierunter fallen auch Maßnahmen zur Gewährleistung eines effektiven Sicherheitsmanagements.

3 Sicherheitsmanagement

Dieses Kapitel dient der Diskussion verwendeter Begrifflichkeiten für Sicherheit und Sicherheitsmanagement und ordnet sie mit Hilfe von [Zar09] in den Rahmen integrierten Managements von Governance, Risk und Compliance ein.

3.1 Governance, Risk, Compliance

Zentralisiert man die zuvor erläuterten Geschäftsprozesse und blickt auf die Ressourcen (Menschen, Arbeit, Technik), die diese Geschäftsprozesse unterstützen, so wird die Komplexität des Sicherheitsmanagements des Gesamtsystems deutlich. Abbildung 3.1 zeigt die relevanten Sicherheitsdimensionen:

- Dimension 1: Geschäftsprozesse
- Dimension 2: Ressourcen & Services
- Dimension 3: GRC-Anforderungen

Die Kenntnis über diese Dimensionen ist zentral zur Beantwortung der Frage, wie ein Modell zur Absicherung föderierter Geschäftsprozesse zu entwickeln ist. Daher sollen die drei Dimensionen näher erläutert werden.

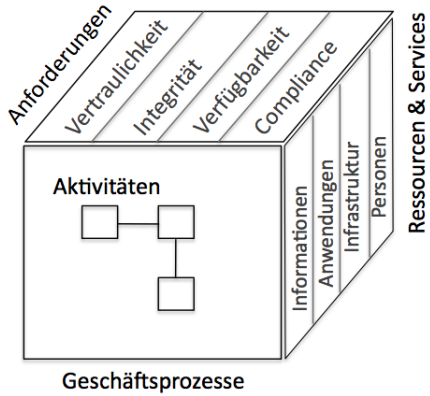

Abbildung 3.1: GRC-Dimensionen

3.1.1 Geschäftsprozesse

Die Sichtweise auf einen Geschäftsprozess wurde bereits im vorherigen Abschnitt erläutert. Vorliegend soll jedoch bereits auf die zusätzliche Relevanz der Zerlegung von Geschäftsprozessen für föderative Zusammenhänge hingewiesen werden. Diese Thematik wird in Teil IV näher erläutert werden. Föderierungen erfordern eine hinreichende Flexibilität des Geschäftsprozesses. Entsprechend ist die Zerlegung von Geschäftsprozessen in Prozessmodule ein wesentlicher Ansatz. Diese Zerlegung führt zu einer Prozess-Intra-Flexibilität (der Flexibilität innerhalb der Prozessmodule) und einer Prozess-Inter-Flexibilität (der Flexibilität und individuellen Kombinierbarkeit der Prozessmodule).

Zu betrachtende Geschäftsprozesse lassen sich dabei nach verschiedenen Kriterien in Prozessmodule zerlegen. Im ERP-Kontext ließe sich beispielsweise ein Geschäftsprozess jeweils an den Stellen zerlegen, an denen verschiedene MAT[1]-Einheiten an der Wertschöpfung beteiligt sind, und sich

[1] Menschen, Arbeit, Technik

diese Teilschritte möglichst stark kapseln lassen. In diesem Fall wäre dies möglich an Stellen, an denen Berichte erzeugt und einer nächsten Einheit übergeben werden.

Geschäftsprozessmodule bestehen aus einem Prozesskern, der die wesentlichen Funktionalitäten umfasst und aus den standardisierten Schnittstellen. Die Zerlegung eines Beschaffungsprozesses in Prozessmodule wurde in [NF12] exemplarisch durchgeführt.

Diese dynamische Verbindung dirigiert eine völlig neue Einheit des Zusammenwirkens von Menschen, Aufgaben und Technik über die Grenzen einer einzelnen Organisation hinaus. Föderationen, beispielsweise Unternehmenskooperationen oder enge Lieferantenbeziehungen, könnten sich damit, im Hinblick auf das Informationssicherheitsmanagement, künftig effizient und agil steuern und kontrollieren lassen.

3.1.2 Ressourcen & Services

Maßgeblich sind hier einerseits die Sicht auf die in [LJH07] definierte Einheit von Menschen, Aufgaben und Technik (MAT) als Informationssystem, andererseits die unter anderem in COBIT [Ins07] definierten Ressourcen & Services *Informationen*, *Anwendungen*, *Infrastruktur* und *Personen*.

Informationen sind vorliegend als Ein- und Ausgabewerte der Aktivitäten, das heißt der *Aufgaben*, innerhalb der Geschäftsprozessmodule zu verstehen. Personen lassen sich direkt den *Menschen* zuordnen, die diese Aufgaben ausführen. Diese können jedoch durch Informations- und Kommunikationstechnologien (IKT) gestützt werden. Anwendungen und Infrastruktur sind entsprechend der Software und Hardware zuzuordnen, das heißt der *Technik* der MAT-Konstellation.

Diese Konstellation kann sich in Abhängigkeit von der Semantik des Prozesses in unterschiedlicher Breite und Tiefe zusammensetzen.

3.1.3 GRC-Anforderungen

Geschäftsprozesse müssen verschiedenen internern und externen Anforderungen gerecht werden, was letztlich durch Kontrollen und Maßnahmen an den beteiligten Ressourcen, die den Prozess unterstützen, sichergestellt werden muss. Später im Kapitel wird auf diese konkreten Anforderungen genauer eingegangen. Wichtig ist zunächst, dass Governance, Risk und Compliance Ebenen darstellen, welche sich gegenseitig bedingen und einander teilweise sogar voraussetzen.

Compliance Auflagen gesetzlicher Natur und geforderte Konformität mit Richtlinien und Kodizes werden durch Anforderungen der *Compliance* ausgedrückt [IDW11]. Obwohl Compliance in der Praxis oft als abstrakt, komplex und intransparent angesehen wird, ist es in der heutigen Geschäftswelt ein unausweichliches Thema. Es benennt die Konformität von Prozessen mit regulatorischen Anforderungen.

Risk Weiterhin sind Schutzbedarfe für die in den Prozessen und durch die Ressourcen verarbeiteten Informationen festzusetzen. Diese gelten jeweils für die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit [BSI09a]. Sie sind verbunden mit der Identifikation, Analyse, Bewertung, Bewältigung, Überwachung und Aufzeichnung von *Risiken* [Kei04]. Die Schutzziele sollen gleich genauer definiert werden.

Governance Um Informationen darüber zu erhalten, an welchen Objekten Maßnahmen durchzuführen sind, welche sich durch Risikoanalysen und Compliancebetrachtungen ergeben haben, ist IT-Governance nötig. Nur mit einer ausreichenden Übersicht über die gerichteten Verbindungen von Geschäftsprozessen zu den beteiligten Menschen, Aufgaben und IT-Systemen

(Software und Hardware) ist die effektive operative Realisierung von Maßnahmen durchführbar. IT-Governance beschreibt Ziele, Aufgaben, organisatorische Aspekte und konkrete Ergebnisse der IT-Steuerung und -Kontrolle [Goe06b].

3.1.4 Zeitliche Dynamik

Als weitere Erschwernis kommt hinzu, dass in unterschiedlichen Phasen des Prozesslebenszyklus auch unterschiedliche Complianceanforderungen auf die jeweiligen Services treffen. Die genannten drei Dimensionen unterliegen somit einer zeitlichen Dynamik.

Ändert man aber nun Teile der MAT-Landschaft ab, so wird auch schnell die Konsistenz der Sicherheitsmaßnahmen beeinträchtigt und ein iteratives Risikomanagement wird unabdingbar. Entsprechend wird der gesamte GRC-Lebenszyklus fortwährend beeinflusst. Dies unterstreicht, dass das Gesamtgefüge aus Governance, Risk und Compliance nicht trennbar ist und, insbesondere in Föderationen, eine agile Methodik benötigt wird.

Später wird auf diese drei Dimensionen in Form von Modell-Perspektiven zurückgegriffen. Zunächst soll ein genauerer Blick auf den Begriff der Sicherheit und die Sicherheitsanforderungen gelegt werden.

3.2 Sicherheit

Für den Begriff der Sicherheit existieren in der Literatur abermals verschiedene Definitionen.

In [GG04] wird der Begriff der *psychischen Sicherheit* geprägt, welche aus menschlicher Zuneigung entsteht. Durch Bindungen wird hier die kognitive, sprachliche und kulturelle Entwicklung gestärkt.

Auch präsent sind Sichtweisen aus dem Bereich der *öffentlichen Sicherheit*. In [Sch04] wird die Sicht auf Sicherheitsgebrauch, -gewährleistung, -bedürfnis und -anspruch in der Gesellschaft geprägt. Hier kommen die Aspekte der Sicherheit durch Macht und der Sicherheit durch Recht zum Tragen, der Betrachtungswinkel stammt demnach klar aus gesellschaftlich-politischer Richtung.

In [Fau02] und [Kri01] wird zudem der Begriff der *kollektiven Sicherheit* geprägt, welche sich insbesondere aus der Schutzfunktion des Staatenbundes und dem Recht zur Selbstverteidigung zusammensetzt. Diese Perspektive fokussiert sich auf den militärischen Aspekt des Sicherheitsbegriffes.

Da sich das Leben und der Wohlstand heutiger Menschen auf das Funktionieren der Wirtschaft, und damit von Organisationen stützt, existiert auch eine Perspektive für den Begriff Sicherheit für Informationen und der Informationstechnik, welche Prozesse der Organisationen unterstützt, wie in Kapitel 2 beschrieben. Hier wird Sicherheit häufig bezeichnet als *Zustand*, der frei von unvertretbaren Risiken ist [Wör08].

Diese Definition über einen statisch/absoluten Zustand ist jedoch fragwürdig, da jede Organisation ständigen, dynamischen Änderungen in Form interner und externer Anforderungen ausgesetzt ist. Diese Änderungen betreffen direkt die abzusichernden Geschäftsprozesse, samt ihrer Menschen, Aufgaben und Technik. In [Mül10] wird Sicherheit daher als Dreiklang aus den jeweils geltenden Bedrohungspotenzialen, der Wertigkeit der Objekte und den errichteten Abwehrmaßnahmen verstanden. Dies führt zum Verständnis der Sicherheit als *Prozess*.

Alle Sichtweisen haben eins gemeinsam: sie schreiben der Sicherheit die Eigenschaft zu, ein Grundbedürfnis des Menschen zu sein, nach dem er auf wirtschaftlicher, sozialer, politischer, militärischer und kulturell-gesellschaftlicher Ebene strebt, um Verletzbarkeit durch Gefährdungen zu beseitigen oder zu minimieren. Die Unterscheidung liegt daher nicht in der Herkunft des Wortes oder seiner Anwendung begründet. Vielmehr ist das primär zu

schützende Objekt ein anderes – die Bindung, die Gesellschaft, das Land, die Information – obgleich hier stets der Mensch Teil der abzusichernden Kette ist. Vorliegend soll Sicherheit als Prozess verstanden und auf Organisationen bezogen werden. Hier stellt sich jedoch weiterhin die Frage, welche Unterscheidung man in Bezug auf das Thema Sicherheit in Organisationen anlegen möchte. Hierzu sollen nachfolgend weitere Aspekte der Unternehmenssicherheit diskutiert werden.

3.3 Informationssicherheit

Die Begriffe Sicherheit, Informationssicherheit und IT-Sicherheit werden in der deutschsprachigen Literatur oft synonym verwendet. Auf Basis der Sichtweise, dass IT nur die technischen Komponenten der MAT-Einheiten meint, ist dies jedoch irreführend, da der resultierende Umgang der zu adressierenden Objekttypen vermischt wird.

Gemäß der internationalen Norm ISO 27002 [fNe05] meint Informationssicherheit die *„[…] Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen“*. Diese Definition wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) mitgetragen [BfSidI09]. Zusätzliche Anforderungen wie Authentizität (Echtheit des Ursprungs, wobei diese vorliegend unter Integrität zählen soll), Nicht-Abstreitbarkeit, Zurechenbarkeit, und Verlässlichkeit können berücksichtigt werden, wofür jedoch kein Zwang besteht.

Hier lässt sich bereits eine erste Unterscheidung ableiten. So gilt es bei der Gewährleistung von Verfügbarkeit darum, dass etwas stets eintritt – die Umsetzung von Vertraulichkeit und Integrität impliziert hingegen, dass gewisse Dinge nicht eintreten sollen. Um dies besser verstehen zu können, sollen nachfolgend alle drei Bereiche näher definiert werden.

Vertraulichkeit (Confidentiality) Vertrauliche Informationen sollen vor dem Zugriff unbefugter Personen geschützt werden. Hierzu sind weitere Begrifflichkeiten relevant: Identifikation (welche Person unternimmt einen Zugriffsversuch), Authentisierung (die Identifikation einer Person wird verifiziert) und Autorisierung (ist die authentifizierte Person zu einer bestimmten Aktion berechtigt).

Integrität (Integrity) Sämtliche Daten sind vollständig und vom Sender zum Empfänger nicht verändert worden. Unter Daten verstehen sich dabei Informationen mit konkreten Attributen (Autor, Erstellungsdatum, etc.) [BfSidI09]. Mangelt es an der Integrität von Informationen, so kann dies bedeuten, dass eine Manipulation stattgefunden hat. Diese Manipulation kann jedes Attribut betreffen, das einer Information zugeordnet wurde - im Falle einer E-Mail beispielsweise den Inhalt der Nachricht. In diesem Rahmen ist auch der Begriff der Authentizität (Authenticity) relevant. Dieser meint jedoch explizit die Echtheit des Ursprungs eines Prozesses. Mangelhafte Authentizität bedeutet entsprechend eine ungenügende Nachverfolgbarkeit einer Tätigkeit zu einem Subjekt, beispielsweise einer Datenbankoperation zu einer Person. Eng damit verknüpft ist auch der Begriff der Nachweisbarkeit (Accountability). Nachweisbarkeit steht für die Möglichkeit, Zugriffe/Interaktionen Subjekten eindeutig zuordnen zu können.

Verfügbarkeit (Availability) Im Kontext der Verfügbarkeit sind nicht nur die Funktionen eines IT-Systems inbegriffen. Auch Dienstleistungen und andere Unternehmensprozesse unterliegen der Not, den Schutz ihrer Verfügbarkeit zu gewährleisten. Wichtig dabei ist, dass die entsprechenden Informationen stets auch zum geforderten Zeitpunkt zur Verfügung stehen.

Compliance-Anforderungen Auflagen gesetzlicher Natur und geforderte Konformität mit Richtlinien und Kodizes werden durch Anforderungen

der Compliance ausgedrückt. Obwohl Compliance in der Praxis oft als abstrakt, komplex und intransparent angesehen wird, ist es in der heutigen Geschäftswelt ein unausweichliches Thema. Es benennt die Konformität von Prozessen mit regulatorischen Anforderungen.

Der Datenschutz bildet hier eine gesonderte Sicherheitsanforderung, da er als Spezialfall der Vertraulichkeit in Bezug auf besondere Daten angesehen werden kann. Inhalt des Datenschutzes ist die Gewährleistung auf informationelle Selbstbestimmung, nach der jede Person selbst entscheiden und beeinflussen können muss, welche Daten auf welche Weise verarbeitet werden [fdDudI10]. Ferner existieren weitere, auch branchenspezifische Regularien, welche durch geeignete Maßnahmen zu adressieren sind. Ein Beispiel ist der Sarbanes Oxley Act (SOX), welcher die Verlässlichkeit der Bericht-Erstattung von Unternehmen, welche am öffentlichen Kapitalmarkt der Vereinigten Staaten von Amerika teilnehmen, verbessern soll.

Compliance-Anforderungen sollen vorliegend zwar nicht primär adressiert werden, jedoch wird auf die Korrelation von Governance, Risk und Compliance (GRC) später noch näher eingegangen. Wichtig ist zunächst, dass die aufgeführten Anforderungen zentraler Bestandteil des Managements von Risiken und Compliance sind, und dass sich dieses Management in einen umfassenden Governance-Rahmen integrieren muss, um effektiv zu sein. Es bleibt jedoch die Frage, wie das Management von Informationssicherheit operativ durchgeführt wird.

3.4 Informationssicherheitsmanagement

Informationssicherheit kann als allumfassender Mantel für die Sicherheitsbelange eines Unternehmens angesehen werden, da jegliche Gefährdungen gegen das Unternehmen letztlich durch den Schutz der verarbeiteten Informationen innerhalb des Unternehmens durch Maßnahmen adressiert werden können. Dies schließt Maßnahmen zur Sicherung der die Information

verarbeitenden Menschen und IT-Systeme sowie die dazu notwendige Infrastruktur mit ein.

Ein Informationssicherheitsmanagementsystem ist daher zu verstehen als eine Aufstellung von Verfahren und Regeln innerhalb einer Organisation, welche dazu dienen, *„die Informationssicherheit zu definieren, zu steuern, zu kontrollieren, aufrecht zu erhalten und fortlaufend zu verbessern“* [fNe05].

Innerhalb einer Organisation werden entsprechend Prozesse geschaffen, die planend, verändernd, prüfend und reaktiv handelnd Schutzbedarfe von bestimmten Objekttypen errichten und erhalten können. Hier wird der Bezug zum PDCA-Zyklus ebenso deutlich wie die Integration in den Prozessmanagement-Rahmen aus Kapitel 2.3. Als Prozesse verstehen sich dabei jedoch nicht Geschäftsprozesse, sondern Verfahren zur Behandlung der die Geschäftsprozesse unterstützenden Ressourcen. Obgleich die Etablierung von Verfahren essenziell ist, formt sich ein Problem darin, dass Geschäftsprozesse selbst nicht Gegenstand der Behandlung sind. Auf diese Problematik wird in den Teilen II und III ausführlicher eingegangen.

Grundsätzlich ist es möglich, Rahmenwerke zum Informationssicherheitsmanagement in übergeordnete Governance-Rahmenwerke wie COBIT zu integrieren. So ließe sich eine Instanziierung der ISO 27001 auch durch den deutschen BSI IT-Grundschutz abbilden und als Mittel der durch COBIT geforderten Maßnahmen zu Errichtung und Erhaltung von Informationssicherheit adressieren. Eine Gegenüberstellung verschiedener relevanter Rahmenwerke soll in Kapitel 6 erfolgen.

3.5 Zusammenfassung

Sicherheit ist ein mehrschichtiger Begriff und muss in einen Kontext gesetzt und als Prozess verstanden werden, obgleich die Literatur überwiegend eine Definition als Zustand vorsieht. IT-Sicherheit ist ein Teilbereich der Informationssicherheit, während Compliance eigenständig und als Konformi-

tät mit externen Auflagen angesehen werden kann. Sicherheitsmanagement beinhaltet entsprechend der aufgeführten Teildefinitionen sowohl organisatorische (prozessuale und personelle) als auch technische Aspekte.

4 Föderalismus

Dieses Kapitel dient der Erfassung und der Diskussion von in der Literatur verwendeten Begrifflichkeiten, Herangehensweisen und Technologien für Föderalismus sowie der Einigung auf deren Bedeutung und Verwendung in der vorliegenden Arbeit.

4.1 Bedeutung

Gemäß [WS04] definiert sich eine Föderationen über Kooperationen von Unternehmen, und diese wiederum als *„[…] mittel- bis langfristige ausgelegte Formen vertraglich geregelter Zusammenarbeit rechtlich selbstständiger, autonomer Unternehmen“*, wobei diese Zusammenarbeit einen gegenseitigen Nutzen haben muss.

4.2 Zweck und Zielsetzung

Symbiotische Beziehungen werden naturgemäß eingegangen, sobald Zeit-, Wissens- oder sonstige Marktvorteile erzielt werden können. Entsprechend stellen Föderationen eine Ressourcengemeisnchaft dar. Diese resultiert aus der engen Zusammenarbeit der beteiligten Organisationen. [WS04]

Letztlich zielen die genannten Vorteile auf das Einsparen von Kosten, beispielsweise durch die Nichtdurchführung von Qualitätskontrollen, auf Basis von Vertrauen ab. Die Notwendigkeit und Realisierung von Kontrolle und Vertrauen in Föderationen soll später detaillierter betrachtet werden.

4.3 Kooperationstypen

Grundsätzlich können föderative organisatorische Zusammenschlüsse verschiedene Formen annehmen. Darunter fallen klassische Unternehmenskooperationen und strategische Allianzen, formale Zusammenschlüsse wie Joint Ventures, aber auch Abkommen, welche über Lizenzgebung und -nutzung definiert sind. Wirtschaftliche und räumliche Grenzen zwischen Organisationen verschwimmen durch Bezug externer Leistungen am Markt über den Einsatz von IKT. [WS04]

In Hinblick auf die spätere Absicherung ist jedoch auch die Ausrichtung der jeweiligen Kooperation von Bedeutung. In [WS04] wird hier unterschieden in horizontale, vertikale und diagonale Kooperationsrichtungen:

- Horizontale Kooperation: symbiotische Zusammenarbeit von zwei oder mehr Unternehmen gleicher Branche und Stufe der Wertschöpfungskette (beispielsweise Forschungskooperationen, Schulungseinrichtungen, etc.)
- Vertikale Kooperation: symbiotische Zusammenarbeit von zwei oder mehr Unternehmen gleicher Branche und aufeinanderfolgenden Stufen der Wertschöpfungskette (klassische Lieferantenbeziehungen, beispielsweise in der Produktion)
- Diagonale Kooperation: symbiotische Zusammenarbeit von zwei oder mehr Unternehmen unterschiedlicher Branche und Stufe der Wertschöpfungskette (als eine kostensparende Form der Anreicherung der eigenen Wertschöpfung, beispielsweise durch Kooperation eines Hotels mit einem Internetprovider für günstige WLAN-Konditionen für Hotelgäste)

Eine Kooperation von Unternehmen unterschiedlicher Branche und gleicher Stufe in der Wertschöpfungskette wird naturgemäß als nicht sinnvoll angesehen. Kooperieren mehr als zwei Unternehmen miteinander, wird von *Netzwerken* gesprochen.

4.4 Kooperationspartnerwahl

Der Ausbildung einer sinnvollen Kooperation müssen verschiedene Aktivitäten vorgeschaltet sein. Eine Kooperation dient keinem Selbstzweck, sondern stellt eine Problemlösung dar. Hierzu muss sich jedes Unternehmen über die eigenen Defizite (beispielsweise im Bereich der Technologien, des Wissens, des Kundenstamms, etc.) bewusst sein. Diese Probleme sollte die Kooperation später wechselseitig beheben können.

Ist dies der Fall, so wandeln sich die Defizite automatisch in Vorteile der Kooperation um. Ist dies nicht der Fall, könnte die Einbeziehung weiterer Unternehmen sinnvoll sein. Eine tatsächliche Kooperation ist aber nur dann gegeben, wenn alle beteiligten Partner Vorteile aus der Zusammenarbeit ziehen. Diese Vorteile müssen dabei stets gegen die Nachteile, beispielsweise die steigende Abhängigkeit, verglichen werden. In einer Kooperation sollten die Vorteile gegenüber den Nachteilen wechselseitig überwiegen.

Dieser Vergleich ist jedoch nicht trivial, da er einer intensiven Bewertung verschiedener Faktoren des Kooperationspartners bedarf. Diese Faktoren stehen in Abhängigkeit von der Geschäftssemantik. So können beispielsweise Marktposition, Unternehmensgröße oder örtliche Ansiedlung(en) des Unternehmens eine wichtige oder weniger wichtige Rolle spielen.

Nach der Identifikation und der Bewertung dieser Faktoren bildet sich über den Vergleich mit den eigenen Defiziten direkt heraus, ob eine Kooperation aus Sicht des eigenen Unternehmens sinnvoll ist. Ist dies der Fall, gilt dies jedoch nicht zwangsläufig auch für das Partnerunternehmen. Auch dieses muss einen identischen Partnerauswahlprozess durchlaufen. [WS04]

4.5 Vertrauen als Notwendigkeit

Alle Formen der Kooperation haben gemein, dass einerseits enorme Mehrwerte geschaffen werden, zeitgleich jedoch starke Abhängigkeiten und Risi-

ken durch *opportunistische Ausnutzung* entstehen können [PRW03]. Entsprechend müssen alle beteiligten Partner einer föderativen Umgebung bereit sein, einen potenziellen Vertrauensbruch zu akzeptieren, um die Vorteile einer Kooperation nutzen zu können.

Bereits an dieser Stelle lassen sich Parallelen zum klassischen Risikomanagement ziehen. Die *Gefährdung Vertrauensbruch*, beispielsweise ausgelöst durch Ausnutzung vertraulicher Informationen, die einem Partner zur Verfügung stehen, hätte für die betroffene Organisation eine wertmäßig vergleichbare *Schadenshöhe*, wie es für die ausnutzende Organisation an wertmäßigem Vorteil bedeuten könnte. Die *Wahrscheinlichkeit*, dass diese Gefährdung diesen Schaden zur Folge hat, wird überwiegend durch die Reife der Kooperationspartner bestimmt [RC70]. Entsprechend dieser beiden Faktoren bestimmt sich das jeweilige *Kooperationsrisiko*.

Diesem Risiko wird durch Maßnahmen wie dem Abschluss von Verträgen begegnet, welche beispielsweise potenzielle Einnahmeverluste durch belastbare Einigung auf Verwendung von Materialien, Nichtangriffsabreden und ähnliche Paragraphen beinhalten können. Resultieren können finanzielle Forderungen im Falle der Verletzung eines solchen Vertrages. Solche Maßnahmen greifen jedoch stets erst im Schadensfall.

Die gewissenhafte Auswahl eines vertrauenswürdigen Vertragspartners vorausgesetzt, besteht kein präventives Mittel zur Abwehr von Vertrauensbruch. Reinhard K. Sprenger [Spr07] beschreibt das Vertrauen von Menschen, die gewählt haben miteinander zu arbeiten, nicht als naiv, sondern als *„reflektiert und kalkuliert“*.

In Föderationen bleibt Vertrauen entsprechend absolut notwendig und kann nicht durch betriebswirtschaftlich sinnvolle Maßnahmen ersetzt werden. Reputation und Dauer der Beziehung sind zusätzliche Einflussfaktoren für Vertrauen.

4.6 Vertragsformen

Das Vertrauen richtet sich insbesondere an die Erwartung, dass ein Kooperationspartner seine Verantwortung zur Unterstützung des Geschäftsprozesses wahrnimmt. Wie erwähnt bildet Vertrauen zwar die Grundlage für eine Kooperation, das Risiko des Vertrauensbruchs wird oft jedoch zusätzlich durch Verträge gemindert.

Entsprechend sollte ein Kooperationsvertrag stets die Erwartung an und nötige Rahmenbedingungen für die Kooperation beinhalten. Auch Privilegien, beispielsweise hinsichtlich der Aufteilung von Gewinnen, kann in diesem Vertrag enthalten sein. Letztlich sind auch Sanktionen für die Durchsetzung der Vertragspflichten benannt. In [WS04] werden folgende Vertragsformen für Föderationen benannt:

- Non-Disclosure: definiert die Pflicht zur Geheimhaltung bezüglich der über die Kooperation erhaltenen Informationen sowie der Übermittlung relevanter Informationen an den Partner. Ziel ist die Nichtverwendbarkeit dieser Informationen durch Dritte.
- Non-Compete: verpflichtet die Vertragspartner, nicht am Markt zu konkurrieren, insbesondere unter Verwendung von Informationen, die über die Kooperation erhalten wurden.
- Service Level Agreements (SLA): definiert Art, Umfang und Handhabung von Services sowie ihrer Preise, der Laufzeit, Verfügbarkeitsanforderungen und Sicherheitsparameter. Dokumentation und Eskalationsmechanismen können ebenso beschrieben werden wie potenzielle Entschädigungsleistungen.

IBM definiert ferner das Web Service Level Agreements (WSLA) Rahmenwerk [LRD03] zur Beschreibung von SLA durch XML. Inbegriffen sind neben den Erwartungen auch Metriken für deren Einhaltung. Hierüber kann die Steuerung von IT-Operationen automatisiert werden.

4.7 Organisation

Die gesichtete Literatur [WS04, PRW03, RM97] bestätigt, dass modulare Organisationsformen eine klare Voraussetzung für Föderierung sind. Dies rührt aus der Tatsache, dass ein sich permanent wandelnder Markt, welcher zusätzlich sich ständig wandelnden Anforderungen unterworfen ist, auch automatisch Planungsunsicherheit bedeutet. Ein Organisationsverbund, bestehend aus symbiotischen Unternehmen, das heißt eine horizontale und modulare Gesamtausrichtung, kann die übergeordneten Aufgaben durch Aufteilung in Teilaufgaben schneller bewältigen, hat kürzere Reaktionszeiten und ist damit insgesamt effizienter.

Abbildung 4.1 verdeutlicht unterschiedliche Organisationsformen, welche bei der jeweiligen Konstellation aus Produktkomplexität und Marktunsicherheit effizient sind. Eine Planung der organisatorischen Aufstellung kann im Falle hoher Produktkomplexität und gleichzeitig hoher Marktunsicherheit nicht hinreichend durchgeführt werden. Entsprechend ist zunächst eine Trennung in verteilte Kompetenzen anzustreben, welche nicht länger durch hierarchisch geführte Fachabteilungen realisiert werden kann.

Gleichzeitig sollten diese beteiligten Kompetenzen möglichst wenig mit sich selbst agieren und möglichst viel Energie in Richtung der Wertbeitragslieferung fließen lassen. Die Ausrichtung der Organisationen erfolgt entsprechend an den Geschäftsprozessen. Dieser Fakt stellt einen Grundbestandteil für das zu entwickelnde Informationssicherheitsmanagementsystem in dieser Arbeit dar. Ziel ist die Reduktion von Transaktionskosten durch Verminderung von Schnittstellen in Richtung des Wertschöpfungsprozesses.

Dies schafft typische Probleme wie Kommunikationsbarrieren, Zielkonflikte und Liegezeiten zwischen (Fach-)Abteilungen ab, welche als eine wichtige Ursache für mangelhafte Wettbewerbsfähigkeit eines Unternehmens identifiziert wurden [RM97].

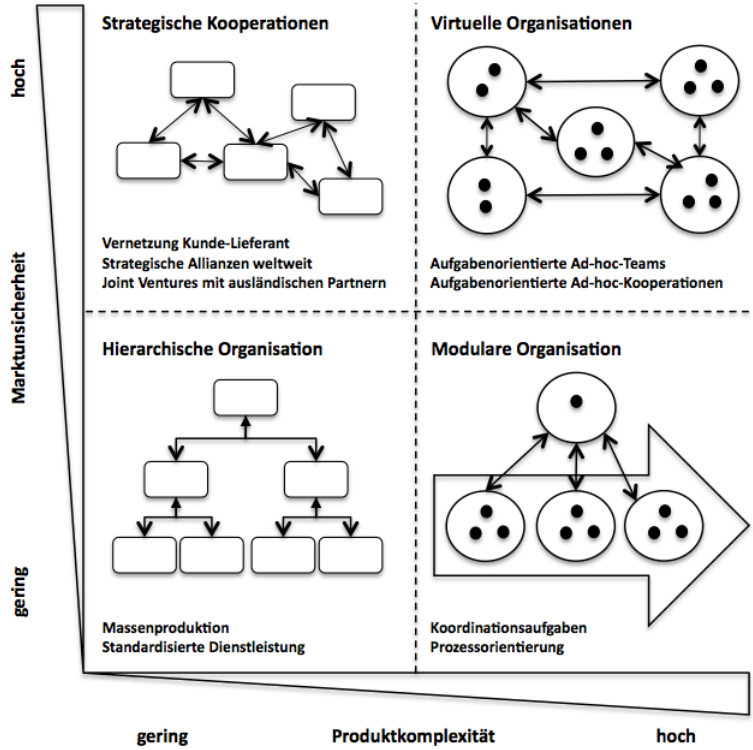

Abbildung 4.1: Organisationstypen nach [PRW03], modifiziert

Eine Ausrichtung an den Geschäftsprozessen über mehrere beteiligte Organisationen erfordert wiederum eine Aufteilung der Geschäftsprozesse in Module. Diese Module besitzen einen Kern und Schnittstellen und kennzeichnen sich durch starke Abhängigkeiten innerhalb der Module sowie schwache Abhängigkeiten zwischen den Modulen [WS04].

In Kapitel 11 sollen diese Grundgedanken als Ausgangsbasis für die Konstruktion des ISMS verwendet werden.

4.8 Menschen und Aufgaben

Neben den rein organisatorischen Leitbildern föderierter Umgebungen stellen Menschen einen zentralen Gegenstand in der erfolgreichen Aufgabenbewältigung innerhalb einer Unternehmenskooperation dar.

Innerhalb dieser Umgebung muss eine Vielzahl von Menschen nicht nur viele operative Tätigkeiten, sondern auch ein hohes Maß an Eigenverantwortung tragen. Nachfolgend sollen Aufgaben und Rollen von Kunden, Mitarbeitern und der Führung innerhalb einer organisationsübergreifenden Kooperation beschrieben werden.

4.8.1 Mitarbeiter

Steigende und vor allem wechselnde Anforderungen des Marktes bedeuten automatisch ebenso steigende Anforderungen an die fachlichen und persönlichen Fähig- und Fertigkeiten der Mitarbeiter.

Aufgrund der in Abschnitt 4.7 erwähnten Ad-hoc-Ausrichtung von Teams im Falle hoher Marktunsicherheit und Produktkomplexität, kann eine hinreichende Kontrolle der Arbeit von Mitarbeitern durch Führungskräfte nicht geleistet werden.

Hieraus wächst eine neue Verantwortung für den Mitarbeiter und seiner Rolle im Unternehmen. Dies hat jedoch zur Folge, dass sich auch die Aufgaben der Führungsebene verändern müssen.

4.8.2 Führung

Grundsätzlich muss die Leistung der Mitarbeiter durch Handlungen der Führung am Markt erhalten und erhöht werden. Mitarbeiter müssen entsprechend gefördert, gefordert und weiterentwickelt werden, was die Führungsebene durch Coaching der Mitarbeiter unterstützen kann. Ziel des

Coaching besteht hier jedoch nicht länger nur in der reinen Assistenz beim Verständnis der zugeteilten Aufgabe, sondern dem In-Einklang-Bringen der Interessen des Mitarbeiters mit den Interessen im Unternehmen. [WS04]

Mitarbeiter müssen den Sinn der Arbeit in Bezug auf das übergeordnete Geschäftsziel verstehen lernen und sich ihrer Rolle in der Föderation bewusst werden. Das Ziel der Führung besteht hier also darin, Mitarbeiter durch Übergabe von Verantwortung und Coaching dazu zu bringen, selbstständig und eigenverantwortlich auf das Gesamtziel zuzugehen.

Der Managementberater Sprenger motiviert hier in [Spr12] eine bevorzugte Verwendung des (präziseren) Begriffes *Problem* vor dem Begriff *Ziel*. Dies wird begründet mit der Tatsache, dass ein Problem Gewicht hat und durch die Mitarbeiter gelöst werden *muss*, ein Ziel jedoch leichtgewichtig ist und die Erreichung nur wünschenswert wäre. Aus diesem Gedanken kann ein Führungsinstrument abgeleitet werden, welches die intrinsische Motivation der Mitarbeiter durch gemeinsame Problemdefinition entstehen lässt.

Die Kontrolle der Wirksamkeit geschieht entsprechend nicht länger auf der Ebene des Überprüfens einzelner Arbeitserzeugnisse, sondern auf Ebene der Überprüfung und Einflussnahme selbstorganisierter Teams und deren Beitrag zum Unternehmenserfolg. Übrige Managementaufgaben sind hiervon jedoch unberührt. Insbesondere geht die Realisierung von Prozessen zur Etablierung und Aufrechterhaltung von Informationssicherheit mit der Betreuung der Wirksamkeit der Kooperation einher. Hier werden Maßnahmen gesteuert, welche die fortwährenden Beiträge der Organisationen an den Geschäftszielen sicherstellen.

Entsprechend lässt sich bereits hier ein potenzieller Mehrwert durch die Etablierung selbstorganisierter Teams zur Realisierung von Prozessen für Planung, Durchführung, Prüfung und Verbesserung der Informationssicherheit ableiten. Die Funktion der Führung wäre unverändert, lediglich die rein inhaltliche Ausgestaltung der aufgestellten Teams und ihrer Aufgabe ist eine andere.

4.8.3 Kunden

Letztlich sind aber nicht nur die Mitarbeiter von Herstellern und Lieferanten Teil der Menschen, die von der Kooperation eingeschlossen werden. Eine zunehmende Rolle kommt auch den Kunden zu, welche sich zunehmend vom Konsumenten zum Entwicklungspartner wandeln. Kunden sind bereits heute an der Spezifikation, Konfiguration und Entwicklung der Produkte und Dienstleistungen beteiligt [RP02, SH00].

Ein Beispiel aus der Produktion: Ein Endkunde definiert qualitative, preisliche und zeitliche Anforderungen eines Produktes für den Hersteller, dieser Hersteller gibt alle Parameter weiter an den/die Lieferanten [WS04].

Entsprechend wächst ein gemeinschaftliches Team aus Kunde, Hersteller und Lieferanten. Hierdurch wird die Ausrichtung des Produktes an reellen Marktbedürfnissen, und damit Innovation, gefördert. Das Vertrauen ist hier erneut eine lohnenswerte Investition für bestehende und künftige Kooperationen.

4.8.4 Querschnittsaufgaben

Alle an der Föderation beteiligten Personen sind mit der Adressierung von Anforderungen des Marktes durch Übertragung von Entscheidungskompetenz über Prozesse an Prozessverantwortliche (Process Owner) betreut. Aus diesem Netz aus Verantwortlichkeiten, welche die Prozesse ihrer jeweiligen Organisation verändern und anpassen können, wächst ein Netz aus befugten Ansprechpartnern, welche einen gemeinsamen Mehrwert für die Organisation schöpfen können.

Diese Partner sollten ihrerseits Partner zur Durchführung von Reviewmeetings akquirieren, welche die Auswirkungen von potenziellen Veränderungen auf bestehende Prozesse analysieren und Handlungen beschließen.

Auf Basis dieser fortwährenden Optimierung der Unternehmensprozesse, ausgehend von den Anforderungen am Markt und der resultierenden Wertschöpfung der Geschäftsprozesse wächst ein zunehmender Kooperationsnutzen auf Basis von Vertrauen zwischen Kunden, Mitarbeitern und der Führungsebene aller beteiligten Organisationen.

Dies geschieht jedoch nicht allein durch Organisationsformen, Prozesse, Aufgaben und Menschen. Auch sind Technologien beteiligt, welche die gewählte Kooperationsform und die jeweiligen Marktbedürfnisse unterstützen, und maßgeblich den Reifegrad der realisierten Prozesse beeinflussen können, da Abläufe automatisiert und vereinfacht werden können.

4.9 Zusammenfassung

Föderationen sind Kooperationen selbstständiger Unternehmen zum wechselseitigen Nutzen. Nützlich äußern sich beispielsweise Zeit-, Wissens- oder andere Marktvorteile zur Kostenersparnis. Es sind symbiotische Zusammenarbeit von zwei oder mehr Unternehmen gleicher und/oder unterschiedlicher Branche sowie gleicher und/oder unterschiedlicher Stufe der Wertschöpfungskette denkbar. Die Wahl eines Kooperationspartners ist abhängig vom Wissen über wechselseitige Vorzüge und Defizite. Wertvoll ist eine Kooperation bei optimaler gegenseitiger Ergänzung. Vertrauen ist in einer Föderation unabdingbar, dennoch sollten Verträge geschlossen werden, die das Risiko des Vertrauensbruchs vermindern. Hier sind Non-Disclosure-, Non-Compete- sowie Service-Level-Agreements denkbar.

Organisationen bilden unterschiedliche Organisationstypen in Abhängigkeit der Faktoren Produktkomplexität und Marktunsicherheit heraus. Im Extremfall dienen virtuelle Organisationen als eine Möglichkeit zur Ausbildung von Ad-hoc-Teams zur aufgabenorientierten gemeinsamen Problemlösung. Den Mitarbeitern werden andere Arten von Aufgaben zugeteilt,

die durch Selbstverantwortung geprägt sind. Die Führung der Mitarbeiter muss diesem Umstand durch geeignete Mittel wie dem In-Einklang-Bringen der Organisationsinteressen mit den Interessen der Mitarbeiter gerecht werden. Das Team besteht letztlich aus Herstellern und Lieferanten, aber auch dem Kunden. Diese Form der Zusammenkunft erhöht die Möglichkeiten zur Zielerreichung ebenso wie die Risiken des Missbrauchs des durch Technologie verarbeiteten Informationen. Mögliche Technologien sollen im Folgenden vor- und gegenübergestellt werden.

5 Technologien und Prozessunterstützung

Gemäß [KMW00] wird das in Abschnitt 4.5 zentralisierte *Vertrauen* von Menschen nicht nur auf andere Menschen, sondern auch auf technische Systeme und Organisationen bezogen. IT-Systemen kommt daher eine wichtige Bedeutung zu, da sie nicht nur dem allgegenwärtigen Vertrauen, sondern auch Effizienz und Effektivität der (automatisierten) Zusammenarbeit Rechnung schuldet.

IT-Systeme werden wiederum bestimmt von den beteiligten Technologien. Die für eine Kooperation notwendigen flexiblen Prozesse benötigen zur Unterstützung eine ebenso flexible, technische Systemarchitektur. Zentral ist hier die Sicht auf eine *Service-orientierte Architektur (SOA)*. SOA beschreibt jedoch keine eigene Technologie, sondern lediglich ein Architekturparadigma, losgelöst von konkreten Implementierungstechniken. SOA ist somit ein Sinnbild für verschiedene Formen technischer Abstraktion und ihrer Nutzbarkeit. Grundsätzlich bestehen verschiedene Ebenen der Integration von IT-Infrastrukturen [WS04]:

- Integration von Informationen: Abgleich von verteilten Daten der Kooperationspartner
- Web Services und Portlets: Wiederverwendung technischer Bausteine zu neuen, aggregierten Geschäftslösungen
- End-to-End-Prozesse: Verknüpfung von Services innerhalb und außerhalb einer Organisation
- E-Service-Strategie: Vorlage zur Beschreibung der Summe aller durch eine Organisation bereitstellbaren Leistungen

Diese Ebenen erfordern jeweils in unterschiedlichem Maße Abstraktion. Diese Abstraktion kann wiederum unterschiedlich umgesetzt werden. Einige Möglichkeiten sollen nun erläutert und später klassifiziert werden.

5.1 Abstraktion durch Server

Eine triviale Form der Abstraktion wird durch die Client/Server-Technologie realisiert. Diese charakterisiert sich durch die Aufteilung von Präsentations- und Verarbeitungsteilen auf Workstations und Server. Durch die Steigerung der Leistung der Netzwerkverbindungen kam Mitte der 90er Jahre zusätzlich der Gedanke zur Trennung von Geschäftslogik und Datenhaltung hinzu. Entsprechend existiert bis heute namentlich die *3-Tier-Architektur*.

Durch die Heterogenität der Clientumgebungen und die zunehmende Größe von Applets kam es später zu einer teilweisen Rückverlagerung der Präsentationslogik auf einen zentralen Server, dort jedoch in einer separaten Schicht. Die in dieser Schicht verwendeten Technologien sind Skriptsprachen wie Java Server Pages (JSP) und Active Server Pages (ASP). Durch diese Entwicklung entstand die *4-Tier-Architektur*. [WS04]

Zusätzlich kamen später Web Services hinzu, welche die technologische Basis für automatische Clients waren, genannt *Consumer*. Diese Consumer konnten Services einer anderen Schicht vollautomatisch nutzen. Services werden in [WS04][1] annähernd mit Anwendungen gleichgesetzt. Ein Dienst ist jedoch vielmehr die IT-Repräsentation fachlicher Funktionalität [Jos08] mit definierter Schnittstelle. Abbildung 5.1 zeigt die beteiligten Schichten.

Jede beteiligte Zone (Consumer, Portal, Prozess, Ressourcen) stellt der jeweils anderen Zone Services zur Verfügung. Dies erlaubt die Konfiguration des Gesamtsystems nach den Kriterien Skalierbarkeit, Wiederverwendbarkeit, Performanz und Sicherheit.

[1] Seite 33

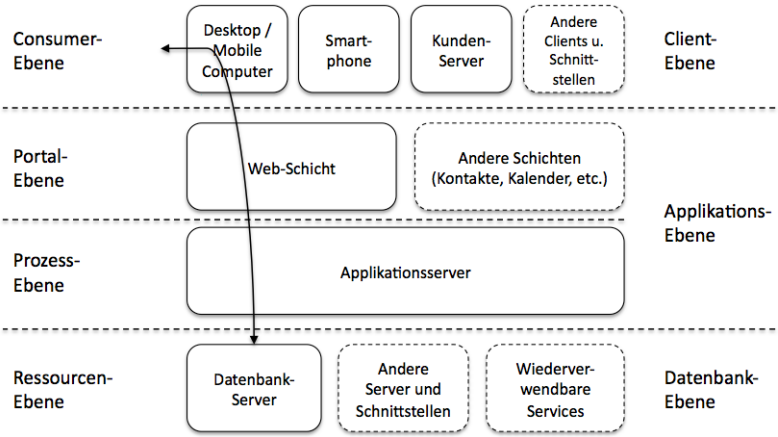

Abbildung 5.1: Abstraktion durch Server [WS04], modifiziert

5.2 Abstraktion durch Middleware

Das Prinzip der Schichtung von Anwendungsebenen nach gestaffelten Abstraktionsgraden erhielt durch Middleware eine neue Ausprägung. Ähnlich der Abstraktion durch Server werden zwar grundsätzlich Kapselungen von geschichteten Systemen angestrebt. Es wird aber zusätzlich adressiert, dass die Definition von Schnittstellen allein nicht immer ausreichend ist, um beispielsweise Legacy-Systeme anzusprechen. Hier werden Adapterschichten relevant, welche den Zugriff vereinfachen und die Wartung auf diese Schichten beschränken, die Wartbarkeit entsprechend insgesamt erhöhen.

Diese *Middleware* liegt oberhalb der Betriebssystemschicht und bietet allgemein verwendbare Funktionalitäten an. Middleware kann nach [WS04] unterteilt werden in:

- Erweiterungen des Betriebssystems: beispielsweise Application Ser-

ver, Portal Server, etc.

- Frameworks als Koppler zwischen Subsystemen: beispielsweise Content Server, Konnektoren, etc.

Abbildung 5.2 zeigt die interagierenden Schichten.

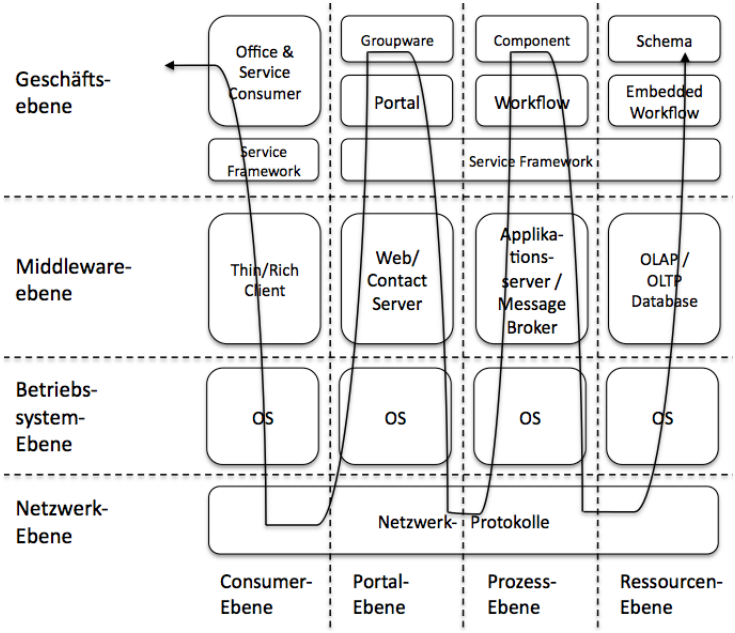

Abbildung 5.2: Abstraktion durch Middleware [WS04], modifiziert

Die Middleware-Komponenten des ersichtlichen Schemas können durch Einsatz von Protokollen wie SOAP[2] auch heterogen ausgerichtet sein. Prominente Beispiele für Middleware sind J2EE als Plattform von Java-Applikationsservern und .NET als proprietäre Laufzeitumgebung, Framework und Toolset der Firma Microsoft.

[2]Simple Object Access Protocol

Das Ergebnis der Nutzung von Middleware ist die leichtere Entwicklung domänenspezifischer Standardlösungen. Waren im Jahr 1995 Standardlösungen noch überwiegend vollständige Eigenentwicklungen bestimmter Hersteller für beispielsweise die Bereiche Finanzen und Kosten, waren zehn Jahre später individuelle Branchenlösungen durch herstellerspezifische Middleware möglich. Diese Middleware unterstützte teilweise auch Sprachen zur Ablaufsteuerung, wie die *Business Process Execution Language (BPEL)*, was zu einer zusätzlichen Erhöhung der Interoperabilität und Automatisierbarkeit führte.

5.3 Abstraktion durch Business-Objekte

Im Bereich der Softwareentwicklung bot das Paradigma der Objektorientierung (OO) viele Vorteile, da oft benötigtes Verhalten einmalig als Klasse definiert, gegebenenfalls benötigte Varianten über Vererbung bezogen, und letztlich als Objekt instanziiert werden konnte. Über die Gedanken der Vorteile von Abstraktion, Kapselung, Modularität und Hierarchie liegt der Wunsch nahe, dieses Paradigma auf die Betriebswirtschaft übertragen zu wollen.

Objekte bestehen grundsätzlich aus ihrem Status (der Summe ihrer Eigenschaften, das heißt ihre aktuellen Datenwerte), ihrem Verhalten (der Art und Weise ihrer Reaktion auf Funktionsaufrufe) und ihrer Identität (auch zwei unterschiedliche Objekte mit gleichem Status und Verhalten sind nicht identisch) [Boo95]. Ferner können sie den Zustand ihrer Datenbasis lesen und verändern.

Hier stellt sich die Frage, ob im Bereich der Betriebswirtschaft für potenzielle Objekte eine ausreichende Abstraktionsebene vorliegt, die das OO-Paradigma fordert. In der Betriebswirtschaft treten jedoch sehr häufig Spezialfälle auf. Zudem existiert ein hoher Vernetzungsgrad der beteiligten Objekte. Der Status eines betriebswirtschaftlichen Objektes definiert sich oft

über einen sehr großen Teil der Datenbank. Ein großer Teil dieser Datenbestände wird jedoch auch von anderen Objekten genutzt. Eine Abgeschlossenheit der notwendigen Daten ist daher nicht gegeben. Abbildung 5.3 visualisiert das Problem des Zugriffs unterschiedlicher Instanzen (Objekte) auf Datenbestände.

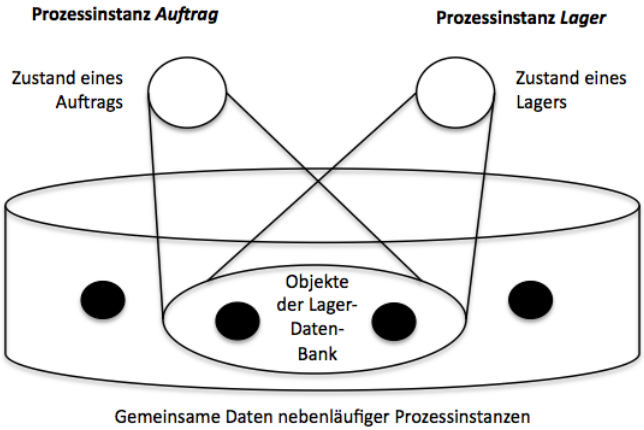

Abbildung 5.3: Abstraktion durch Business-Objekte [WS04], modifiziert

Wie ersichtlich wird, teilen sich Objekte potenziell die gleiche Datenbasis. Zusätzlich können diese Objekte die vorrätigen Daten auch verändern. Es bestünde entsprechend eine Abhängigkeit des Zustands eines Objektes vom Zustand anderer Objekte, woraus ein nicht deterministisches, und damit inkonsistentes Verhalten gegenüber dem OO-Paradigma resultiert. Diese Sichtweise wird in verschiedener Literatur bestätigt [Fie00].

Entsprechend kann eine Operation auf einem betriebswirtschaftlichen Objekt unvorhersehbare Folgen haben, woraus kein konsistentes Vorhersage- oder Planungsmodell für Geschäftsabläufe entstehen kann. Eine Kompensierung dieses Umstandes durch standardisierte Prozesse wäre einem Un-

ternehmen nicht zuträglich, da Marktvorteile stark abhängig von optimierten Prozessen sein können. Ferner stellt Prozessflexibilität eine zentrale Voraussetzung funktionierender Unternehmenskooperationen dar. Im Bereich der Analysewerkzeuge sind Business-Objekte jedoch denkbar. [WS04]

5.4 Abstraktion durch Workflows

Ein Workflow beschreibt die Teilautomatisierung eines Geschäftsprozesses durch Unterstützung von Workflow-Management-Systemen (WMS) und anderen Applikationen. Er enthält eine Beschreibung von Aktivitäten und Steuerungsinformationen. Diese Beschreibung wird vom WMS interpretiert, welche als Middleware zur Koordinierung von Personen und Anwendungen bezeichnet werden kann. Es initiiert einen Workflow als Instanz, eingeleitet durch ein bestimmtes Ereignis, und startet diese Instanz. [WS04]

Auf Basis der angelaufenen Workflow-Instanz werden vom WMS die im Workflow definierten Aktivitäten auf einzelne Mitarbeiter verteilt, deren Bearbeitung kontrolliert und Nachrichten zwischen den beteiligten Mitarbeitern transportiert. Auch können konkrete Abläufe, welche die Interaktion mit anderen Anwendungen zum Inhalt haben, gesteuert werden. Die Hauptkomponente eines WMS ist die *Workflow-Engine*. Diese ist für die Steuerung und Überwachung laufender Instanzen zuständig. [WS04]

Das Ziel des Einsatzes von WMS ist entsprechend die Wiederverwendbarkeit statischer funktionaler Komponenten und die Modifizierbarkeit des Ablaufes durch die Beschreibung von Workflows. Das Gesamtsystem kann als Folge von Transformationen aufeinanderfolgender Eingabeströme verstanden werden. Transformiert werden hierbei Daten von beteiligten Programmen, welche voneinander unabhängig sind und sequenziell ablaufen. Abbildung 5.4 zeigt die Integration eines Workflows in ein System aus Client und Server. [WS04]

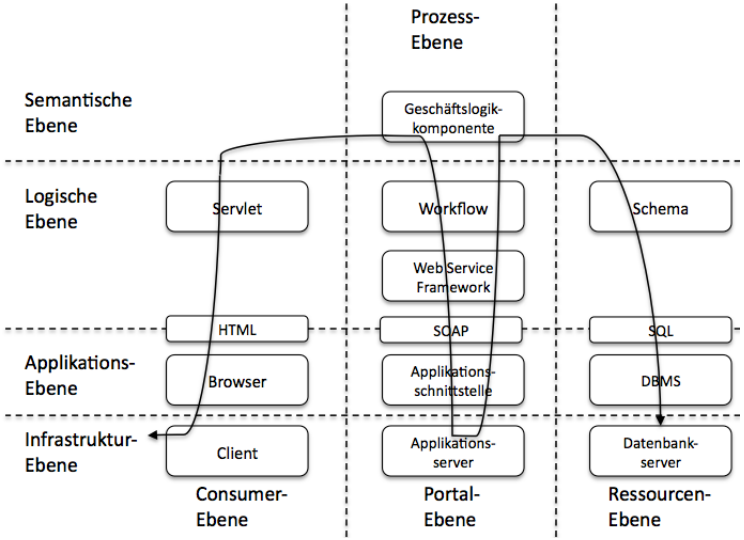

Abbildung 5.4: Abstraktion durch Workflows [WS04], modifiziert

Kritisch zu beurteilen ist die Abstraktionsebene von Workflows, die durch die starke Abhängigkeit von den beteiligten Komponenten (beispielsweise dem Datenmodell im DBS oder heterogenen übertragenen Datenformaten) gekennzeichnet ist. Eine Abstraktion ist durch die normalisierende Transformation der Daten zwar vorhanden, sie ist jedoch vergleichsweise schwacher Natur.

5.5 Abstraktion durch die Cloud

Der gegenwärtige Stand der Technik sieht letztlich eine vollständig abstrahierte Form des Zugangs zu IT-Infrastruktur, Plattformen und Anwendungen vor. Dabei kann der zur Erledigung von Aufgaben relevante Zugang zu Ressourcen bedarfsgerecht beliefert und abgerechnet werden. Dies umfasst

beispielsweise Zugang zu großer Rechenkapazität, Datenspeicher, Netzwerkkapazitäten oder kompletten Anwendungen.

Die jeweiligen Ein- und Ausgabeinformationen werden jeweils über das Netzwerk bezogen. Somit reduziert sich der Kontakt zur IT-Infrastruktur auf den korrekten Umgang mit Schnittstellen und Protokollen. Es resultiert eine fast ausschließlich auf Angebot und Nutzung einer Dienstleistung reduzierte Sicht auf das Gesamtsystem, was die für eine Organisation gegenwärtige Komplexität drastisch reduziert und letztlich hohe Kostenersparnisse zur Folge hat. Abbildung 5.5 veranschaulicht die Abstraktionsebene der Cloud.

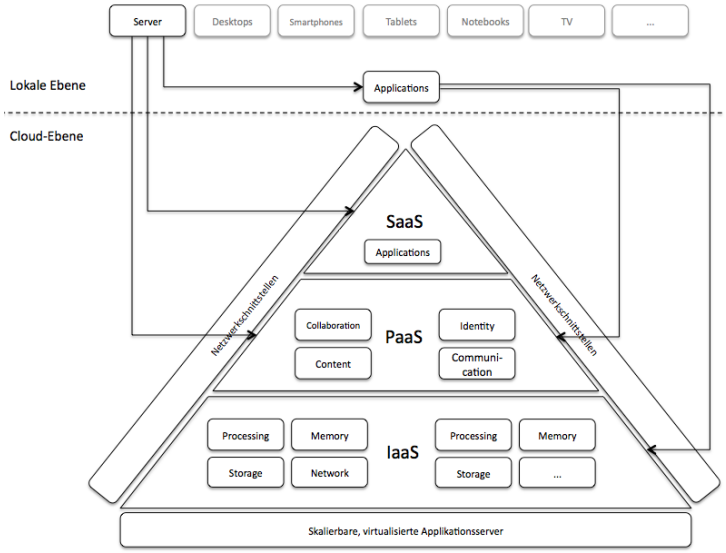

Abbildung 5.5: Abstraktion durch die Cloud

Erkennbar sind die drei Arten des Cloud-Computings, in der obere Schichten auf den unten liegenden aufbauen können, dies aber nicht müssen: In-

frastruktur, Plattform, Anwendung. Bevor die technische Realisierung zum Betrachtungsgegenstand werden kann, ist eine Betrachtung essenzieller Charakteristika für Cloud-Computing im Allgemeinen sinnvoll.

Hier lassen sich gemäß [MG09] fünf Aspekte ableiten:

- On-demand self-service: Bereitstellung von automatisiert abrufbaren Möglichkeiten zur Nutzung von Verarbeitungsleistung, Speicherung und anderen Diensten (kein Einfluss durch Personen notwendig)
- Broad network access: diese Möglichkeiten werden über das Netzwerk bereitgestellt, entsprechend ist die Anbindung über heterogene Thin- und Thick-Clients möglich (Desktoprechner, Notebooks, Mobiltelefone, etc.)
- Ressource pooling: die Ressourcen des Cloud-Providers (Storage, Processing, Memory, Network Bandwidth, Virtual Machines, etc.) sind in einem Pool verfügbar, wodurch eine hohe Effizienz bei der Verwendung dieser Ressourcen sichergestellt werden kann; technisch wird dies über Virtualisierungsmechanismen realisiert
- Rapid elasticity: es besteht eine sehr hohe Skalierbarkeit in der Zuweisung von Ressourcen abhängig von Budget und Anforderungen eines Service Consumers (Cloud-Nutzers beziehungsweise Kunden)
- Measured service: abhängig von der Art der zur Verfügung gestellten Ressourcen kann die Verwendung dieser Ressourcen auf einem abstrahierten Level gemessen, gesteuert und berichtet werden (beispielsweise aktuell verwendete CPU-Last, verwendeter Speicherplatz, verwendete Netzwerkbandbreite, ec.)

Hierzu bleibt zu erwähnen, dass durch den hohen Grad der Virtualisierung eine ebenso große Unwissenheit über die Lokation der verarbeiteten Informationen vorherrscht. Dies ist sowohl auf der „Mikroebene“ (der Rückschließbarkeit der Datenverarbeitung auf konkrete IT-Objekte wie CPU, Festplatten, Netzwerke, etc.), als auch auf der „Makroebene“ (Verarbeitung der Daten in verschiedenen Ländern) präsent.

Die technische Realisierung des Cloud-Computings lässt sich anhand der drei Abstraktionsgrade Anwendung, Plattform und Infrastruktur gemäß [MG09] durchführen und betrifft entsprechend:

- Software as a Service (SaaS): fertige Anwendungen des Konsumenten werden auf der Infrastruktur des Cloud Providers ausgeführt und den Clients der Konsumenten zugänglich gemacht
- Platform as a Service (PaaS): ausführbare Anwendungen des Konsumenten werden auf der Infrastruktur des Cloud Providers samt Editierbarkeit von Code-Bestandteilen (über vom Cloud Provider unterstützte Programmiersprachen und/oder Tools) den Konsumenten zugänglich gemacht
- Infrastructure as a Service (IaaS): alle Ressourcen (Storage, Processing, Memory, Network Bandwidth, Virtual Machines, etc.) der Infrastruktur des Cloud Providers werden den Konsumenten zur Ausführung eigener Betriebssysteme und Anwendungen zugänglich gemacht

Steuerung und Kontrolle der Ressourcen des Cloud-Providers, welche die lauffähigen Anwendungen unterstützen, liegen stets außerhalb des Einflussbereiches der Konsumenten (dies gilt in Abhängigkeit vom Typ ggf. auch für die Anwendung selbst, abzüglich möglicher offener Anwendungs- und /oder Hosting-Konfigurationsmöglichkeiten). Der Vorteil liegt stets in der Auslagerung der Verwaltung der IT sowie der nutzungsabhängigen Kostenverteilung beim Konsumieren der bereitgestellten Services. Das Risiko der Beziehung von Cloud-Services wächst jedoch aufgrund der steigenden Manipulationsmöglichkeiten proportional mit den geschäftsseitigen Vorteilen. Tabelle 5.1 stellt die verschiedenen Cloud-Abstraktionstypen einigen Kriterien gegenüber.

Schließlich kann auch gemäß [MG09] in vier unterschiedliche organisatorische Formen von Clouds, *Deployment Models*, unterschieden werden:

- Private Cloud: die Cloud-Infrastruktur wird nur für eine Organisation betrieben

- Community Cloud: von mehreren Organisationen nach bestimmten gemeinsamen Anforderungen geteilte Cloud-Infrastruktur
- Public Cloud: Cloud ist der allgemeinen Öffentlichkeit zugänglich
- Hybrid Cloud: Komposition einer oder mehrerer Cloud-Modelle als eigenständige Entität jedoch verbunden über gemeinsame Technologie zur Übertragbarkeit von Daten und Applikationen (Cloud Bursting für Load-Balancing zwischen Clouds, etc.)

Kriterium	**SaaS**	**PaaS**	**IaaS**
Anwendungs-ausführung	Cloud	Cloud und cloud-lokal	Lokal
Ressourcen	Processing	Processing	alle*
Einfluss-möglichkeiten	Anwendungs-konfiguration	Anwendung-code	Anwendungs-code, Hosting
bedarfsgerecht	wenig	teils	ja
relatives Risiko	gering	mittel	hoch

Tabelle 5.1: Klassifizierung Cloud-Abstraktionstypen (*Storage, Processing, Memory, Network Bandwidth, Virtual Machines, etc.)

Deployment-Modelle lassen sich wie in Tabelle 5.2 ersichtlich einordnen.

Kriterium	**Private**	**Community**	**Public**	**Hybrid**
Betrieb für	eine Organisation	eine oder mehrere Org.	Öffentlichkeit	unterschiedlich
Betrieb von	eigene o. fremde Org.	eigene oder fremde Org.	Public Cloud Provider	unterschiedlich
Lokalität	lokal oder entfernt	lokal oder entfernt	entfernt	lokal oder entfernt
bedarfsgerecht	ja	teilweise	nein	teilweise
relatives Risiko	gering	mittel	hoch	mittel

Tabelle 5.2: Klassifizierung Cloud Deployment Models

Die Hybrid-Cloud nimmt eine Sonderstellung ein, da sie in Abhängigkeit der realisierten Konstellation aus anderen Cloud-Modellen steht. Nachfolgend soll eine Klassifizierung aller technologischen Abstraktionsmöglichkeiten vorgenommen werden.

5.6 Klassifizierung der Abstraktionsmöglichkeiten

Tabelle 5.3 stellt die Abstraktion via Server, Middleware (MW), Business-Objekten (BO), Workflows und der Cloud gegenüber und ordnet sie in die möglichen Integrationsebenen ein.

Integrationsebene	Server	MW	BO	Workflow	Cloud
Informationen	ja	ja	ja	ja	ja
Web Services	teils	ja	ja	ja	ja
End-to-End-Proz.	nein	teils	teils	ja	ja
E-Service-Strat.	nein	nein	teils	teils	ja

Tabelle 5.3: Klassifizierung Abstraktionskonzepte nach Integrationsebenen

Wie ersichtlich wird, stellt die Cloud eine sehr hohe Abstraktionsform dar, welche geschäftsmäßige und technische Kriterien hinreichend adressieren kann. Mit jeder Abstraktion geht jedoch auch ein hohes Risiko bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen einher, welche im Rahmen der Geschäftsprozesse, welche Cloud-Dienste verwenden, verarbeitet werden. Entsprechend ist das Risiko bei der Nutzung von Cloud-Services in Relation zu anderen Abstraktionsmöglichkeiten am höchsten zu bewerten.

Nicht zuletzt existieren keine standardisierten Möglichkeiten zum Monitoring der Informationen in der Cloud. Der nachfolgende Abschnitt zeigt die Dimensionen, die beim Sicherheitsmanagement von Cloud-basierten, föderierten Geschäftsprozessen zu betrachten sind.

5.7 Dimensionen des Sicherheitsmanagements

Die erläuterten Organisationstypen, die neuen Rollen für Kunden, Mitarbeiter und der Führungskräfte sowie die beteiligten Technologien und deren Möglichkeit zur Unterstützung interner und organisationsübergreifender Prozesse stehen, wie auch vor der Föderierung, einer Vielzahl interner und externer Anforderungen gegenüber.

Das Augenmerk soll vorliegend auf den Schutzzielen der Vertraulichkeit, der Verfügbarkeit und der Integrität der über den Geschäftsprozess ausgetauschten und verarbeiteten Informationen liegen. Hinzu kommt eine allgemeine Sicht auf Compliance-Anforderungen.

Auf Compliance liegt in der vorliegenden Untersuchung zwar kein Schwerpunkt, jedoch liegt deren Erhalt ein ganz ähnliches Denken zugrunde wie dem des integrierten Risikomanagements. Auch haben Compliance-Anforderungen oft das Erreichen eines effektiven Risikomanagements zum Ziel.

Für die Adressierung der Föderierung, die aus den in diesem Kapitel aufgeführten Gründen erstrebenswert ist, und der damit verbundenen Modularisierung der Geschäftsprozesse, entsteht ein neues System aus miteinander über einen Informationsfluss verknüpften Einheiten aus Menschen, Aufgaben und Technik.

Aus diesem neuen System auf der einen Seite, und den nach wie vor präsenten Sicherheits- und Compliance-Anforderungen auf der anderen Seite, resultiert ein komplexes Betrachtungsgefügte, dem es mit Maßnahmen zur Sicherstellung der Anforderungen zu begegnen gilt. Abbildung 5.6 visualisiert dies am Beispiel des in [NF12] in Prozessmodule zerlegten Beschaffungsprozesses.

Für diese Risiko- und Compliance-Betrachtungen ist tiefgreifendes Wissen über die gerichteten Verknüpfungen der beteiligten Ressourcen – und damit letztlich den Informationsfluss zwischen den MAT-Einheiten – notwendig. Diese soll vorliegend als Governance benannt werden. Entsprechend

existiert eine Notwendigkeit zum gesamtbildhaften Management von *Governance, Risk, Compliance* – kurz *GRC*.

Für das GRC-Management innerhalb der Grenzen einer einzelnen Organisation existieren bereits verschiedene Rahmenwerke, welche in Teil II identifiziert und klassifiziert werden sollen.

5.8 Zusammenfassung

Föderative Technologien adressieren das Problem der für Kooperationen notwendigen Flexibilität der Unterstützung von Geschäftsprozessen, und damit der Agilität der Organisation. Service-orientierte Architekturen lassen sich über verschiedene Abstraktionsmöglichkeiten erreichen. Hier sind die Abstraktion durch Server, Middleware, Business-Objekte, Workflows und Cloud-Services möglich, wobei Cloud-Services die größte Abstraktionsstufe darstellen, da lediglich ein Dienst in Anspruch genommen wird und dieser zudem dediziert abgerechnet werden kann.

Ein effektives und effizientes GRC-Management muss die drei Dimensionen der Geschäftsprozesse, ihre Ressourcen (Aufgaben, Menschen, IT-Systeme bzw. Dienste und ggf. die darunterliegende Infrastruktur) sowie die jeweiligen Anforderungen (in Abhängigkeit der Schutzbedarfe) berücksichtigen. Hierbei sind die Schutzbedarfe der in der Kooperation verarbeiteten Informationen von zentraler Bedeutung. Über die Gefährdungen, insbesondere hinsichtlich Compliance bei der Verwendung von Cloud-Services, ergibt sich für jeden Geschäftsprozess eine Risikoindikation. Nach einer Sichtung und einer Einordnung vorhandener Konzepte soll dieses Problem vertieft und später eine Lösung konstruiert werden.

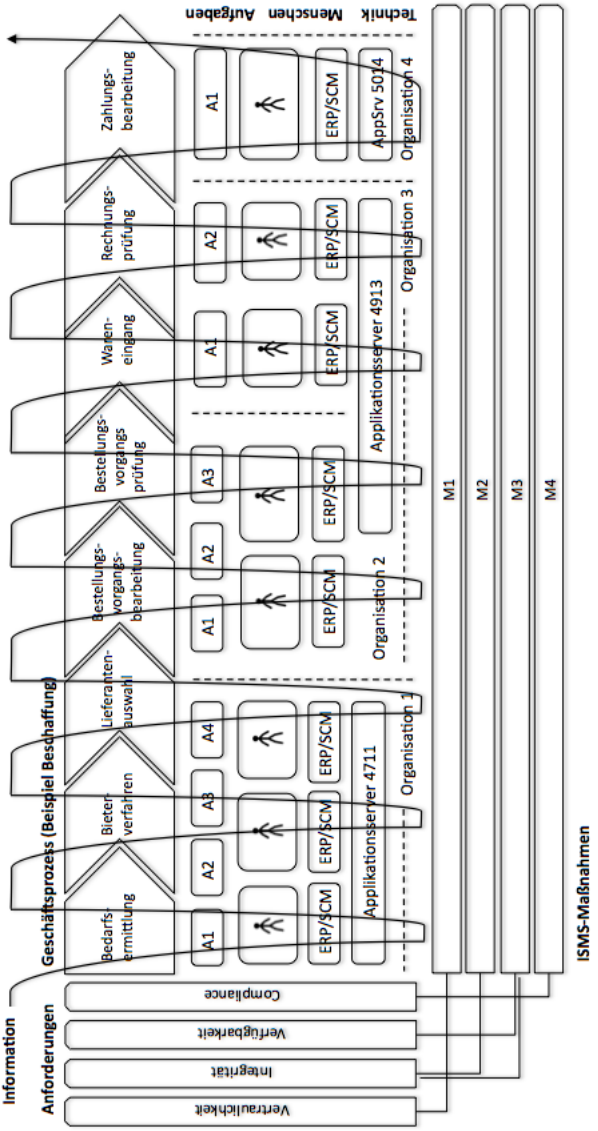

Abbildung 5.6: GRC im MAT-System eines föderierten Geschäftsprozesses

Teil II

Sichtung und Einordnung vorhandener Konzepte

Überblick Teil II

Da wie in Kapitel 1 beschrieben kein Rahmenwerk existiert, welches explizit das vielschichtige Problemgeflecht adressiert, welches von den Themen aus Teil I aufgespannt wird, sollen in einem nächsten Schritt die bislang vorhandenen Konzepte zum methodisch gestützten Sicherheitsmanagement von Informationen in Organisationen identifiziert, erläutert und klassifiziert werden.

Kapitel 6 liefert eine Übersicht über Rahmenwerke, welche hierfür relevant sind. In Kapitel 7 werden Kriterien zur Klassifizierung dieser Rahmenwerke abgeleitet und die Klassifizierung durchgeführt.

6 Traditionelle Rahmenwerke

Verschiedene Arten von Rahmenwerken können gewinnbringende Einflüsse auf die zu erarbeitende Lösung geben. Zunächst scheint es aufgrund der kontrollierenden Natur eines Informationssicherheitsmanagementsystems sinnvoll, allgemeine interne Kontrollsysteme zu untersuchen. Schließlich bieten sich klassische ISMS sowie die weit verbreitete IT Infrastructure Library (ITIL) sofort an.

6.1 Interne Kontrollsysteme

Zur Ausrichtung organisatorischer Bestandteile auf Basis definierter Anforderungen dienen interne Kontrollsysteme als Hilfestellung bei der Formulierung von Zielvorgaben. Das für Unternehmen denkbar allgemeinste Rahmenwerk wurde formuliert durch das Committee of Sponsoring Organizations of the Treadway Commission (COSO). Es bildet einen Rahmen für das unternehmensweite Risikomanagement, kann jedoch vorliegend mangels IT-Konkretisierung für die Betrachtung einer IT-spezifischen Problemstellung nicht verwendet werden. Das für die IT geeignetere Rahmenwerk ist COBIT, von der ISACA entwickelt und gewachsen aus u.a. der IT Infrastructure Library (ITIL) und dem Capability Maturity Model (CMM). Es wurde zwar, insbesondere in Abgrenzung zu ISMS, in der Literatur mehrfach erschöpfend untersucht. Dennoch soll ein kurzer Einblick an dieser Stelle nicht ausbleiben, um dem Leser einen vollständigeren Überblick zu bieten.

6.1.1 COBIT 5.0, COBIT 4.1, Val IT 2.0 und Risk IT

COBIT steht für „Control Objectives in Information and Related Technology“ und hat die effektive und effiziente Ausrichtung der IT zur Unterstützung der Geschäftsziele zum Gegenstand. Die Produktfamilie umfasst:

- COBIT-5-Framework (Beschreibung der Gesamtintegration)
- COBIT-5-Enabler-Guides (Beschreibung von Voraussetzungen für Governance und Management)
- COBIT-5-Professional-Guides (Implementierungsvorgaben)

Derzeit werden im Rahmen der Professional Guides auch Rahmenwerksbausteine für Informationssicherheit, Assurance und Risikomanagement entwickelt, stehen aber derzeit noch nicht für eine Untersuchung zur Verfügung. Die vier Domänen des COBIT-Rahmenwerks [Ins12] haben eine klare Beziehung zum PDCA-Zyklus:

- Plan & Organise (PO)
- Aquire & Implement (AI)
- Deliver & Support (DS)
- Monitor & Evaluate (ME)

Diese Domänen stehen in COBIT den IT-Ressourcen Anwendung, Information, Infrastruktur und Personen gegenüber. Als dritte Dimension kommen die allgemeingültigen Anforderungen Effektivität und Effizienz sowie die sicherheitsspezifischeren Anforderungen Vertraulichkeit, Integrität, und Verfügbarkeit sowie Compliance und Verlässlichkeit hinzu, siehe Abbildung 6.1. Die fünf „COBIT-Prinzipien“ beschreiben den Umgang der Domänen mit diesen Dimensionen [Ins12]:

- Adressierung von Stakeholder-Vorgaben
- Ende-zu-Ende-Abdeckung des Unternehmens
- Anwendung eines einzigen, integrierten Rahmenwerks
- Gewährleistung eines holistischen Ansatzes

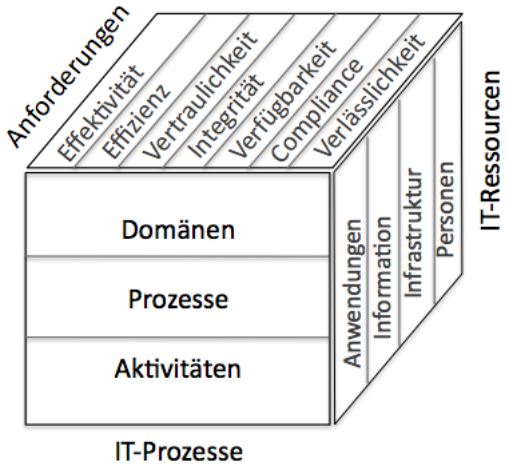

Abbildung 6.1: COBIT-Würfel

- Separierung von Governance und Management

Zunächst wurde COBIT in Version 5 jüngst dahingehend optimiert, dass es an individuelle Unternehmensvorgaben angepasst werden kann. Es kann eine Übersetzung von bestimmten Geschäftszielen in spezifische, messbare IT-Ziele stattfinden.

Mit der Ende-zu-Ende-Ausrichtung gewährleistet COBIT die Sicht auf Informationen als Wertgegenstand, welcher sich unternehmensweit erstreckt, und sich nicht auf das Abbild und die Verantwortlichkeit einer isolierten IT-Funktion beschränken lässt.

Der Anspruch eines integrierten Rahmenwerks meint eine Vereinheitlichung der Sinngebung anderer Rahmenwerke (COBIT 4.1, Val IT 2.0, Risk IT) und Best-Practice-Ansätze (wie ITIL) auf einer abstrakten Ebene in Bezug auf IT-Governance und IT-Management. Weitere Rahmenwerke, darunter auch

ISMS, können ebenso in COBIT integriert werden, um einem ganzheitlichen IT-Governance-Rahmen zu dienen.

COBIT sieht in einer effektiven und effizienten Handhabung von IT ferner verschiedene interagierende Akteure [Ins12]:

- Prinzipien, Regeln und Rahmenwerke, welche Vorgaben ausdrücken
- (IT-)Prozesse, dessen Reife mittels CMM festgehalten wird
- Organisationsstrukturen, mit RACI-Charts als Werkzeug
- Kultur, Ethik & Verhalten
- Informationen
- Services, Infrastruktur & Anwendungen
- Menschen, Fähigkeiten & Kompetenzen

Letztlich werden unter Governance und Management gänzlich verschiedene Dinge verstanden. Governance ist gemäß [Ins12] ein Mittel zur Gewährleistung, dass Stakeholder-Bedürfnisse, Konditionen und anderweitige Optionen evaluiert werden können, um Geschäftsziele abzuleiten. Hierauf folgt eine Richtungsvorgabe durch Priorisierungen und Entscheidungen, abgeschlossen mit der Überwachung von Performance und Compliance gegen die vereinbarten Zielvorgaben.

Management hingegen plant, entwickelt, betreibt und überwacht Aktivitäten im Einklang mit der Governance-Ausrichtung, um die Geschäftsziele zu erfüllen. [Ins12] Auf Basis dieser Definitionslage sieht COBIT zu einem gewissen Grad eine Einbettung des Managements in einen höheren Governance-Raum vor. Dies schlägt sich auch in der Rollenzuweisung des Managements zur Instanz eines Chief Executive Officers (CEO) in Abgrenzung zur Governance, getragen durch eine *Chairperson*, nieder.

Sind alle relevanten Normen, Standards sowie die IT-Ziele hinreichend abgestimmt, werden sie mit dem derzeitigen Stand verglichen, Maßnahmen an den IT-Prozessen durchgeführt und die Auswirkungen fortwährend über-

wacht. Hierfür werden Messgrößen (Key Performance Indicators, KPI) verwendet.

Melden diese Steuerungsinformationen eine unzulängliche Konformität der IT-Prozesse mit den gesetzten IT-Zielen, findet eine unmittelbare Rückkopplung mit vorhergehenden Teilschritten statt. Dieses Kontrollmodell ist in Abbildung 6.2 visualisiert.

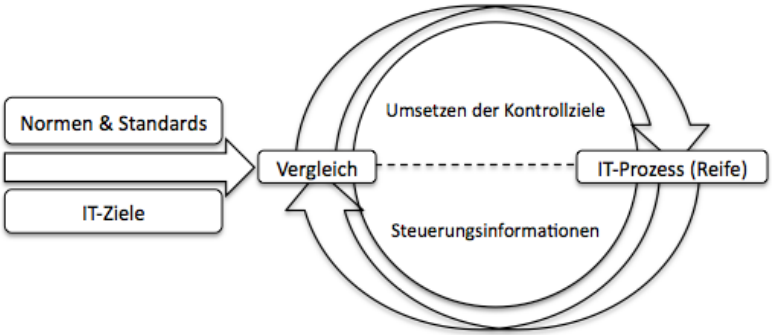

Abbildung 6.2: COBIT-Kontrollmodell

Kritisch zu betrachten sind die Ansprüche, einerseits ein einziges, übergreifendes und integriertes Rahmenwerk zu schaffen, welches andererseits aber auch operative und individuelle Vorgaben und Handlungen ermöglichen soll. Diese Ansprüche sind gegenläufig. Die Sicht auf eine notwendige Integration der Ebenen Geschäft und IT werden hingegen ebenso abgebildet wie die drei Informationssicherheitsanforderungen Vertraulichkeit, Verfügbarkeit und Integrität.

Das Abstraktionsniveau ist jedoch noch zu generisch, als dass es tatsächlich zu einer Operationalisierbarkeit für bestimmte Anforderungen wie der Gewährleistung von Informationssicherheit führen könnte. COBIT kann als Deckmantel für eine spezifischere Methodik mit Fokus auf Informationssicherheit verstanden werden. Verschiedene Gedanken sollen für die spätere

ISMS-Konstruktion aufgegriffen werden. Es können nur Personen, jedoch keine Organisationen nach COBIT zertifiziert werden.

6.1.2 IT Infrastructure Library (ITIL)

Da im vorherigen Abschnitt mehrfach Bezug zu ITIL genommen wurde, soll an dieser Stelle noch ein kurzer, tieferer Einblick gegeben werden. Die IT Infrastructure Library ist ein de-facto-Standard, gewachsen aus einer Sammlung von Best-Practice-Ansätzen zur Ausgestaltung eines integrativen IT-Managements und daher vorrangig für IT-Abteilungen interessant. ITIL besteht in Version 3 aus einer Vielzahl von IT-Prozessen, darunter folgende mit direkter Relevanz zur Informationssicherheit [Klo08]:

- Strategy Management
- Financial Management
- Service Level Management
- Information Security Management
- IT Service Continuity Management
- Availability Management
- Change Management
- Release and Deployment Management
- Incident Management
- Problem Management
- Service Reporting

Diese (IT-)Prozesse entstammen unterschiedlichen ITIL-Publikationen, welche nicht Gegenstand näherer Betrachtung sein sollen. Deutlich wird an der oben genannten Auswahl an Prozessen jedoch die Notwendigkeit der integrativen Verzahnung des allgemeinen IT-Managements mit dem Thema Informationssicherheit. Diese Verzahnung ist durch ITIL grundsätzlich adressierbar. Die Ausrichtung einer Teilorganisation nach ITIL kann ent-

sprechend in einer sehr strukturierten IT-Abteilung mit klaren Vorgaben für Zuständigkeiten und Verfahrensweisen resultieren [Klo08].

Gleichzeitig ist jedoch eben dieses Konstrukt, in Bezug zur Thematik GRC-Management, nur eine stark optimierte Möglichkeit zur Behandlung von Problem-Symptomen der IT, kein Mittel zur Behandlung von dessen Ursprung. Dies meint nicht die Unterscheidung von Incident- und Problemmanagement. Hier wird in ITIL eine Möglichkeit geboten, die Serviceerbringung wieder herzustellen (Incident-Management), und später, idealerweise durch isoliertes Personal, nach Ursachen für wiederkehrende Störfälle zu suchen (Problemmanagement). Gemeint ist vielmehr, dass die IT selbst gar nicht die Möglichkeit hat, Ursachen von GRC-Problemen beseitigen zu können, da GRC-relevante Informationen an den Arbeitspaketen von Geschäftsprozessen hängen, und somit außerhalb der Zuständigkeit der IT (und jeder anderen Ressourcen verwaltenden Einheit, wie etwa dem Personalmanagement) liegen.

6.2 Informationssicherheitsmanagementsysteme

Dieses Kapitel dient Beschreibung und Diskussion von Rahmenwerken für Erschaffung und Unterhaltung eines ISMS.

6.2.1 ISO/IEC 27001

Die ISO/IEC 27001 ging aus dem Britischen Standard 7799-2 hervor und ist entstanden unter Abstimmung mit den Standards ISO 9001 (Qualitätsmanagement-Anforderungen) sowie ISO 14001 (Umweltmanagement-Anforderungen). Sie beschreibt Anforderungen an ein ISMS. Die ISO 27002 definiert als Implementierungshilfe Best Practices für die Definition von Zielen und Kontrollen der Risikobehandlung [ISO13]. Weitere Ergänzungen von ISO 27001 und ISO 27002 finden sich in:

- ISO 27000 (Überblick und Vokabular)
- ISO 27003 (Implementierungsführer)
- ISO 27004 (Messbarkeit von Sicherheit)
- ISO 27005 (IS-Risikomanagement)
- ISO 27006 (Voraussetzungen für Auditing und Zertifizierung von ISMS)

Die Methodik der ISO/IEC 27001 lässt eine direkte Korrelation mit dem PDCA-Zyklus erkennen, und ist so strukturiert in die folgenden Phasen:

1. Planung (Festlegung von Zielen und Strategien)
2. Umsetzung und Durchführung (Bereitstellung von Ressourcen für und Realisierung von Maßnahmen an IT-Objekten)
3. Überwachung und Prüfung (Messung des Erreichten gegen die Ziele)
4. Wartung und Verbesserung (korrektive und vorbeugende Maßnahmen, die Operationalisierung betreffend)

Unternehmen können sich nach ISO/IEC 27001 zertifizieren lassen.

Die Norm behandelt Informationssicherheit jedoch primär ausgehend von der Sicht auf die in einer Organisation verwendeten Ressourcen. Durch strategische Überlegungen resultieren Maßnahmen, die an diesen IT-Objekten realisiert werden. Charakterisiert wird die operative Umsetzung der genannten Phasen durch die Anforderungen, Ziele, die internen Prozesse, Größe und Struktur der jeweiligen Organisation.

Grundsätzlich gewährt die ISO 27001 einen gewissen Freiheitsgrad bei der Wahl und konkreter Ausgestaltung der Kontrollen. Es ist jedoch stets eine spezifische Risikoanalyse für jede abzusichernde Ressource notwendig.

6.2.2 BSI IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte einen internationalen Informationssicherheitsstandard, genannt „IT-Grundschutz“. Er sieht zunächst vor, einen Teilbereich der Informationslandschaft, genannt

Informationsverbund, aus der Gesamtheit der Organisation abzugrenzen. Dieser Teilbereich wird dann unterteilt in (Ziel-)Objekte aus den Kategorien Organisation, Personal, Technik und Infrastruktur. Zu erkennen ist hier, analog zur ISO 27001, die Sicherheits-Perspektive ausgehend von den IT-Ressourcen.

Der BSI IT-Grundschutz umfasst die BSI-Standards und die sogenannten BSI IT-Grundschutz-Kataloge [BfSidI09]. Die BSI-Standards geben Empfehlungen für Methoden und Maßnahmen und gliedern sich wie folgt [fSidI08]:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (Anforderungen an ein ISMS, kompatibel zur ISO/IEC 27001)
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise (detaillierte operative Vorgaben zur Realisierung des ISMS)
- BSI-Standard 100-3: Risikoanalyse auf Basis des IT-Grundschutz (Vorgaben zur Durchführung einer Risikoanalyse)
- BSI-Standard 100-4: Notfall-Management (in Ergänzung zur 100-2)

Die IT-Grundschutz-Kataloge beinhalten Bausteine, Gefährdungen und Maßnahmen. Sie basieren auf generischen Risikoanalysen für normalen Schutzbedarf und schlagen standardisierte Maßnahmenpakete vor. Hierdurch entfällt die Notwendigkeit von Risikoanalysen für jedes IT-Objekt, der Dokumentationsaufwand steigt jedoch an. IT-Objekte mit hohem oder sehr hohem Schutzbedarf werden einer Risikoanalyse gemäß BSI-Standard 100-3 unterzogen.

Die Bausteine der IT-Grundschutz-Kataloge sind in übergreifende Aspekte, Infrastruktur, IT-Systeme, Netze und Anwendungen unterteilt. Die Gefährdungskataloge unterscheiden in die Bereiche höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen. [fSidI08]

Die Maßnahmenkataloge sind strukturiert nach Infrastruktur, Organisation, Personal, Hardware & Software, Kommunikation und Notfallvorsor-

ge. Sie sehen ferner einen Lebenszyklus vor, welcher aus den Phasen der Planung & Konzeption, der Beschaffung, der Umsetzung, dem Betrieb, der Aussonderung und der Notfallvorsorge besteht – eine Maßnahme ist genau einer der jeweiligen Phase zugeordnet.

Der BSI IT-Grundschutz hat eine zum PDCA-Zyklus und der ISO/IEC 27001 kompatible Vorgehensweise:

1. Initiierung des Sicherheitsprozesses (Schaffung von Voraussetzungen auf organisatorischer Ebene)
2. Erstellung des Sicherheitskonzeptes (gemäß BSI-Standard 100-2: Strukturanalyse, Schutzbedarfsfeststellung, Maßnahmenauswahl, Basis-Sicherheitscheck, ergänzende Sicherheitsanalyse)
3. Umsetzung des Konzeptes (Sichtung der Ergebnisse, Maßahmenkonsolidierung, Aufwandsschätzung, Festlegung der Reihenfolge der Umsetzung, Ableitung der Aufgaben sowie Realisierung begleitender Maßnahmen)
4. Aufrechterhaltung & Verbesserung (Retrospektive und gegebenenfalls Anpassung des Vorgehens)

Organisationen können ihren Informationsverbund nach ISO/IEC 27001 auf Basis des IT-Grundschutz zertifizieren lassen. Hierfür sind ferner Siegelstufen der Maßnahmen vorgesehen: A (Einstieg), B (Aufbau), C (Zertifikat), Z (zusätzlich) sowie W (Wissenstransfer). Je nach Siegelstufe können verschiedene Testate erworben werden.

Der BSI IT-Grundschutz erlaubt zwar weniger Kreativität bei der Maßnahmenauswahl und -umsetzung, spart jedoch den Aufwand der Erstellung spezifischer Risikoanalysen für jedes relevante IT-Objekt. Dennoch ist der Blickwinkel, analog zur ISO/IEC 27001, von einer IT-Objekt-Sicht geprägt.

6.2.3 ISO 20000

Als internationaler Standard für das IT-Service-Management wurde die ISO 20000 entwickelt, welcher sich gliedert in einen Teil der Spezifikation, in welchem die Zertifizierungsanforderungen und damit Vorgaben zur Errichtung und Wartung des IT-Service-Managements beschrieben werden, und einen Teil zur Festlegung von Revisionsrichtlinien.

ISO 20000 verbindet Inhalte der ISO 9000 (Aufbau eines Qualitätsmanagementsystems) mit den Best Practices zur Umsetzung des IT-Service-Managements nach ITIL (IT Infrastructure Library). [BSI09b]

Die ISO 20000 liefert zwar einen Mehrwert bezüglich der Abgrenzung zwischen internem Kontrollsystem und IT-Service-Management. Die Anforderungen an das Informationssicherheitsmanagement reduzieren sich jedoch auf einen Verweis zur ISO 2700x, welche in Abschnitt 6.2.1 bereits diskutiert wurde. Die vorliegende Norm wird daher nicht näher untersucht.

6.3 Vorgaben und Prüfverfahren

Dieses Kapitel stellt die zuvor diskutierten Rahmenwerke einigen vorgabe- und/oder prüfungsorientierten Normen gegenüber.

6.3.1 PCI DSS Version 1.2

Die vorbezeichneten Rahmenwerke haben primär oder sekundär die Sicherheit aller in einer Organisation verarbeiteten Informationen zum Gegenstand. Auch im Fall eines abgegrenzten Informationsverbunds im BSI IT-Grundschutz wird ein Teilbereich verschiedenartiger Informationen zusammengefasst. Das Rahmenwerk Payment Card Industry Data Security Standard (PCI DSS) betrifft hingegen speziell Informationen, welche im Rahmen der Verarbeitung von Kreditkartentransaktionen notwendig werden.

Es wurde entwickelt vom PCI Security Standards Council, einem Konsortium bestehend aus führenden Kreditkarten-Organisationen.

PCI DSS muss von allen Organisationen umgesetzt werden, welche Karteninhaberdaten, darunter die Primary Account Number (PAN), speichern, verarbeiten oder übertragen. Die betreffenden Daten sind der Inhaber-Name, der Servicecode sowie das Ablaufdatum der Kreditkarte. Die Authentisierungsdaten hingegen sind streng vertraulich und dürfen nicht gespeichert werden. Sämtliche genannten Daten unterliegen jedoch Sicherheitsanforderungen, welche weitreichende Konsequenzen für die IT der betreffenden Organisation haben. [BSI09b]

So sind im Standard 12 Anforderungen aufgeführt [Cou08]:

- Etablierung & Wartung eines sicheren Netzwerks
- Schutz von Daten des Karteninhabers
- Wartung eines Anfälligkeits-Managementsystems (Virenschutz, etc.)
- Implementierung von starken Zugriffskontrollmaßnahmen
- Regelmäßiges Überwachen und Überprüfen von Netzwerken
- Realisierung einer Informationssicherheitsrichtlinie

Insbesondere aus der Realisierung von Anfälligkeits-Managementsystem und Informationssicherheitsrichtlinie folgt unmittelbar die Notwendigkeit für ein Informationssicherheitsmanagementsystem. PCI DSS vermittelt hier jedoch nur Anforderungen für die genannten Informationen und gibt keine Vorgaben für die Prozesse des ISMS. Dennoch kann und muss die Konformität von Organisationen, welche Kreditkartendaten verarbeiten, speichern oder übermitteln über Zertifizierungen bestätigt werden. Für die vorliegende Untersuchung ist PCI DSS nicht geeignet, da eine definierte Methodik zur Realisierung von Informationssicherheit fehlt.

6.3.2 IDW-Standards

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) stellt einen Zusammenschluss von Wirtschaftsprüfungsgesellschaften dar. Das Ziel liegt in der fachlichen Unterstützung von Wirtschaftsprüfern [dWiDeH13].

Das IDW veröffentlicht verschiedene Arten von Werkzeugen [BSI09b] [IDW11]:

- Prüfungsstandards (IDW PS)
- Stellungnahmen zur Rechnungslegung (IDW RS)
- IDW-Standards (IDW S)
- Prüfungs- & Rechnungslegungshinweise (IDW PH und IDW RH)

In den IDW PS sind Anforderungen zur Rechnungslegung und Fragen zur Prüfung festgelegt. Ein Teil dieser Veröffentlichungsreihe beschäftigt sich direkt oder indirekt mit Informationssicherheit, darunter [BSI09b]:

- Abschlussprüfung bei Einsatz von IT (IDW PS 330)
- Checkliste zur Abschlussprüfung bei Einsatz von IT (IDW PH 9.330.1)
- Grundsätze ordnungsgemäßer Buchführung bei Einsatz von IT (IDW RS FAIT 1)
- Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Electronic Commerce (IDW RS FAIT 2)
- Grundsätze ordnungsgemäßer Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)
- Erteilung, Verwendung von Softwarebescheinigungen (IDW PS 880)
- Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen (IDW PS 951)

Festzustellen ist zunächst eine inhaltliche Parallele zum Gebiet der Föderationen im zuletzt aufgeführten Punkt. Auch die IDW-Veröffentlichungen sind jedoch für die vorliegende Untersuchung ungeeignet, da keine Methodik zur Realisierung von Informationssicherheit definiert, sondern lediglich

Voraussetzungen in Hinblick auf die Buchführung oder Prüfungskriterien ausgesprochen werden.

6.3.3 SAS 70

Das American Institute of Certified Public Accountants (AICPA) hat ebenfalls einen Prüfstandard, den Statement on Auditing Standard No. 70 (SAS 70), entwickelt, welcher insbesondere im Rahmen des U.S.-amerikanischen Sarbanes-Oxley-Act (SOX) angewandt wird. Inhaltlich entsteht ein Mehrwert durch die Vereinheitlichung des Vorgehens bei der externen Prüfung von Dienstleistungsorganisationen. [BSI09b]

Der Standard beschreibt zwar das Vorgehen bei der Auditierung, jedoch weder die Inhalte der Prüfung noch eine Methodik zur Errichtung des internen Kontrollsystems, welches der Prüfung unterzogen wird. Entsprechend ist es analog zum PCI DSS und den IDW-Standards für die vorliegende Untersuchung nicht relevant.

6.4 Zusammenfassung

Nicht alle Rahmenwerke sind für das vorliegende Problem gleichermaßen relevant. Vorliegend sollen besonders die Rahmenwerke betrachtet werden, welche bei der Konstruktion eines ISMS für föderierte Umgebungen dienlich sein können. Diese Anforderung ist dann erfüllt, wenn ein starker Bezug zu den Themen IT-Ausrichtung und -Kontrolle sowie Informationssicherheit erkennbar ist. Die relevanten Rahmenwerke lauten:

1. COBIT (Version 5)
2. ITIL (Version 3)
3. ISO 2700x
4. BSI IT-Grundschutz

COBIT und die ISO 27001 bieten eine weiträumige Gestaltungsfreiheit, der BSI IT-Grundschutz bietet eine Konkretisierung im Bereich der Maßnahmen für relevante IT-Objekte, ITIL bietet Schablonen für die Ausgestaltung des IT-Managements.Es stellt sich nun die Frage, wie sich diese Rahmenwerke zueinander abgrenzen lassen.

7 Klassifizierung der traditionellen Rahmenwerke

Die zuvor identifizierten relevanten Rahmenwerke sind zunächst heterogener Natur. COBIT kann zwar als ein übergreifendes Kontrollsystem angesehen werden, ist aber in seiner Natur kein primär auf Informationssicherheit ausgerichtetes Rahmenwerk. ITIL ist eine Konkretisierung von COBIT hinsichtlich des IT-Managements. Die ISO 27001 und der BSI IT-Grundschutz sind zueinander zwar kompatibel, unterscheiden sich jedoch maßgeblich in ihrer Konkretisierung. Nachfolgend soll eine übergreifende Klassifizierung vorgenommen werden.

7.1 Kriterienerhebung

Dieser Abschnitt dient der Erfassung von Kriterien, welche sowohl der Einordnung der Rahmenwerke, als auch der späteren Evaluation des zu entwickelnden ISMS dienen sollen. Entsprechend wurden Vergleichskriterien aus Anforderungen für ein künftiges ISMS abgeleitet. Aufgrund der Ausrichtung des Problemfeldes sind sowohl Kriterien aus dem Bereich der Informationssicherheit, als auch des Prozessmanagements anzulegen. Diese sollen wie folgt benannt sein:

- Unterstützung von föderativen Prozessstrukturen (Gering, Mittel, Hoch)
- Unterstützung von GRC-Prozessen (Vollständig, Teilweise, Nein)
- Konformität mit PDCA-Zyklus (Ja, Nein)

- Operationalisierbarkeit (Gering, Mittel, Hoch)
- Dokumentationsnotwendigkeit (Gering, Mittel, Hoch)
- Konkretisierung hinsichtlich der Maßnahmen (Gering, Mittel, Hoch)
- Kosten der Realisierung (Gering, Mittel, Hoch)
- Zertifizierbarkeit der Organisation (Ja, Nein)

7.2 Einordnung der Rahmenwerke

Die in Abschnitt 7.1 gesammelten Kriterien sollen nun an die in Kapitel 6 identifizierten Rahmenwerke angelegt werden. In Tabelle 7.1 ist diese Klassifizierung ersichtlich.

Kriterium	**COBIT**	**ITIL**	**ISO 27001**	**BSI**
Föderierbarkeit	Mittel	Mittel	Mittel	Gering
GRC-Prozesse	Teilweise	Hoch	Vollst.	Vollst.
PDCA-Konformität	Ja	Nein	Ja	Ja
Operationalisierbarkeit	Gering	Hoch	Mittel	Hoch
Dokumentationsaufwand	Gering	Gering	Gering	Hoch
Konkretisierung	Gering	Mittel	Mittel	Hoch
Implementierungskosten	Gering	Mittel	Mittel	Hoch
Zertifizierbarkeit (Org.)	Nein	Ja	Ja	Ja

Tabelle 7.1: Klassifizierung relevanter IS-Rahmenwerke

Abbildung 7.1 zeigt die Abgrenzung der einzelnen Rahmenwerke zueinander schematisch.

7.3 Zusammenfassung

Die für die vorliegende Untersuchung relevanten Rahmenwerke sind die COBIT 5.0, ITIL Version 3, die ISO 2700x sowie der BSI IT-Grundschutz. Die Betrachtung dieser Rahmenwerke zeigt in einer qualitativen Bewertung

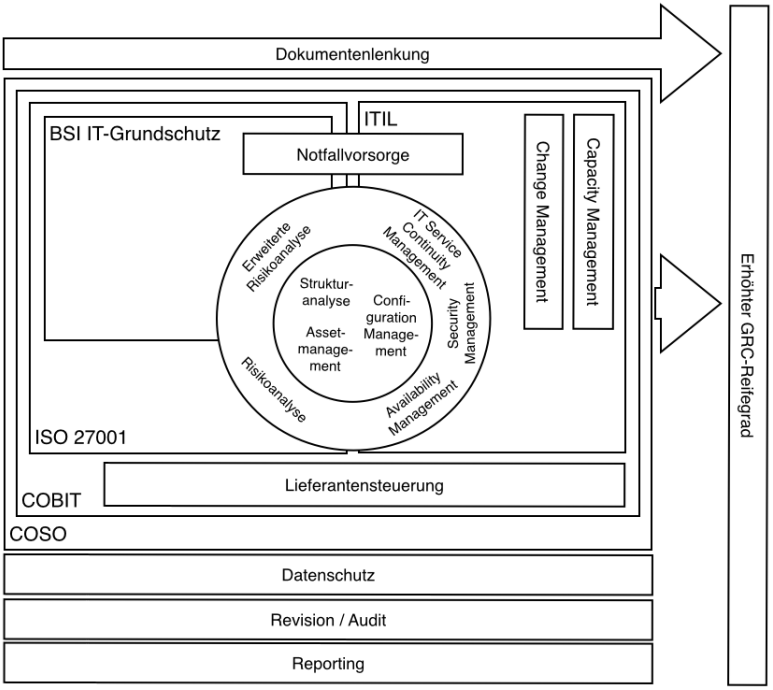

Abbildung 7.1: Gegenüberstellung traditioneller Rahmenwerke [HF10]

zueinander unterschiedliche Ausprägungen. COBIT ist generisch gehalten und dient als Governance-Instrument vornehmlich als Integrationsrahmen für verschiedene Rahmenwerke, unter anderem für IT-Management (ITIL) sowie Informationssicherheit. Für letzteres lassen sich sowohl die ISO 2700x als auch der BSI IT-Grundschutz problemlos integrieren. Der IT-Grundschutz kann als Instanziierung der ISO 2700x verstanden werden.

Abzüglich ITIL sind alle Rahmenwerke PDCA-konform. Die Operationalisierbarkeit nimmt mit dem Dokumentationsaufwand zu, wobei das beste Verhältnis beider Kriterien bei der ISO 2700x liegt, welche Freiräume bei der

Realisierung lässt und dennoch informationssicherheitsrelevante Prozesse etabliert. Die Agilität liegt erwartungsgemäß bei den generischen Rahmenwerken höher und nimmt in Richtung der spezifischeren Rahmenwerken ab. Entgegengesetzt proportional steigen die Kosten bei spezifischeren Rahmenwerken. Keine der genannten Rahmenwerke kann eine Föderierbarkeit vollständig unterstützen, da eine Beschränkung auf Organisations- und Sys-temgrenzen vorliegt.

Eine Zertifizierbarkeit für Organisationen ist für ITIL v3 (über die ISO/IEC 20000-1:2011), die ISO 2700x und BSI IT-Grundschutz gegeben, nach COBIT 4.1 und 5.0 lassen sich hingegen nur Personen zertifizieren. Dies schließt Betrachtung und Klassifizierung relevanter Rahmenwerke ab.

Teil III

Betrachtungsgegenstand und Problemstellung

Überblick Teil III

Nachdem in Teil II relevante ISMS-Rahmenwerke identifiziert, erläutert und klassifiziert wurden, soll in diesem Teil die sich daraus ergebende Lücke benannt und der für die Realisierung anvisierte Betrachtungsgegenstand beschrieben, d.h. Anforderungen für das zu entwickelnde Rahmenwerk für Föderationen erhoben werden. In Kapitel 8 wird ein typisches Föderierungsszenario benannt. Kapitel 9 beschäftigt sich mit der Isolierung des Problemfeldes.

8 Ende-zu-Ende-Föderierungsszenarien

Es wird nun der Problemraum definiert, d.h. die Szenarien für Föderationen benannt, welche als Grundlage für die weiteren Untersuchungen dienen. Hierzu wurde untersucht, welche Anwendungsfälle im Rahmen von Föderierungen die größte Verbreitung haben. Es konnte herausgearbeitet werden, dass Ende-zu-Ende-Prozesse (*End-to-End* oder *E2E Business Processes*) insofern von größter Relevanz sind, als dass sie einen Rahmen für viele konkrete Prozessimplementierungen bilden können. Dies ist dem Vorteil der Zerlegung von Prozessen in Module zu schulden. Aus diesen Modulen können beliebig viele Ende-zu-Ende-Prozesse generiert werden.

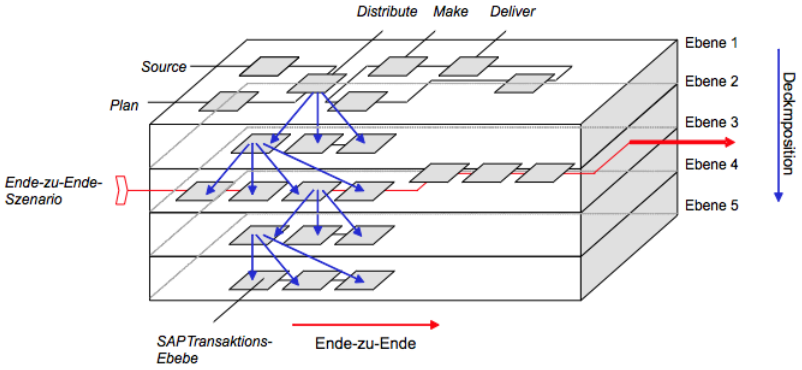

Abbildung 8.1: Ende-zu-Ende-Geschäftsprozesse

Abbildung 8.1 visualisiert diese Ende-zu-Ende-Beziehung. Ferner wurde untersucht, welche Ende-zu-Ende-Prozesstypen die größte Komplexität aufweisen. Hier wurde der E2E-Prozess *Order-to-Cash (OTC)* als der Prozess identifiziert, welcher die meisten Schnittstellen zu anderen Modulen, und dadurch innerhalb einer Föderation potenziell anderen Organisationen, besitzt. Tabelle 8.1 zeigt Schnittstellen des OTC zu anderen Subsystemen (eingangs und ausgangs) am Beispiel SAP ERP.

OTC-relevantes Subsystem	**Input/Output Prozessschnittstelle**
Multi Level Campaign	Out: SP, Procurement
Sales Project (SP)	In: Multi Level Campaign Out: QP, PM
Quote Process (QP)	In: SP, AppEng Out: COE
Application Engineering (AppEng)	In: Tooling Mngmt Out: QP, DM, PM
Project Mngmt (PM)	In: AppEng, SP, Tooling Mngmt, Product & Process Design, Development and Quotation Out: COE, Capital Expenditure, Tooling Mngmt, Production Forecasting, DM, Procurement
Drawing Mngmt (DM)	In: AppEng, PM, Production Execution, WMO, Production Planning Out: Production Execution, Warehouse Management, Production Planning
Customer Order Entry (COE)	In: SP, COM, QP, PM Out: Procurement, WMO, Production Forecasting, Production Planning
Customer Claim Mngmt (CCM)	Out: WMO, CC, Customer Order Management
Cash Collection (CC)	In: SCM Intercompany Recharges, WMO, Receive Payment, Fixed Assets Out: Intercompany Invoices, Receive Payment
Customer Order Mngmt (COM)	In: COE, Production Execution, Production Planning, Procurement, WMO, Customer Claim, Out: Production Planning, COE, WMO, Procurement
Warehouse Mngmt Outbound (WMO)	In: COE, CCM, COM, Procurement, WM (Inbound), Production Execution, Compound planning and production processes Out: CC, SCM Intercompany Recharges, Procurement, WM (Inbound), Production Execution, Compound planning and production processes
Production Forecasting	In: PM Out: Medium Term Planning, Procurement

Tabelle 8.1: Technische OTC-Schnittstellen am Beispiel SAP ERP

8.1 Der Order-to-Cash-Geschäftsprozess

Der OTC besitzt somit die für die vorliegende Untersuchung größte Relevanz und soll daher als Grundlage für die weitere Untersuchung dienen. Abbildung 8.2 zeigt die Prozessschritte des OTC, wie sie im gängigen Literaturverständnis auftreten [oD14].

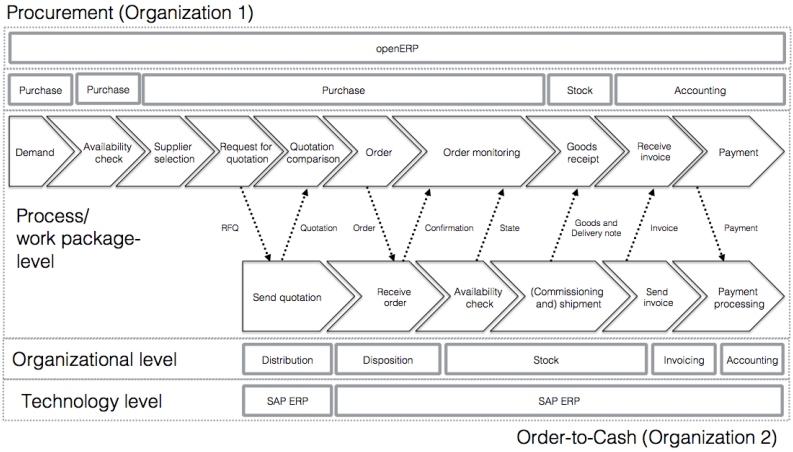

Abbildung 8.2: Order-to-Cash E2E-Geschäftsprozess

Für das vorliegende Modell sind die Inhalte der Prozessschritte von größter Relevanz. Einerseits sind sie bereits jetzt wichtig, um die Eignung einer Gruppe von Geschäftsprozessen als Bezugsobjekt für das zu entwickelnde Rahmenwerk einzuschätzen. Später sind die jeweiligen Prozessschritte mit ihren Aufgaben Träger genau der Informationen, welche durch ein Rahmenwerk, welches „top down“ arbeitet, abzusichern sind, und sich der Schutzbedarf dieser Informationen genau daran ausrichtet, welcher inhaltlichen Art die jeweilige Information ist. Schließlich sind sie wichtig, um die

Attribute zu ermitteln, welche im Rahmen des Monitorings von Informationen, die in einem komplexen Ende-zu-Ende-Prozess verarbeitet werden, als wichtig anzusehen sind.

8.2 Traditionelle Absicherung mittels ISO 27001

In der Praxis wird bislang versucht, einen übergreifenden Ende-zu-Ende-Prozess mit den zuvor erläuterten Rahmenwerken (meist mittels ISO 27001) abzusichern, in welchen jeder Geschäftsprozessbestandteil nicht als Modul eines übergeordneten, die Föderation verbindenden Geschäftsprozesses, sondern als eigenständiger Geschäftsprozess für die jeweilige Organisation verstanden wird, welche das Rahmenwerk nutzt.

Eine Absicherung des Geschäftsprozesses findet über eine Schutzbedarfsfeststellung der verarbeiteten Informationen beziehungsweise konkreter relevanter Objekte statt. Dies kann top-down (ausgehend vom Prozess) oder Bottom-Up (ausgehend von der letzten Instanz beteiligter Komponenten, die miteinander in gerichteter Verbindung stehen, d.h. vorliegend die Infrastruktur) stattfinden. Ein effizienter und in der Informationssicherheitsberatung verbreiteter Best-Practice-Ansatz besteht in einer Kombination beider Methoden, welche Effektivität und Effizienz in einem gesunden Verhältnis mischt. Das Resultat besteht stets aus identifizierten Maßnahmen, welche an den beteiligten Ressourcen (Personen, Anwendungen, IT-Systeme, IT-Infrastruktur und Infrastruktur) zu realisieren sind. Der Umsetzungsgrad jeder Maßnahme wird dokumentiert. Ein Teil dieses Vorgehens soll nachfolgend am Beispiel der ISO 27001 detaillierter beschrieben werden.

Innerhalb des Vorgehens der Plan-Phase der ISO 27001 würden zunächst eine Scope-Definition, die Definition einer ISMS-Policy, die Festlegung eines Risiko-Aufnahme-Ansatzes, die Identifizierung von Risiken sowie die Analyse und Bewertung von Risiken durchgeführt werden. Es ist dieser Teil des Vorgehens der ISO 27001, der für ein föderiertes Szenario näher untersucht

werden sollte. Betrachtet man die Schritte der Identifizierung und der Analyse von Risiken genauer, wird deutlich, dass die ISO 27001, stets nur von der Perspektive der ausführenden Organisation ausgeht. Hier lässt sich einerseits in den Betreiber des OTC (die verkaufende Organisation), und den Nutzer des OTC (die einkaufende Organisation), unterscheiden, siehe auch Abbildung 8.2 weiter vorn. Das Ergebnis der Risiko-Erfassung eines OTC-Betreibers (verkaufende Organisation) könnte aussehen wie ersichtlich in Tabelle 8.2.

#	Prozessschritt	Information	Schutzbedarf	Gefährdung
1	RFQ erhalten	RFQ	**Normal**	**keine wahrgenommen**
2	Angebot senden	Angebot	**Hoch**	**Kompromittierte Vertraulichkeit gegenüber Wettbewerbern**
3	Auftrag erhalten	Auftrag	**Normal**	**keine wahrgenommen**
4	Bestätigung senden	Auftragsbestätigung	Normal	rechtliche Belange
5	Verfügbarkeit senden	Verfügbarkeitsnachricht	Normal	keine wahrgenommen
6	Lieferschein senden	Lieferschein	**Normal**	**keine wahrgenommen**
7	Rechnung senden	Rechnung	Hoch	Datenintegrität
8	Zahlung erhalten	Zahlungsinformationen	Sehr hoch	Datenintegrität

Tabelle 8.2: Risiko-Erhebung eines OTC-Betreibers

Das Ergebnis der Risiko-Erfassung eines OTC-Nutzers (einkaufende Organisation) könnte hingegen aussehen wie ersichtlich in Tabelle 8.3.

Im Anschluss schreibt das Vorgehen der ISO 27001 die Identifizierung von

Risikobehandlungsplänen, die Auswahl von Maßnahmen, eine Kostenanalyse, die Bewertung der Anwendbarkeit und die Zusicherung der Geschäftsführung vor.

#	Prozessschritt	Information	Schutzbedarf	Gefährdung
1	RFQ senden	RFQ	**Hoch**	**Kompromittierte Vertraulichkeit hinsichtlich Produktzusammensetzung (Betriebsgeheimnis)**
2	Angebot erhalten	Angebot	**Normal**	**keine wahrgenommen**
3	Auftrag senden	Auftrag	**Sehr hoch**	**Kompromittierte Vertraulichkeit hinsichtlich Produktzusammensetzung (Betriebsgeheimnis)**
4	Bestätigung erhalten	Auftragsbestätigung	Normal	keine wahrgenommen
5	Verfügbarkeit erhalten	Verfügbarkeitsnachricht	Normal	keine wahrgenommen
6	Lieferschein erhalten	Lieferschein	**Hoch**	**Notwendig für das Anstoßen interner Prozesse**
7	Rechnung erhalten	Rechnung	Hoch	rechtliches Problem, Datenintegrität
8	Zahlung senden	Zahlungsinformationen	Sehr hoch	rechtliches Problem, Datenintegrität

Tabelle 8.3: Risiko-Erhebung eines OTC-Nutzers

Das gesamte Vorgehen wird einerseits mangels effektiverer Alternativen genutzt, welche explizit für föderierte Einsatzszenarien spezifiziert wären. Andererseits wird jedoch auch ein nachvollziehbarer Blick auf die Notwendigkeit der Durchführung und Aufrechterhaltung von Zertifizierungen für Informationssicherheit gelegt. Diese ist in vielen Branchen sogar vorgeschrieben, in jedem Fall bietet sie einen Vorteil in der Vermarktung eigener Produkte und Services.

8.2.1 Kritik

Von zentraler Bedeutung ist, dass sich die vorbezeichneten Überlegungen stets innerhalb einer geschlossenen Organisation zutragen. Im Falle eines föderierten OTC würde demnach nur das Ausgangsunternehmen die für sich als hoch schutzbedürftig identifizierten Objekte mit entsprechenden Maßnahmen absichern. Den übrigen Unternehmen bleibt es frei, beispielsweise ein Rahmenwerk wie den BSI IT-Grundschutz anzunehmen. Selbst wenn es realisiert wird, ist die Frage nach den Schutzbedarfen jedoch aus Sicht des übergeordneten Geschäftsprozesses nicht objektiv.

Die ISO optimiert derzeit einen Standard zur Erweiterung der ISO 27000er Reihe zur Implementierung eines ISMS in Communities, welche Informationen miteinander teilen [fS14]. Hier wird vorgeschlagen, dass sämtliche beteiligten Organisationen in Bezug auf die sensitiven Informationen ein einheitliches, gemeinsames ISMS realisieren. Einerseits scheint dieser Ansatz in einer mehrschichtigen Lieferantenkette wenig praktikabel, andererseits würden hierdurch lediglich Vertraulickheitsaspekte adressiert werden. Die Auswahl gemeinsamer IT-Ressourcen und der Umgang mit Informationen ausgehend von einem untereinander abgeglichenen Schutzbedarf für nicht nur Vertraulichkeit, sondern auch Integrität und Verfügbarkeit, werden auch durch die ISO/IEC 27010 nicht unterstützt. Sie dient abermals als Mittel zur Behandlung von Symptomen, nicht als Werkzeug zur Weichenstellung, um Probleme zu verhindern.

Es zeigt sich, dass traditionelle Rahmenwerke für den Föderierungsfall nicht geeignet sind. Es sollen nun jedoch auch aktuellere Ansätze als nur die rein klassischen Rahmenwerke diskutiert werden.

8.3 State of the Art föderativer Ansätze

Naturgemäß bildet sich der State of the Art nicht nur über die ISO 27001 und die erläuterten Rahmenwerke heraus. Einige aktuelle, relevante Ansätze sollen nachfolgend beschrieben werden.

Das Shibboleth Project [Mor04] bietet mit dem Shibboleth System beispielsweise einen Ansatz zur Adressierung von Authentisierung, Autorisierung und Verzeichnisdiensten über mehrere Organisationen hinweg. Dies ermöglicht einen sicherheitsgestützten Zugang zu Ressourcen. Von Fraser wird in [Hat05] ein ähnlicher Gedanke basierend auf Webservices vorgestellt. Von Gaedke et. al. wird in [GMN05] ein Ansatz für Authentisierung, Autorisierung und Identitätsmanagement in heterogenen Systemen beschrieben. Ähnliche Gedanken werden von Brown et. al. in [WS13] vorgestellt.

Douglas S. Ransom beschreibt in [Ran06] einen Ansatz, welcher sich mit dem sicheren Austausch von Daten zwischen mehreren Organisationen beschäftigt, die nicht eng verbunden, d.h. auch unter der vorliegenden Betrachtungsweise als föderiert zu bezeichnen sind. Auch hier werden Authentisierung und Zugriffskontrolllisten (Access Control Lists, ACL) zentralisiert. Das Smart Firewall Project innerhalb des DARPA-Programms Dynamic Coalitions hat in [Bha03] Technologien vorgestellt, welche die Definition, das Monitoring und die Neugenerierung von high-level Netzwerk-Policies ausgehend von low-level Konfigurationseinstellungen von Netzwerkgeräten ermöglicht.

Während der Ansatz von Ransom zwar sogar Verarbeitungsprotokolle vorsieht, und damit maßgeblich die Verarbeitung von (automatisierten) Prozessschritten ermöglicht, adressiert jeder der Ansätze ausschließlich techni-

sche Detailprobleme, welche im Rahmen der föderierten Verarbeitung von Daten relevant werden, wenngleich das Identitäts- und Zugriffsmanagement hierbei zentral ist.

Paul Stephenson stellt in [Ste06] hingegen Richtlinien vor, die Unternehmen gegenseitig anlegen sollten, um zu gemeinschaftlichen Vorgaben für Datenhandhabung, Softwarehärtung, Virenschutz, Nutzungsverhalten und weiteren Themen zu gelangen. Dieser Ansatz zeigt in eine Richtung, die nicht ausschließlich technische Aspekte berücksichtigt. Er bildet jedoch keine Grundlage zur Entwicklung von Geschäftsprozessen. Auch wird kein Augenmerk auf Risikomanagement in einer Wertschöpfungskette gelegt.

Autry et. al. beschreiben in [CWA08], dass Sicherheit in Wertschöpfungsketten verschiedenen finanziellen und kundenspezifischen treibenden Kräften unterliegt, die noch dazu von Unternehmen zu Unternehmen stark variieren. Jharkharia und Shankar zeigen in [SJ05] auf, dass die IT hierbei eine besondere Rolle spielt, und sowohl Enabler als auch Hindernis beim Aufbau von Wertschöpfungsketten sein können. Zhang und Li liefern in [LL08] ein praktisches Beispiel für moderne Sicherheitsbedarfe im Rahmen der Geheimhaltung von Preisen bei einem Bieterwettbewerb. Der Bayerische IT-Sicherheitscluster e.V. hat darüber hinaus erkannt, dass die klassischen Lösungen und Konzepte keinen Rückhalt für aktuelle Bedrohungen liefern [Wie14]. Die vier genannten Untersuchungen unterstreichen die Notwendigkeit der Schaffung eines neuen Rahmenwerks.

In [DJC04] wird von IBM zunächst ein Werkzeug zur Erfassung und Begegnung von Sicherheit bzw. Sicherheitsmängeln in einer Wertschöpfungskette beschrieben. Faisal et. al. stellen in [MNF06] darüber hinaus einen Ansatz zur Risikohandhabung in Lieferketten vor. Das Ergebnis ist ein nützliches Werkzeug welches Lieferantenmanager nutzen können, um abhängige und unabhängige Faktoren für ein gesamtbildliches Risikomanagement zu erkennen. Manuj und Mentzer beschreiben in [MM08] zudem einen ersten Versuch, bestehende SCM- und Risikomanagementansätze zu harmonisieren. Beide Ansätze dienen jedoch der Behandlung bereits bestehender Ge-

schäftsprozesse, nicht der Entwicklung neuer Geschäftsprozesse samt eingesetzter IT-Ressourcen.

Stärkeres Augenmerk auf den Prozessgedanken legt hier TAS3, Trusted Architecture for Securely Shared Services [Pro14], ein Projekt zur Schaffung einer vertrauenswürdigen Architektur mit adaptiven Sicherheitsdiensten zur Wahrung von Datenschutz und Vertraulichkeit von Informationen in dynamischen Umgebungen. Hierbei werden Anforderungen der Geschäftsprozesse berücksichtigt und ein Werkzeug bereitgestellt, um dem Einzelnen die Kontrolle über den Austausch seiner eigenen Informationen zu ermöglichen. Ermöglicht wird diese über die Schaffung einer europaweiten, gemeinsamen, sicheren Infrastruktur. Im TAS3 EC FP7 [Mee11] werden Möglichkeiten zur Annotation von Geschäftsprozessen vorgeschlagen, welche sich jedoch abermals auf Authentisierung und Autorisierung sowie das Audit-Logging konzentrieren. Die später ablaufenden Geschäftsprozesse erfordern bei Ausführung eine datenspezifische Autorisierung oder sicherheitsspezifische Nutzereinbeziehung. Dem Föderationsgedanken wird hierbei mittels gemeinsamer Ontologie begegnet, welche die Beziehung zwischen Kernksicherheitskonzepten definiert.

Der letztgenannte Ansatz bezieht nicht nur nicht-technische Aspekte ein, sondern liefert auch einen Mehrwert bei der Entwicklung von sicheren Geschäftsprozessen in Bezug auf die Verwendung von Daten. Es wird jedoch kein gemeinschaftliches Verständnis von Schutzbedarfen und dem Risikomanagement über mehrere Organisationen hinweg gefördert. Auch die passende Auswahl von IT-Ressourcen wird nicht als Ergebnis der Risikoeinschätzung von Geschäftsprozessen vorgesehen. TAS3 kann somit zwar als Hilfsmittel für die Kontrolle des Datenflusses in Föderationen, nicht aber als prozessbasiertes Werkzeug entlang des gesamten Lebenszyklus von Geschäftsprozessen über mehrere Organisationen hinweg eingesetzt werden.

Aufgrund der verschiedenen Cloud-spezifischen Gefährdungen, wie vorgestellt von Subashini und Kavitha [SS11], wurde das Open Certification Framework von der Cloud Security Alliance (CSA) entwickelt. Es ist ein

Rahmenwerk zur globalen, akkreditierten, vertrauenswürdigen Zertifizierung von Cloud-Providern [All14]. Es erlaubt die Adressierung von Compliancebedarfen durch Best-Practice-Ansätze, die bei der Verwendung von Cloud-Services in Geschäftsprozessen eingesetzt werden können. Für Cloud-Umgebungen wurden von Bernsmed et. al. in [BJMU11] zudem spezielle Cloud-SLAs vorgeschlagen, um einheitliche Sicherheitsniveaus in verteilten System- und Organisationslandschaften zu begünstigen.

Die Vielzahl vorhandener Ansätze, welche als Quelle für Vorschläge zur Etablierung eigener Compliance-Anforderungen herangezogen werden können, können mit dem Unified Compliance Framework (UCF) [Fro11] harmonisiert werden. Das UCF ist ein patentiertes GRC-Rahmenwerk und besteht aus einer Datenbank, welche die Relation vieler regulatorischer Kontrollen aus externen Quellen zu vereinheitlichten, generischen Kontrollen beinhaltet. Es kann somit als zentrale Anlaufstelle für die Auswahl von Compliance-Kontrollen genutzt werden.

Für die Betrachtung des in diesem Kapitel skizzierten Szenarios bilden die in der Literatur gefundenen Ansätze entsprechend keinen Mehrwert unter Maßgabe der Zielstellung eines konsistenten, sicherheitsoptimierten Geschäftsprozessmanagements.

8.4 Zusammenfassung

Dieses Kapitel beschreibt, dass der Föderierungsfall des Ende-zu-Ende-Prozesses Order-to-Cash (OTC) die größte Komplexität hinsichtlich der Schnittstellen zu anderen Prozessschritten, Systemen und Organisationen aufweist. Ferner wurde prägnant demonstriert, dass eine in Hinblick auf das Gesamtsystem ganzheitliche, hinreichende Absicherung eines föderierten OTC mit sowohl traditionellen Mitteln als auch aktuell diskutierten Ansätzen nicht gelingen kann. Das Problem wird nachfolgend detailliert diskutiert.

9 Problemisolierung

Dieses Kapitel beschreibt die identifizierbaren Probleme bei der Behandlung föderierter Ende-zu-Ende-Geschäftsprozesse mittels traditioneller GRC-Rahmenwerke. Zudem wird das Element isoliert, welches für das Management von GRC-Anforderungen geeignet ist. Schließlich werden Geschäftsprozessrahmenwerke betrachtet sowie Notwendigkeit und Relevanz eines neuen Rahmenwerks diskutiert.

9.1 Findings

Legt man die in der Literatur verfügbaren und in Teil II untersuchten Konzepte an das Problemfeld von integrierten oder teil-integrierten Föderationen (beispielsweise Unternehmenskooperationen oder langfristige Lieferantenbeziehungen) aus Kapitel 8 an, so wird deutlich, dass die bestehenden GRC-Rahmenwerke mit ihrer Limitierung auf den Einflussbereich einer Einzelorganisation nicht ausreichend sind. Dies begründet sich durch den Referenzpunkt, der seitens einer Organisation, welche das jeweilige Rahmenwerk verwendet, für das Risikomanagement der verarbeiteten Informationen angesetzt wird. Hier wird schon bei der Festsetzung des Schutzbedarfs der im eigenen Geschäftsprozess verarbeiteten Informationen lediglich von der Relevanz dieser Information für die eigene Organisation ausgegangen. In einem kooperierenden Geflecht aus Auftraggebern, Auftragnehmern, Lieferanten für Produkte und Dienstleistungen, insbesondere Lieferanten für ausgelagerte Teile des eigenen Geschäftsprozesses, ergibt

sich der Schutzbedarf jedoch nicht aus dem Bezugspunkt der Einzelorganisation. Vielmehr gilt hier der für die jeweilige Information höchste Schutzbedarf für einen der beteiligten Föderierungspartner.

Standards wie die ISO 27001 können zwar, so sie in jeder der beteiligten Organisationen erfolgreich umgesetzt wurden, einen Beitrag für die Sicherheit der Föderation leisten. Selbst wenn jede der beteiligten Organisationen jedoch einen Standard etabliert, rührt es aus der Natur separat realisierter Managementsysteme, dass

- keine zentrale Steuerung der ISMS-Prozesse,
- kein für die Föderation allgemeingültiges Verständnis der Schutzbedarfe der Informationen,
- kein direkter Bezug von Maßnahmen und Zuständigkeiten zum föderierten Geschäftsprozess und den darin genutzten Ressourcen zur Informationsverarbeitung (auch die ISO 27001 liefert zwar einen Anhang mit Maßnahmen, jedoch lassen sich Maßnahmen nicht automatisch auf Basis der Methodik zuordnen)

existieren.

Den existenten GRC-Rahmenwerken fehlt es somit an einer hinreichenden Betrachtung des Gesamtgefüges aus Prozessen, Menschen, Arbeit und Technik, im Speziellen hinsichtlich des föderierten Gedankens von Geschäftsprozessen und ihrer partiellen Auslagerung. Gleichzeitig existieren jedoch auch weitere, ältere Modelle, auch wenn diese nicht primär die Informationssicherheit zum Inhalt haben. Auch diese wurden vorliegend untersucht. Sie fokussieren sich jedoch wiederum entweder auf ein Informationsmodell – entweder aus Geschäfts- oder aus Datensicht, wie die Ansätze von [BCN92], [MS98b] oder [MS98a], oder ausschließlich auf speziellen Anforderungen und Kontrollen [BFN03], [ZLR93].

Traditionelle Ansätze nutzen zudem ein „Dokumentationsprinzip“, welches auf der fortwährenden Aktualisierung etablierter Prozesse und Prozesserzeugnisse besteht. Ein häufig beobachtetes Problem in Unternehmen

ist gleichwohl das Fehlen ausreichender Dokumentationen, welche zur erfolgreichen Durchführung eines ISMS-Projektes jedoch absolut notwendig sind. Dieses Problem ist jedoch insoweit nachvollziehbar, dass das Pflegen von Dokumentationen aufgrund ständiger Änderungen durch Innovation, neue externe Regelungen oder interne Restrukturierung hohe Kosten verursacht, deren Nutzen nicht direkt nachvollziehbar ist.

Letztlich wird grundsätzlich gern beklagt, dass der Mensch das schwächste Glied der Sicherheitskette darstellt [Glo09]. Diesem Problem wird (im Idealfall) mit massiven Mitarbeiterschulungen und Awareness Trainings für die Geschäftsführung begegnet. Es rührt jedoch aus der Natur der Sache, dass wenn der Mensch nur als Objekt für an ihm zu realisierende Maßnahmen, und nicht als sicherheitsschöpfender Teil der Kette genutzt wird, er nicht Teil der Lösung, sondern Teil des Problems bleibt. Dies unterstreicht, dass ein Denken ausgehend von den Ressourcen – unabhängig ob IT- oder Personal-Ressourcen – kein zielführendes Mittel für konsistentes Informationssicherheitsmanagement darstellt. Es geht einher mit der Argumentationslinie aus Abschnitt 6.1.2, in der bereits dargelegt wurde, dass auch strukturiertes IT-Management keinen maßgeblichen Einfluss auf das Beseitigen von tieferen Ursachen von GRC-Problemen haben kann. Die Schwierigkeiten beginnen bei der Entwicklung von Geschäftsprozessen, nicht bei den genutzten Ressourcen.

Dies alles gilt bereits im Falle nicht-föderierter Szenarien, obgleich hier mit traditionellen Mitteln ein nützliches Ergebnis erzielt werden kann. Im Bereich von Föderierungen stellt sich nun jedoch ganz besonders stark die Frage nach dem verknüpfenden Element, welches Ausgangspunkt der Betrachtung für die Reduzierung von GRC-Problemen darstellen sollte. Die innerhalb der beteiligten Organisationen verwendeten Ressourcen unterliegen potenziell den gleichen organisatorischen Grenzen wie die traditionellen Rahmenwerke. Die im Geschäftsprozess abgearbeiteten Aufgaben sind ebenfalls nicht das Element, welches die Organisationen miteinander verbindet, da ja gerade die Aufteilung der Aufgaben Sinn der Föderierung ist.

Es bleibt nur der Geschäftsprozess selbst, welcher das einzige Element darstellt, welches die beteiligten Organisationen miteinander verbindet. Die innerhalb des Geschäftsprozesses verarbeiteten Informationen werden angereichert und sind letztendlich Grund dafür, dass Werte geschöpft werden. Entsprechend lässt sich hier das Element für eine weitere Betrachtung isolieren.

Wenn jedoch Geschäftsprozesse Ausgangspunkt für moderne GRC-Überlegungen sein sollen, muss geprüft werden, wie traditionelle Rahmenwerke, welche die Entwicklung solcher Geschäftsprozesse zum Inhalt haben, mit GRC-Anforderungen umgehen.

9.2 Traditionelle Geschäftsprozessrahmenwerke

Bis hier hin lässt sich feststellen, dass traditionelle GRC-relevante Rahmenwerke nicht in der Lage sind, beziehungsweise sich nicht zur Aufgabe stellen, sichere Geschäftsprozesse zu entwickeln. Ironischerweise ist das Gegenteil ebenso wahr: Rahmenwerke, welche den Bau von Geschäftsprozessen zur Aufgabe haben, adressieren GRC-Anforderungen entweder gar nicht oder nur unzulänglich.

Geschäftsprozessmanagement ist nicht länger nur ein Werkzeug für die Entwicklung von Arbeitspaketen, welche sequenziell aneinandergereiht werden, um Effektivität und Effizienz hinsichtlich eines geschäftlichen Nutzens zu erzeugen. Aktuelle Geschäftsprozessrahmenwerke müssen dem Zweck der Ableitung von Prozessen ausgehend von Geschäftszielen dienen und dabei verschiedene Erfolgs- und Risikofaktoren mit einbeziehen. Zusätzlich müssen Geschäftsprozessrahmenwerke jedoch potenzielle Gefährdungen gegen Menschen, Dienste und Technologien adressieren, die jeden Geschäftsprozess unterstützen. Geschäftsprozesse werden zunächst stets geplant und später implementiert, im Anschluss kann jeder Geschäftsprozess gemessen und optimiert werden.

9.2.1 ARIS Process Lifecycle

Es existieren verschiedene Geschäftsprozessrahmenwerke. Eines dieser Rahmenwerke ist der ARIS Prozessmanagement-Lebenszyklus [Sch00]. ARIS ist ein Werkzeug zum Mappen der Geschäftsstrategie zu Geschäftsprozessen mit Augenmerk auf Effektivität und Effizienz. Es hat große Akzeptanz in Industrien über verschiedene Sektoren erhalten. Im von ARIS vorgeschlagenen methodischen Ansatz werden Geschäftsprozesse abgeleitet von Geschäftszielen und externen Erfolgsfaktoren, ihrem Potenzial und ihren geschäftsseitigen Gefährdungen. In einer Abfolge von Schritten werden diese Geschäftsprozesse analysiert, geplant, implementiert, gemessen und optimiert. GRC-Anforderungen werden hingegen nicht adressiert.

9.2.2 McKinsey 7s Framework

Zudem existiert das McKinsey 7s Framework, welches Struktur, Strategie, Systeme, Fertigkeiten, Stil, Personal und gemeinsame Werte von Organisationen adressiert. [T84] Das 7s Framework ist ein Managementmodell, welches Änderungen der Gesamtorganisation durch erfolgte interne Anpassungen erfassbar macht. Es kann somit als Diagnosewerkzeug für Change-Management-Prozesse aufgefasst werden. GRC-Anforderungen werden hier ebenfalls nicht adressiert.

9.2.3 Weitere Rahmenwerke

Folgende andere Geschäftsprozessrahmenwerke konnten ermittelt werden, welche oft Referenzmodelle darstellen:

- MIT Process Handbook [oT03]
- OPEN Process Framework [Org09]
- Process Classification Framework (PCF) der APQC [APQ14]

- Value Chain Reference Model (VRM) der Value Chain Group [Gro14]
- Supply Chain Operations Reference (SCOR) [Cou14]
- Value Chain Modell nach Michael E. Porter [Por08]
- eTOM [TMF14]
- SPICE [QMC14]

Keines dieser Rahmenwerke adressiert GRC-Anforderungen im Rahmen der Entwicklung föderierter Ende-zu-Ende-Geschäftsprozesse.

Auch wenn inzwischen verschiedene Empfehlungen für die Behandlung von Governance und Compliance in Geschäftsprozessen von Markus und Jacobsen (2010) vorhanden sind, adressieren die bisherigen Rahmenwerke keine GRC-Anforderungen im Rahmen der Entwicklung von Geschäftsprozessen, insbesondere bei föderierten Ende-zu-Ende-Szenarien.

9.3 Bezugsebene und Gültigkeitsbereich

Der Gültigkeitsbereich des vorliegend zu entwickelnden Modells bezieht sich auf Ende-zu-Ende-Prozesse und ihre unterstützenden ERP- und SCM-Konfigurationen, die sich aus einer Föderation von mindestens zwei Organisationen zusammensetzen. Diese Konfigurationen arbeiten mit Transaktionen (Softwareinstanzen, welche einen Informationsfluss steuern, der über einen Geschäftsprozess abgebildet wird).

Vorliegend wird versucht, die MAT-Einheiten dieser Anwendungsfälle effizienter abzusichern als es durch die bisherigen Modelle realisiert werden kann. Genauer soll ein Modell entworfen werden, welches vom Design der Geschäftsprozesse bis zum Monitoring der verarbeiteten Informationen reicht. Der OTC soll fortwährend als Leitlinie dienen.

9.4 Zusammenfassung

Dieses Kapitel zeigt, welche Probleme bei der Absicherung föderierter Geschäftsprozessstrukturen existieren. Hierzu zählen die nicht vorhandene zentrale Etablierung und Steuerung von ISMS-Prozessen, das mangelnde objektive Verständnis von Schutzbedarfen der in föderierten Prozessen verarbeiteten Informationen sowie der fehlende Bezug von Maßnahmen und Zuständigen zum Gesamtprozess.

Klassische GRC-Rahmenwerke können aufgrund ihrer organisatorischen Grenzen, ihrer mangelnden Ausrichtung am Geschäftsprozess und der fehlenden Möglichkeit, Geschäftsprozesse zu entwickeln, Föderierungen nicht hinreichend adressieren. Der Geschäftsprozess ist jedoch das einzige Element, welches Föderationen miteinander verbindet. Rahmenwerke zur Entwicklung von Geschäftsprozessen adressieren hingegen GRC-Anforderungen entweder gar nicht oder unzureichend in Bezug auf Ende-zu-Ende-Geschäftsprozesse.

Hierzu ist eine Sicht notwendig, welche bislang noch nicht adressiert wird: die Entwicklung von Geschäftsprozessen, unter Verwendung von für den Geschäftszweck potenziell nützlichen und gleichzeitig hinreichend ungefährlichen Ressourcen in Abhängigkeit von einem einheitlich verstandenen Schutzbedarf über die zur Ausführung von Ende-zu-Ende-Prozessen beteiligten Organisationen.

Ein neues Rahmenwerk zum Management GRC-optimierter Geschäftsprozesse besitzt große Relevanz, da sich bei unsicheren Marktlagen und starker Innovation (vgl. Kapitel 4.7) bei gleichzeitig leicht realisierbaren organisatorischen (vgl. Kapitel 4) und technischen Möglichkeiten (vgl. Kapitel 5), Föderierungen zunehmend verbreiten werden, und die Notwendigkeit der Adressierung von (sich zudem ständig ändernden) Anforderungen unverändert ist und mit den gegenwärtigen Mitteln (vgl. insb. Kapitel 6) nicht hinreichend adressiert werden kann (vgl. Kapitel 8.2 und 9.2).

Teil IV

Realisierung des Rahmenwerks

Überblick Teil IV

„Die Gesellschaft der Zukunft ist zum Vertrauen verurteilt."
(Peter Sloterdijk, Philosoph)

Die in Teil III benannte Lücke soll nun durch die Entwicklung eines neuen Ansatzes adressiert und die Erfüllung definierter Anforderungen im Anschluss validiert werden.

Die notwendigen Anforderungen an ein neues GRC-optimiertes Geschäftsprozessrahmenwerk werden in Kapitel 10 erhoben. Kapitel 11 beschreibt die Konstruktion des Rahmenwerks unter Berücksichtigung der definierten Anforderungen. Kapitel 12 schließt mit einer Evaluierung samt Akzeptanzprüfung des entwickelten Rahmenwerks.

10 Anforderungserhebung

In diesem Kapitel sollen die aus der vorherigen Problembetrachtung resultierenden Anforderungen für die Entwicklung des föderativen ISMS und dessen nachgelagerte Validierung erhoben werden. Diese werden von den Stakeholdern abgeleitet, welche zuvor identifiziert werden.

10.1 Stakeholder und Use Cases

Aus der Problembeschreibung wird die Einnahme der Perspektive des Geschäftsprozesses notwendig, wodurch sich automatisch die Geschäftsführung als wichtigster Stakeholder ableitet. Die Geschäftsführung ist für die Durchführung eines Geschäftsprozesses auf Basis der Zielrichtung der Organisation verantwortlich und hat entsprechende Entscheidungskompetenz inne. Ferner kann sie die Föderierungs- und auch die Risikostrategie maßgeblich beeinflussen. Die strukturierte Entwicklung eines solchen Geschäftsprozesses ist ein elementarer Use Case, welcher adressiert werden soll.

Für taktische und operative Belange des Risikomanagements sind Beauftragte für Informationssicherheit und Compliance verantwortlich, welche vorliegend unter der Personengruppe „GRC-Management“ benannt sein sollen. Sie steuern die Nutzung zugewiesener Ressourcen für die Durchführung von (GRC-)Prozessen, welche gesetzliche und informationssicherheitstechnische Anforderungen der vorgegebenen Geschäftsprozesse realisieren müssen. Der Use Case, welcher hier bedient wird, ist sowohl die

Auswahl von zur Risiko-Strategie passenden Ressourcen, als auch ihre Beeinflussung durch geeignete Maßnahmen, welche ableitbar sein müssen.

Schließlich sind zur Ausführung der Aufgaben des Geschäftsprozesses, wie insbesondere in den Grundlagen erläutert, sowohl Menschen als auch IT-Systeme mitsamt der darunterliegenden Infrastruktur notwendig. Hier lassen sich das IT-Management (als Personengruppe für IT-Manager, Administratoren, Finanzverwaltung und verwandte Aufgaben), das Personalmanagement (über den gesamten Lebenszyklus des Mitarbeiterwesens, von der Personalgewinnung über die Weiterbildung, Bewertung, Verwaltung bis zur Entlassung von Mitarbeitern) sowie sämtliches Personal des Infrastrukturmanagements (beispielsweise Facility Management) identifizieren.

Nicht alle zur Erfüllung der Aufgaben notwendigen Personenkreise sind direkt an der Nutzung des Rahmenwerks beteiligt. Viele erleben abermals lediglich die Symptome seiner erfolgreichen Verwendung. Die direkt an der Nutzung des Rahmenwerks beteiligten Stakeholder sind stets jene, die den künftigen (GRC-)Prozessen angehören, welche zur Realisierung der Geschäftsprozesse beitragen (Haupt-Use-Case). Dies sind die Geschäftsführung („G“), das GRC-Management („GRC“) und das IT-Management („IT“), wobei letzteres in Vertretung sämtliche auf die IT Einfluss nehmenden Personengruppen meint, also beispielsweise auch IT-Berater.

Hieraus lässt sich erkennen, dass das Rahmenwerk in der Lage sein muss, die strategische, taktische und operative Ebene abzubilden. Die strategische Ebene meint die Adressierung betriebswirtschaftlich sinnvoller Geschäftsprozesse. Die taktische Ebene meint das Mapping von Geschäftsanforderungen hin zur Ressourcensteuerung. Die operative Ebene meint eben diese Ressourcensteuerung, wobei die personalseitige Steuerung durch das Rahmenwerk kaum beeinflusst werden muss, da diese für die Zielstellung der Informationssicherheitsoptimierung nicht direkt von Relevanz ist. Die IT-seitige Steuerung ist jedoch von zentraler Bedeutung, da die Entscheidung bestimmter technischer Ressourcen (beispielsweise Cloud-Services) für das Risikomanagement einen entscheidenden Einfluss hat. Hier leitet

sich entsprechend die Anforderung der Möglichkeit zur Generierung von Maßnahmen auf Basis von Anforderungen ab.

Ferner ist Zielstellung sämtlicher Stakeholder die effektive Adressierung sowohl föderierter als auch nicht-föderierter Szenarien, da für die zuvor angesprochene Flexibilität bei hoher Produktkomplexität und hoher Marktunsicherheit das Geschäftsszenario frei gestaltbar sein muss. Schließlich kann sich der Geschäftsprozess selbst ebenfalls ändern, wodurch sich für die Geschäftsführung die Abbildung eines gesamtintegrierten GRC-Managements über die gesamte Lebensspanne eines Geschäftsprozesses ergibt. Das GRC-Management hat hier wiederum ein Interesse, bereits vorhandene Werkzeuge möglichst verlustfrei integrieren zu können, wodurch sich die Anforderung der Einhaltung des PDCA-Zyklus ergibt.

Letztlich besteht für die Geschäftsführung zur Wahrung von Nachweisbarkeit, Revisionssicherheit, und verschiedener Wettbewerbsvorteile ein grundsätzliches Interesse an der Aufrechterhaltung und/oder Etablierung von Zertifizierungen aufgrund positiver Außen- und Innenwirkung.

10.2 Anforderungen an ein GRC-optimiertes GP-Rahmenwerk

Die aus der Stakeholder-Analyse abgeleiteten Anforderungen sollen nachfolgend noch einmal zusammengetragen werden. Zunächst sei darauf hingewiesen, dass die in Abschnitt 7.1 identifizieren Kriterien des Vergleichs vorhandener Rahmenwerke angelegt werden können, um einen späteren Vergleich des entwickelten Rahmenwerkes zu den bisherigen zu ermöglichen. Ferner muss die Absicherbarkeit der in Kapitel 8 am Beispiel des OTC analysierten, Ende-zu-Ende-Föderierungsszenarien hinreichend adressiert werden können, um eine Lösung für das konkrete Problemfeld zu bieten.

Im Sinne der Adressierung von Stakeholder-Interessen muss das zu entwickelnde Rahmenwerk daher die in Tabelle 10.1 aufgeführten Anforderungen adressieren.

#	Anforderung	Betr.
A1	Integration der Geschäftsebene (bezüglich Unterstützung maximaler Flexibilität der Prozessgestaltung zur Erreichung des Geschäftsziels sowie der Adressierung geschäftskritischer Fragestellungen: Kosten/ Nutzen-Verhältnis, Erfolgsfaktoren, Risikofaktoren)	G
A2	Integration der GRC-Ebene (Überlegungen für die zu adressierenden Schutzbedarfe und regulatorischen Anforderungen)	G, GRC
A3	Integration der Ressourcen-Ebene (Überlegungen zur Ausgestaltung von Menschen und Technologie, insbesondere zur Etablierung von Schnittstellen)	GRC, IT
A4	Effektive Generierung von Anforderungen und Maßnahmen für die zu behandelnden Geschäftsprozesse	GRC, IT
A5	Möglichkeit zur Nutzung des neuen Rahmenwerks zur Adressierung von nicht-föderierten Szenarien (konkretes Ziel: Erhalt der gleichen Resultate wie bei Behandlung mit ISO 27001)	G, GRC
A6	Möglichkeit zur Nutzung des neuen Rahmenwerks zur Adressierung föderierter Szenarien (konkretes Ziel: Erhalt von Resultaten ohne das in Kapitel 9 erläuterte Problem unterschiedlicher Schutzbedarfe für Informationen innerhalb eines gemeinsamen Geschäftsprozesses)	G, GRC
A7	Gesamtbildhafte Abbildung eines integrativen Managements von Governance, Risk und Compliance mit Fokus auf Informationssicherheit entlang der Lebensspanne eines Geschäftsprozesses	G, GRC
A8	Konformität mit dem PDCA-Zyklus	G, GRC
A9	Zertifizierbarkeit	G

Tabelle 10.1: Anforderungen an neues Rahmenwerk

10.3 Zusammenfassung

Es wurden Kriterien für ein neu zu entwickelndes Rahmenwerk erfasst, welche sich auf die Integration von Geschäfts-, Ressourcen- und GRC-Ebene beziehen. Es werden Möglichkeiten zur Generierung von Maßnahmen für föderierte und nicht föderierte Szenarien gefordert. Hierbei sollen GRC-Anforderungen über den gesamten Lebenszyklus von Geschäftsprozessen adressiert werden, ohne den PDCA-Zyklus zu verletzen. Für eine Evaluation sollen all diese Kriterien nach Konstruktion des ISMS an selbiges angelegt und bewertet werden.

11 Konstruktion des Rahmenwerks

In diesem Kapitel wird ein Vorschlag für ein GRC-optimiertes Geschäftsprozessrahmenwerk erarbeitet. Es wird gezeigt, welche Prämissen für die Konstruktion verwendet werden, von welchen Sichten ausgegangen wird und wie einzelne Phasen entlang des Lebenszyklus von Geschäftsprozessen angesetzt werden sollten.

11.1 Konstruktionsprämissen

Aus den definierten Anforderungen ergibt sich eine von bisherigen ISMS grundsätzlich verschiedene Perspektive. Traditionelle Ansätze für Informationssicherheit gehen von bereits präsenten Geschäftsprozessen aus, da sie als von der Geschäftsführung unabhängiges Instrument angedacht und somit nur in der Lage sind, Symptome im Bereich beteiligter IT-Ressourcen zu adressieren, wie zuvor erläutert. Gleichzeitig wurde festgestellt, dass für föderierte Geschäftsszenarien lediglich die Basis des Geschäftsprozesses als Bindeglied über die beteiligten Organisationen angesehen werden kann.

11.1.1 Einnahme der Perspektive des Geschäftsprozesses

Aus beiden Punkten ergibt sich die Notwendigkeit zur Zentralisierung des Geschäftsprozesses. Ein Geschäftsprozess muss entlang seines Lebenszyklus, d.h. vom Entwurf über den Betrieb bis zur Änderung von Geschäftsanforderungen GRC-seitig optimiert werden. Entsprechend wird vorliegend

kein neues ISMS konstruiert, sondern ein spezielles Rahmenwerk zum Management von Geschäftsprozessen für föderierte sicherheitskritische Umgebungen entworfen.

11.1.2 Trennung von Geschäftsprozessen und GRC-Prozessen

Bereits auf Ebene der Geschäftsprozesse lassen sich GRC-Anforderungen identifizieren, die in direkter Abhängigkeit von der Kritikalität der über den Geschäftsprozess verarbeiteten Informationen in den jeweiligen Aufgaben stehen, die für die Ausübung des Geschäftsprozesses notwendig sind. Analyse, Entwurf, Implementierung, Monitoring und Anpassung von Geschäftsprozessen werden jedoch als vollkommen isolierte Prozesse angesehen. Der Geschäftsprozess ist Betrachtungsgegenstand und Resultat der GRC-Prozesse.

11.1.3 Einbeziehung vorhandener Rahmenwerke

Die Integration von Geschäfts-, Ressourcen- und der GRC-Ebene erfordert ein sehr breites Fundament. Viele Teilprobleme zur Adressierung der notwendigen Aufgaben entlang des Geschäftsprozess-, IT-, Personal- und GRC-Managements wurden in der Literatur, für sich genommen, mehrfach in Tiefe diskutiert. Der Mehrwert des zu entwickelnden Rahmenwerkes soll in der Orchestrierung der beteiligten Ebenen liegen, um die vielseitigen Geschäftsprozessmanagement-Aufgaben für das vorliegende Problemfeld zu integrieren.

11.2 Grundstruktur des Rahmenwerks

Für ARIS wird in [EI08] ein Vorschlag für Sichten auf Geschäftsprozesse gegeben. ARIS fokussiert sich hierbei jedoch auf Effektivität und Effizienz

von Geschäftsprozessen. Es wird vorgeschlagen, die vorhandenen Sichten wie folgt zu erweitern:

- Ressourcen-Sicht: für Geschäfts- und GRC-Prozesse relevantes Personal, Anwendungen, Infrastruktur und ihre Beziehungen untereinander
- GRC-Funktions-Sicht: Aktivitäten zum Entwurf von Input für Entwicklung und Beeinflussung von Geschäftsprozessdefinitionen
- GRC-Daten-Sicht: Anforderungen (Restriktionen und Obligationen für geschäftliche Funktionen und Datennutzung), Key-Performance-Indikatoren (KPI), Monitoring- und andere Daten um GRC-Funktionen zu verarbeiten
- GRC-Prozess-Sicht: Verwendung von GRC-Funktionen und GRC-Daten zur Lieferung von Geschäftsprozessentwürfen
- Geschäftsfunktions-Sicht: Transaktionen/Aktivitäten, welche geschäftliche Daten auf wohl-definierte Weise verwenden (Arbeitspakete)
- Geschäftsdaten-Sicht: geschäftliche Informationsobjekte und ihre Attribute sowie deren Relation untereinander
- Geschäftsprozessmodul-Sicht: Nutzung von GRC-Prozess-Ergebnissen zur Verwendung von Geschäftsfunktionen, Geschäftsdaten und Ressourcen zur Lieferung von Produkten und Dienstleistungen
- Sicht für Services und Produkte: Ergebnis von Geschäftsprozessen zur Wertbeitragslieferung

Abbildung 11.1 illustriert diese Sichten-Integration.

Der Vorteil der frühzeitigen Integration von GRC-Anforderungen ist, dass bereits die Selektion von (Personal- und IT-relevanten) Ressourcen beeinflusst werden kann. Davon unberührt lassen sich später Maßnahmen aussprechen, welche zu erwartenden Incidents entgegenwirken können.

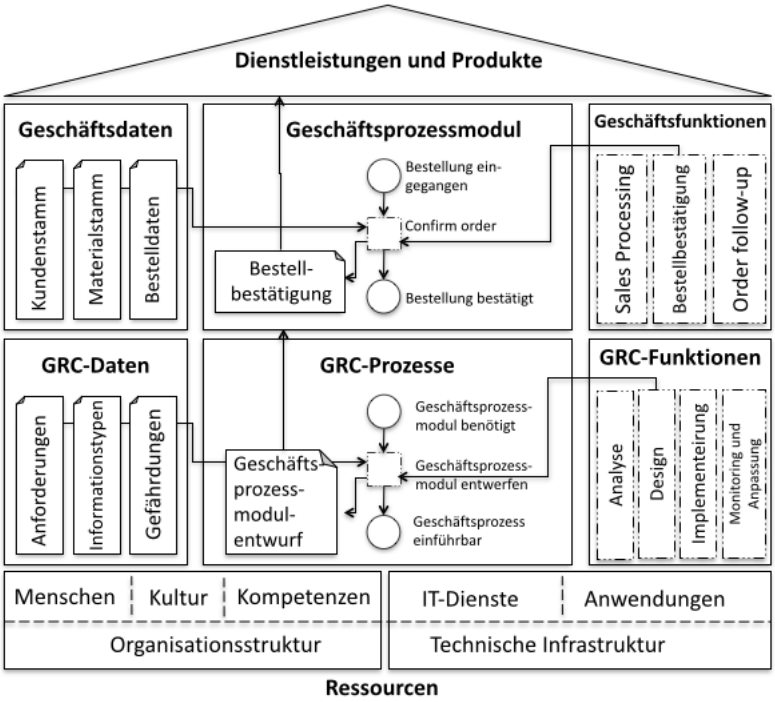

Abbildung 11.1: Integrierte Sichten auf Geschäftsprozesse

11.3 Geschäfts- und GRC-Daten

Im Bereich der Informationssicherheit sind zunächst die in Kapitel 3.3 definierten Schutzziele der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit als zu erfassende Daten von zentraler Bedeutung. Auch sind die Gefährdungen und die für diese gegenüber jeder Organisation individuell verschiedenen Schutzbedarfe und die vorherrschenden Risiken, bestehend aus den für eine Gefährdung wirkenden Schadenshöhen und Eintrittswahrscheinlichkeiten relevant. Vorliegend wird jedoch argumen-

tiert, dass ganzheitliche GRC-Betrachtungen nicht losgelöst von den im Geschäftsprozess verarbeiteten Informationen vollzogen werden können. Von Oracle [Ora12] werden im Rahmen eines Enterprise Architecture Models hierfür folgende Informationsbereiche definiert, welche geschäftliche Informationen vorhalten können, die direkte Relevanz für sämtliche GRC-Betrachtungen haben:

- Transaktionsdaten: Daten aus Geschäftstransaktionen die während der Ausführung von Aufgaben eines Geschäftsprozesses anfallen
- Metadaten: Beschreibung der zuvor genannten Daten (Name, Einheiten, Kalkulationen, etc.)
- Stammdaten: nicht durch Transaktionen bewegte, auf Geschäftsebene angesiedelte Daten von Entitäten, beispielsweise Kunden, Lieferanten und Produkte.
- Referenzdaten: intern verwaltete oder extern bezogene Fakten zur wissensbasierten Unterstützung der Verarbeitung von Transaktionen und Stammdaten, beispielsweise Geo- und Marktdaten.
- Unstrukturierte Daten: über 70% der Assets von Unternehmen, beispielsweise Dokumente, Multimediadateien und Geospatialdaten.
- Analytische Daten: Ableitungen von Geschäftsabläufen und Transaktionsdaten für Reportingzwecke.
- Big Data: große Datenaufkommen, welche aufwändig zu speichern, durchsuchen, teilen, visualisieren und analysieren sind.

Durch den Inhalt der über die geschäftlichen Daten transportierten Informationen folgt die Bewertung des Schutzbedarfs. Somit bilden sie zunächst den Ausgangspunkt einer weiteren Betrachtung zum Bau des Geschäftsprozesses. Die unterschiedlichen Arten der Daten fordern der IT unterschiedliche technische Realisierungsformen zur Speicherung und Verarbeitbarkeit ab. Entsprechend werden hier Maßnahmen relevant, durch welche die Implementierung des Geschäftsprozesses beeinflusst wird. Anschließend muss der Zugriff auf die Informationen, welche über diese Daten ausge-

tauscht werden, überwacht werden, um der Einhaltung der informationssicherheitsseitigen Anforderungen gerecht zu werden. Zusätzlich werden die für einen Geschäftsprozess administrativ-betriebswirtschaftlich bedeutsamen Daten relevant, wie sie in ARIS beschrieben wurden. Hierunter fallen Geschäftsprozesskosten, Potenzial-, Stör- und Erfolgsfaktoren. Entsprechend bildet sich ein komplexes Geflecht aus betriebswirtschaftlich und sicherheitstechnisch relevanter Daten heraus. Eben dieses Geflecht ist vorliegend mit „GRC-Daten“ gemeint – „Geschäftsdaten“ meinen hingegen die beim Geschäftsprozess inhaltlich relevanten Daten (Stamm- und Bewegungsdaten, beispielsweise Materialstammsätze und Bestelldaten).

Alle zuvor genannten Daten sind für GRC-Betrachtungen relevant, um Geschäftsprozesse zu analysieren, zu entwickeln, zu implementieren, zu monitoren und anzupassen. Sie erstrecken sich somit über den gesamten Lebenszyklus eines Geschäftsprozesses, welcher durch eine zusätzliche Dimension, die GRC-Prozesse, verwendet werden können.

11.4 GRC-Prozesse

Die zuvor beschriebenen Sichten lassen sich verwenden, um den gesamten Lebenszyklus eines Geschäftsprozesses zu behandeln. Unter Verwendung der beschriebenen Sichten wird nachfolgend gezeigt, wie sich diese Sichten verwenden lassen, um föderierte Geschäftsprozesse zu optimieren. Hierzu existieren die Phasen der Analyse, des Designs, der Implementierung, des Monitorings und der Anpassung von Geschäftsprozessen.

11.4.1 Geschäftsprozess-Analyse

Die Analyse-Phase dient einerseits der Erfassung bereits bestehender Geschäftsprozesse, richtet sich andererseits aber auch an völlig neu zu entwickelnde Geschäftsprozesse.

Die Analyse-Phase besteht aus folgenden Teilschritten:

1. Definition des Betrachtungsraumes (Scope-Definition)
2. Ermittlung von Position und Wertigkeit des ggf. bereits bestehenden Geschäftsprozesses in der Geschäftsprozesslandschaft der Organisation
3. Ermittlung der aktuellen Geschäftsprozesskosten
4. Ermittlung der Potenzial-, Erfolgs- und Störfaktoren
5. Erfassung der Ressourcen-Konfiguration des Geschäftsprozesses
6. Identifizierung der kritischen Geschäftsinformationen
7. Identifizierung der regulatorischen Obligationen
8. Ermittlung der resultierenden Schutzbedarfe der Informationen
9. Identifizierung der Gefährdungen gegen die Informationen auf Basis der aktuellen Ressourcen-Konfiguration des Geschäftsprozesses
10. Identifizierung aktueller und anvisierter Geschäftsziele
11. Identifizierung aktueller und anvisierter IT-Ziele

Abbildung 11.2 stellt diese Schritte schematisch dar. Der Lesbarkeit wegen werden nur GRC-Daten und GRC-Prozessschritte dargestellt.

Zwar werden nach der Scope-Definition zunächst bestehende Elemente identifiziert. Hierunter fallen bereits betriebswirtschaftliche als auch technische Kriterien wie Potenzial-, Erfolgs- und Störfaktoren sowie die Erfassung der aktuellen Personal- und IT-Ressourcen hinweg über alle beteiligten Kooperationspartner, wie sie von ARIS bereits vorgesehen werden.

Von zentraler Bedeutung ist im Anschluss jedoch die Identifizierung kritischer Geschäftsinformationen, unabhängig davon, ob diese bereits durch bestehende MAT-Konstellationen verarbeitet werden oder nicht. Die in einem Geschäftsprozess über verschiedene Informationstypen (siehe Abschnitt 11.3) transportierten Informationen sind einerseits Schnittstelle beteiligter Aufgaben, und somit Träger der Wertschöpfung, genau aus diesem Grund

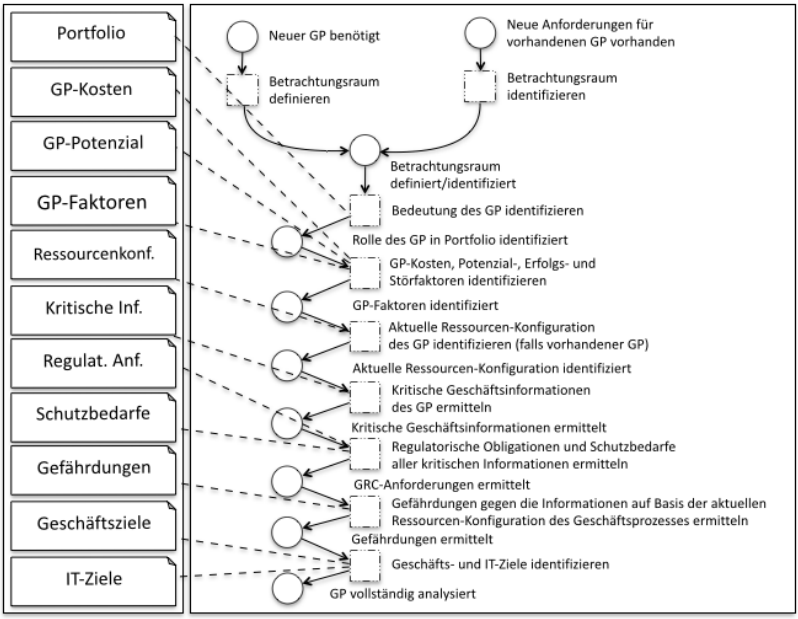

Abbildung 11.2: GRC-Prozess Analyse

aber auch höchstes Schutzobjekt, welches gleichzeitig den Ursprung aller nachgelagerten Überlegungen hinsichtlich GRC-Management bildet.

Die kritischen Geschäftsinformationen sind einerseits vor der Gefährdung des Verstoßes gegen obligatorische Anforderungen, andererseits vor verschiedenen informationssicherheitskritischen Gefährdungen zu schützen. Entsprechend sind zwei Dinge von wesentlicher Bedeutung—die Identifizierung regulatorischer Obligationen, beispielsweise durch Gesetzestexte, und die Schutzbedarfe, welche ausgehend von der Kritikalität der Information für die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu bewerten sind.

Nun sind die tatsächlich anliegenden Gefährdungen, bislang noch unabhängig von ihrem gegenwärtigen Risiko, in Abhängigkeit von der gegenwärtigen technischen Umgebung zu identifizieren. Schließlich sollte geprüft werden, was der Geschäftsprozess aus betriebswirtschaftlicher Sicht leisten soll, woraus sich auch IT-Ziele ergeben. Hier kann COBIT als Werkzeug zum Mapping von Geschäftszielen zu IT-Zielen eingesetzt werden, um Grundlage für die spätere Messung zu bilden.

11.4.2 Geschäftsprozess-Design

Liegen alle notwendigen Informationen über die betriebswirtschaftlichen, GRC-seitigen und ggf. technischen Anforderungen des Geschäftsprozesses von allen beteiligten Partnern vor, kann ein Entwurf des neuen Geschäftsprozesses angegangen werden.

Die Design-Phase besteht aus folgenden Teilschritten:

1. Segmentierung des Geschäftsprozesses in Module
2. Referenzierung der Module zu Organisationen und Abteilungen
3. Abgleich der für die Föderation geltenden Schutzbedarfe
4. Durchführung einer Risiko-Analyse
5. Erstellung eines Geschäftsprozessmodul-Entwurfs
6. Auswahl von GRC-relevanten Maßnahmen
7. Re-Evaluation des Geschäftsprozessmoduls
8. Erstellung finaler Geschäftsprozessmoduldefinition

Abbildung 11.3 stellt diese Schritte schematisch dar. Der Lesbarkeit wegen werden nur GRC-Daten und GRC-Prozessschritte dargestellt.

Zunächst ist der Geschäftsprozess an einer sinnvollen Stelle in Module aufzugliedern. Dies geschieht pragmatisch an der jeweiligen Stelle zweier separater Aufgaben, welche sich durch eine Übergabeinformation, beispielsweise einen Beleg (PDF-Dokument, ERP-Systembeleg, Schriftstück, etc.),

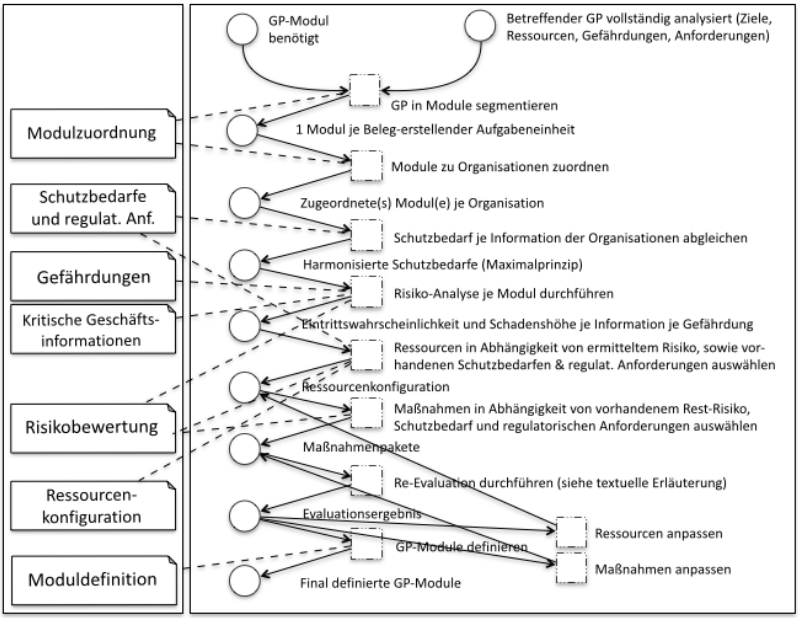

Abbildung 11.3: GRC-Prozess Design

voneinander trennen lassen. Diesen Teileinheiten lassen sich isolierbare Ressourcenzuweisungen zuschreiben, welche es erlauben, dass die jeweiligen Aufgabeninhalte durch unterschiedliche Organisationen abgearbeitet werden können. Dies erfordert eine entsprechende Verteilung der Aufgaben und damit auch der sequenziellen Abfolge der Zusammenarbeit. Dieser Gedanke wurde vom Autor bereits in [NF12] vorgestellt.

Anschließend sind die in der Analyse-Phase individuell ermittelten Anforderungen der Kooperationspartner gegeneinander abzugleichen. Bei der Schutzbedarfsermittlung fand eine Bewertung geschäftskritischer Informationen für die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität statt.

Nun muss ein Wechsel der Perspektiven zwischen den beteiligten Organisationen eingeleitet werden. Dies geschieht für jede Information eines jeden Geschäftsprozessmoduls einer jeden Organisation. Anschließend gilt das Additionsprinzip, das heißt der höchste Schutzbedarf einer Information ist Maßgabe für jeden Kooperationspartner, der diese Information speichert, liest oder weiterverarbeitet.

Auf Basis dieser neuen Schutzbedarfsvorgabe kann nun jeder Partner eine Risiko-Analyse durchführen, bei der für jede eigens identifizierte Gefährdung einer jeden kritischen Information Schadenshöhe und Eintrittswahrscheinlichkeit der Gefährdung erfasst werden—und zwar unter Berücksichtigung bereits vorhandener Maßnahmen. Gegenseitige Audits der Partnerorganisationen sind hierbei ratsam, um die Objektivität dieses GRC-Prozesses sicherzustellen.

Anschließend kann ein Geschäftsprozess-Modul entworfen, das heißt eine personalseitige und technische Ressourcenzuweisung zu den jeweiligen Aufgaben durchgeführt werden, die zum für die Organisation eigenen Teil des Geschäftsprozesses gehören. Schon hier können die bestehenden Risiken gesenkt werden, was einen enormen Vorteil gegenüber der rein symptomatischen Behandlung von Risiken darstellt.

Beispielsweise können Cloud-Dienste bei zu hohen Risiken von Beginn an vermieden werden, wodurch bestimmte Maßnahmen eingespart werden können. Ferner wird eine organisatorische Struktur eingeführt, die die jeweiligen Arbeitspakete, die dafür benötigten Rollen/Profile sowie die notwendigen Kompetenzen der Mitarbeiter berücksichtigt. Darüber hinaus können Stör-, Erfolgs- und Potenzialfaktoren adressiert werden.

Da nicht alle Risiken durch abgeänderte Ressourcenwahl adressiert oder gar vermieden werden können, muss in einem nächsten Schritt die Auswahl GRC-relevanter Maßnahmen vollzogen werden. Zunächst werden allgemeine Kontrollen mit den Gefährdungen und Schutzzielen der geschäftskritischen Informationen des Geschäftsprozesses abgeglichen. Die Inten-

sität einer Kontrolle, das meint die Auswahl einer konkreten technischen Maßnahme, kann dann über den identifizierten Schutzbedarf bestimmt werden. Hierzu ist jedoch ein ebenso konkretes technisches Szenario notwendig. Dieser Teil des Rahmenwerks wird daher in Kapitel 12 separat evaluiert.

Anschließend wird das gesamte Geschäftsprozessmodul einer erneuten betriebswirtschaftlichen und GRC-seitigen Analyse unterzogen. Hierzu zählen Machbarkeitsplanungen, Kosten/Nutzen-Analysen, ggf. Prototyping sowie das Überprüfen auf durch die Ressourcen- und Maßnahmenauswahl neu erzeugten Gefährdungen und Risiken. Nach potenziell weiterer Anpassungserfordernisse wird schließlich das finale Modul beschlossen.

11.4.3 Geschäftsprozess-Implementierung

Sobald jeder Kooperationspartner über eine anforderungskonforme Definition der für sie geltenden Geschäftsprozessmodule verfügen, kann der Geschäftsprozess implementiert werden.

Die Implementierungsphase beinhaltet folgende Teilschritte:

1. Implementierung der organisatorischen Struktur
2. Implementierung der Personalzuordnung
3. Implementierung der IT-Ressourcen-Zuordnung
4. Implementierung der GRC-Maßnahmen
5. Aufbau von Geschäftsprozesskompetenz

Die Implementierung der organisatorischen, personal- und IT-seitigen Struktur entspricht dem Standardset an Aufgaben des klassischen Geschäftsprozessmanagements. Die Realisierung von GRC-Maßnahmen kommt ergänzend hierzu hinzu und ist somit nicht länger Aufgabe isolierter Überlegungen. In Folge dessen ist der gesamte Geschäftsprozess verändert worden, wodurch der Aufbau von Erfahrung bei der Erledigung der Aufgaben kein trivialer Prozess für die beteiligten Organisationen darstellt.

11.4.4 Geschäftsprozess-Monitoring

Sind sämtliche mit dem Geschäftsprozess in Verbindung stehenden Elemente implementiert, folgt der Betrieb. Dieser muss fortwährend überwacht werden, um zu prüfen, ob der umgesetzte Geschäftsprozess den Zielen entspricht.

Die Monitoring-Phase beinhaltet folgende Teilschritte:

1. Monitoring des Informationszugriffs
2. Geschäfts- und GRC-relevante Revision des Geschäftsprozesses
3. Performance-Messungen
4. Incident-Tracking
5. Kombiniertes Geschäfts- und GRC-Reporting

Es kann unterschieden werden in das Monitoring der Inhalte des Geschäftsprozesses und das Monitoring des Geschäftsprozesses selbst, das heißt der definierten Struktur wie sie während der Design-Phase festgesetzt wurde. Beide Bereiche können untergliedert werden in die Betrachtung betriebswirtschaftlich relevanter Anforderungen (Effektivität und Effizienz), das heißt klassische Geschäftsprozessmanagementaufgaben, und informationssicherheitsrelevante Anforderungen, welche bislang zwar in isolierten Rahmenwerken abgehandelt wurden, aber dennoch zum Standardset der dortigen Aufgaben gehören.

An dieser Stelle kann die Mess-Vorrichtung des generischen Rahmenwerks COBIT integriert werden, um den Grad der Zielerreichung von Prozessen zu ermitteln. Ein dedizierter Vorschlag für das inhaltliche Monitoring von Informationszugriffen in föderierten Ende-zu-Ende-Geschäftsprozessen wurde vom Autor in [EN13] erarbeitet. Es richtet sich an das Monitoring von Informationen über Cloud-Systeme als konkrete technische Unterstützungsform föderierter E2E-Prozesse.

11.4.5 Geschäftsprozess-Anpassung

Abhängig von Inhalt und Häufigkeit der durch das Monitoring erhobenen Missstände, aber auch bei der Änderung von Anforderungen, ist die Konfiguration des Geschäftsprozesses anzupassen.

Die Anpassungsphase beinhaltet folgende Teilschritte:

1. Positionsanalyse
2. Anpassung der Geschäftsprozessspezifika zur Sicherstellung der Compliance mit regulatorischen und informationssicherheitsseitigen Anforderungen
3. Änderungsmanagement (Konzeption, Planung, Realisierung, Monitoring)

Die Anpassung eines Geschäftsprozesses birgt in sich hohe Risiken. Das vorgeschlagene Verfahren integriert eine Vielzahl von betriebswirtschaftlichen, technischen und GRC-Faktoren. Eine Abänderung des Gesamtkonstrukts kann daher nur über ein geregeltes Änderungsmanagement erfolgen, welches jedoch ebenfalls zu den etablierten Verfahren zählt.

11.5 Zuordnung von Geschäftsprozessmodulen zu Kontrollen

In der Design-Phase müssen Kontrollen von den GRC-Anforderungen jeder kritischen Information eines jeden Geschäftsprozessmoduls abgeleitet werden. Da diese Beschreibung sehr generisch ist, soll schrittweise an einem konkreten Beispiel gezeigt werden, wie eine solche Zuordnung ausgehend von einem konkreten technischen Szenario aussehen kann.

Tabelle 11.1 zeigt zunächst weitreichend allgemeingültige Kontrollen und

ihre adressierten GRC-Anforderungen (Schutzziele[1]). Compliance-Aspekte werden eingeklammert dargestellt, da die Adressierbarkeit abhängig von einer konkreten regulatorischen Anforderung ist, welche hier nicht Betrachtungsgegenstand sein soll.

#	Kontrolle	C	I	A	Co
1	Authentifizierung und Autorisierung	X			(X)
2	Verschlüsselung übertragener und gespeicherter Daten	X	X		(X)
3	Zugriffsprotokollierung	X	X	X	(X)
4	Daten-Persistenz			X	(X)
5	Konfigurationsmanagement			X	(X)
6	Sammlung von System-Metriken			X	(X)
7	Absicherung von Anwendungs- und Netzwerk-Infrastruktur	X	X	X	(X)
8	Informationssicherheits-Audits	X	X	X	(X)

Tabelle 11.1: Zuordnung von Kontrollen und GRC-Anforderungen

Auf Basis dieser Kontrollen-Anforderungen-Zuordnung können die ersichtlichen Kontrollen nun an die zuvor erfassten Informationen angelegt werden. Den notwendigen Vergleichsschlüssel bietet die vorherige Gefährdungsanalyse der jeweiligen Information.

Konkret bedeutet dies: Aus den Tabellen 8.2 und 8.3 aus Kapitel 8.2 ergab sich eine Risiko-Erhebung für eine bestehende OTC-Instanziierung. Tabelle 11.2 verschmilzt nun die Perspektiven von OTC-Betreiber und OTC-Nutzer hinsichtlich Prozessschritten und Gefährdungen (reduziert auf das Haupt-Schutzziel, den Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit) und ergänzt die obige Kontroll-Nummer, welche durch beide Parteien (Betreiber und Nutzer des OTC) zu adressieren ist.

Diese Werte könnten durch zentralisierte Prozessbeschreibungen und teilautomatisierte Tools für das Konfigurationsmanagement (vgl. ehemaliges

[1] C = Confidentiality / Vertraulichkeit, I = Integrity / Integrität, A = Availability / Verfügbarkeit, Co = Compliance

#	Prozessschritt	Information	Schutzziel	Kontrollen (#)
1	RFQ austauschen	RFQ	**Vertraulichkeit**	1, 2, 3, 7, 8
2	Angebot austauschen	Angebot	**Vertraulichkeit**	1, 2, 3, 7, 8
3	Auftrag austauschen	Auftrag	**Vertraulichkeit**	1, 2, 3, 7, 8
4	Bestätigung austauschen	Auftragsbestätigung	Integrität	2, 3, 7, 8
5	Verfügbarkeit austauschen	Verfügbarkeitsnachricht	Integrität	2, 3, 7, 8
6	Lieferschein austauschen	Lieferschein	**Verfügbarkeit**	4, 5, 6, 7, 8
7	Rechnung austauschen	Rechnung	Integrität	2, 3, 7, 8
8	Zahlung austauschen	Zahlungsinformationen	Integrität	2, 3, 7, 8

Tabelle 11.2: Verschmolzene Risikoerhebung OTC-Betreiber und -Nutzer

GSTOOL des Bundesamtes für Sicherheit in der Informationstechnik, welches jedoch lediglich den BSI IT-Grundschutz abbildet), an alle an der Föderation beteiligten Partner propagiert werden. Dies ist jedoch nicht Betrachtungsgegenstand der vorliegenden Untersuchung. Es sei angemerkt, dass zur Herleitung allgemeiner Maßnahmen das zuvor beschriebene Unified Compliance Framework genutzt werden könnte. Hierüber können allgemeine Kontrollen abgeleitet werden, die den spezifischeren Vorgaben verteilter Rahmenwerke gerecht zu werden. Natürlich bilden allgemeine Kontrollen aber noch keine Grundlage für eine Operationalisierung, beispielsweise die Durchführung eines Einführungsprojektes, für die wiederum konkretere Maßnahmen vorgeschlagen werden müssen. Um konkret nachzuvollziehen, wie das konstruierte Rahmenwerk eingesetzt werden kann, evaluiert das nächste Kapitel das vorgeschlagene Verfahren am Beispiel einer konkreten technischen Instanziierung des OTC.

11.6 Zusammenfassung

Als Zwischenfazit zeigt Tabelle 11.3 die bis dato adressierten Anforderungen nach Konstruktion der GRC-Prozesse.

#	Adressiert?	Kommentar
A1	Ja	Einbeziehung betriebswirtschaftlicher Entscheidungsfaktoren
A2	Ja	Einbeziehung von Schutzbedarfen, Gefährdungen und Risikobetrachtungen
A3	Ja	Einbeziehung von Entscheidungsgrundlagen für IT-Konfiguration
A4	Ja	Modell zur Ableitung von konkreten Maßnahmen über allgemeine GRC-Kontrollen
A5	Nein	Noch unbetrachtet, in Evaluation erläutert
A6	Nein	Noch unbetrachtet, in Evaluation erläutert
A7	Ja	Verflochtene Integration von A1, A2 und A3 entlang eines GRC-Prozessrahmens entlang des Geschäftsprozess-Lebenszyklus
A8	Ja	GRC-Phasen bauen auf PDCA-Zyklus auf
A9	Nein	Noch unbetrachtet, in Ausblick erläutert

Tabelle 11.3: Adressierte Anforderungen nach GRC-Prozessen

Unter den Prämissen der Einnahme der Perspektive des Geschäftsprozesses, der Trennung von Geschäftsprozessen und GRC-Prozessen sowie der Integration der Geschäfts-, IT- und GRC-Ebenen wurde ein neues Rahmenwerk zum GRC-optimierten Management von Geschäftsprozessen konstruiert. Es fußt auf den Sichten der Ressourcen, der GRC-Funktionen, GRC-Daten, GRC-Prozessen, der Geschäftsfunktionen, Geschäftsdaten, Geschäftsprozessmodule sowie der resultierenden Services und Produkte und wird somit der zuvor definierten Anforderungen gerecht.

Das Rahmenwerk sieht die GRC-Prozess-Phasen der Analyse, des Designs, der Implementierung, des Monitorings und der Anpassung von Ge-

schäftsprozessen vor. Insbesondere in der Analyse- und der Design-Phase wird die Integration der Geschäfts-, GRC- und der technischen Anforderungen deutlich.

Während die Analyse-Phase sowohl betriebswirtschaftliche, technische als auch anforderungsseite Erfordernisse und Gegebenheiten erfasst, sind Kernpunkte der Design-Phase einerseits die Aufteilung des Geschäftsprozesses in Module, welche über die an der Föderation beteiligten Organisationen verteilt werden. Andererseits findet ein Abgleich der durch die beteiligten Partner ermittelten Schutzbedarfe geschäftskritischer Informationen nach dem Maximalprinzip statt.

Eine innerhalb der Design-Phase ansetzende Risiko-Analyse gibt anschließend Aufschluss über die Notwendigkeit zur Adressierung der von anderen Partnern als kritisch erachteten Informationen, und damit der darunterliegenden IT-Systeme, welche vorliegend bereits vor ihrer Zuweisung zum Geschäftsprozess (um)geplant werden können. Kritische Systeme wie Cloud-Services können so bereits vor dem Betrieb des Geschäftsprozesses von der Nutzung ausgeschlossen werden. Dies unterstreicht die Möglichkeit der Behandlung von Ursachen anstatt Symptomen.

Unberührt davon müssen Maßnahmen hergeleitet und umgesetzt werden können. Hierzu beschreibt das Kapitel die Zuordnung von Geschäftsprozessmodulen zu zunächst allgemeinen Kontrollen auf Basis der Gefährdungen, reduziert auf die Hauptschutzziele, beispielsweise dem Verlust von Vertraulichkeit bei der Angebotsabwicklung im OTC. Für den Erhalt konkreter technischer und/oder organisatorischer Maßnahmen wird verwiesen auf das Kapitel der Evaluation, in dem zunächst ein konkretes technisches Szenario definiert, und anschließend mit dem hier entwickelten Rahmenwerk behandelt wird.

12 Evaluierung

Auf Basis der Problemstellung aus Teil III sowie der Herleitung eines neuen Verfahrens innerhalb der Kapitel 10 und 11 werden in diesem Kapitel die Untersuchungsergebnisse an einem konkreten Anwendungsbeispiel des OTC evaluiert. Es findet eine Einschränkung des Geltungsbereichs, eine Erläuterung der Erschwernisse bei der Evaluierung, die Vorstellung des Evaluierungsszenarios, ein Nachweis zur Maßnahmenerhebung in diesem Szenario sowie ergänzend eine Akzeptanzprüfung des Rahmenwerks statt.

12.1 Geltungsbereich und Evaluationsziele

Das entwickelte Rahmenwerk adressiert sowohl föderierte als auch nicht föderierte Szenarien. Die Zerlegung eines Geschäftsprozesses in Module und das Maximalprinzip der Schutzbedarfe sind nicht als verpflichtende Schritte zu verstehen. Vorliegend soll zunächst ein Nachweis zur Effektivität des entwickelten Rahmenwerks zu nicht föderierten Geschäftsprozessen geführt werden, um die Deckungsgleichheit der Ergebnisse traditioneller Verfahren zu demonstrieren. Im Anschluss soll gezeigt werden, dass auch föderierte Geschäftsprozesse behandelt werden können:

Evaluationsziel 1: nicht-föderierte Szenarien lassen sich mit neuem Rahmenwerk behandeln

Evaluationsziel 2: föderierte Szenarien lassen sich mit neuem Rahmenwerk behandeln

Für eine möglichst breite Anwendbarkeit des entwickelten Rahmenwerks wurde in Kapitel 8 der Order-to-Cash Geschäftsprozess aus zwei Gründen als Referenzobjekt ausgewählt: aufgrund seiner Komplexität sowie seiner Verbreitung. Innerhalb dieser OTC-Referenz soll eine Evaluation stattfinden, welche als erfolgreich angesehen wird, wenn man mit dem vorgeschlagenen Modell in der Lage ist, konkrete Maßnahmen vorzuschlagen, welche in Bezug zu den Schutzbedarfen des Ausgangsszenarios stehen.

Es lässt sich jedoch kein allgemeingültiges Maßnahmenpaket für jede OTC-Instanz aussprechen, da organisatorische und technische Maßnahmen stets in Abhängigkeit von eingesetzten Technologien stehen, vgl. Kapitel 5. Daher wird in diesem Kapitel eine konkrete technische Instanziierung des OTC vorgenommen, welcher später erläutert wird. Innerhalb dieses noch enger spezifizierten Problemraums wird ein konkreter Nachweis zum Erhalt von Maßnahmen erbracht.

12.2 Erschwernisse

Die folgenden Faktoren erschweren die vorliegende Evaluation:

1. Erschwernis: Methodiken lassen sich schwer evaluieren, da passende Vergleichsobjekte fehlen, und wird das bereits behandelte Objekt als Referenzobjekt für eine erneute Evaluation verwendet, entsteht Spielraum für mögliche Fehlinterpretationen

2. Erschwernis: Im Bereich der Informationssicherheit ist es unmöglich festzustellen, welche Incidents (Sicherheitsvorfälle) verhindert wurden, da sie nicht eingetreten sind

3. Erschwernis: Unternehmenskritische Daten zur Reproduktion realer Abläufe und Nutzung realer Informationen werden von Unternehmen nicht oder nur unzureichend tiefgreifend herausgegeben

4. Erschwernis: Befragungen zu Rahmenwerken liefern lediglich Informationen bezüglich der Akzeptanz, nicht jedoch Informationen zur Effektivität eines Rahmenwerks

Aus den vorbezeichneten Erschwernisfaktoren ergibt sich die Notwendigkeit der argumentativen Evaluierung am Beispiel. Nachfolgend erläutert werden das konkrete Szenario, das Verfahren zur Maßnahmenerhebung und schließlich eine Akzeptanzprüfung des Rahmenwerks.

12.3 Konkretes OTC-Evaluierungsszenario

Um den Erhalt von Maßnahmen mit dem vorgeschlagenen Rahmenwerk, insbesondere auf Basis der vorherigen Matrix (vgl. Tabelle 11.1) zu demonstrieren, und damit insbesondere die Grundlage für eine Evaluierung zu bilden, wird nun ein dediziertes technisches OTC-Szenario isoliert. Aufgrund der wachsenden Verbreitung mobiler Unterstützung von Geschäftsprozessen bei gleichzeitig hoch kritischer Eigenschaften mobiler Endgeräte [ea11] soll sich dieses Szenario auf die parzielle OTC-Unterstützung durch mobile Anwendungen konzentrieren.

Für diesen Kontext wurde ein eigener Maßnahmenkatalog entwickelt. Um sich diesem anzunähern, zeigt Abbildung 12.1 zunächst die technische Architektur einer möglichen Mobil-Landschaft realisiert durch SAP UI5 [AG14].

Anhang A zeigt eine Gegenüberstellung der für die vorbezeichnete Architektur identifizierten, möglichen konkreten Maßnahmen mit Referenzierung der abstammenden allgemeinen Kontrolle (vgl. Tabelle 11.1) und des durch die Maßnahme abgedeckten Schutzbedarfs. Zur Übersichtlichkeit gilt stets, dass Maßnahmen, die einen höheren Schutzbedarf adressieren, zusätzlich zu den darunter eingeordneten Maßnahmen umzusetzen sind.

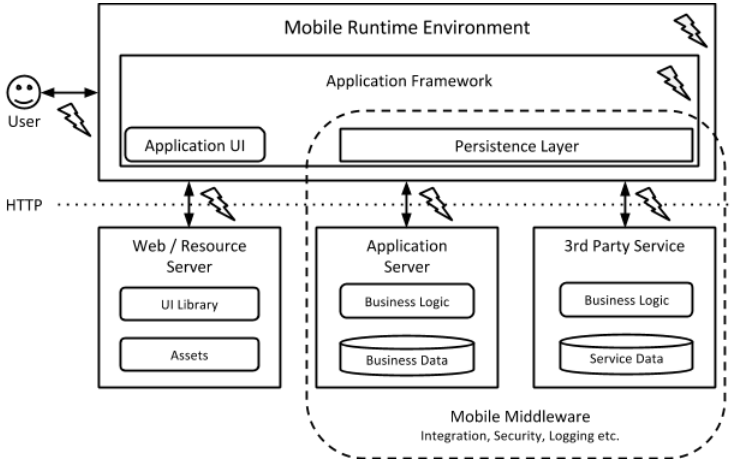

Abbildung 12.1: SAP-UI5-Architektur [AG14]

Die Tabellen 12.1 und 12.2 zeigen die vorliegend angenommene Ressourcenunterstützung eines (mobil unterstützen) OTC, die mit dem vorbezeichneten Maßnahmenkatalog effizient zu behandeln ist.

#	**Prozessschritt**	**IT-System**
1	RFQ entgegennehmen	SAP ERP, mobile Interface
2	Angebot senden	SAP ERP
3	Auftrag entgegennehmen	SAP ERP, mobile Interface
4	Bestätigung senden	SAP ERP
5	Verfügbarkeit senden	SAP ERP
6	Lieferschein senden	SAP ERP
7	Rechnung senden	SAP ERP
8	Zahlung entgegennehmen	SAP ERP, mobile Interface

Tabelle 12.1: Ressourcenunterstützung eines OTC aus Betreibersicht

Wie ersichtlich wird, sollen stets die eine kritische Information entgegen-

nehmenden Prozessschritte mobil unterstützt sein. Zur Vereinfachung gilt dies für beide Seiten der (hier zweiseitigen) Föderierung.

#	Prozessschritt	IT-System
1	RFQ senden	openERP
2	Angebot entgegennehmen	openERP, mobile Interface
3	Auftrag senden	openERP
4	Bestätigung entgegennehmen	openERP, mobile Interface
5	Verfügbarkeit entgegennehmen	openERP, mobile Interface
6	Lieferschein entgegennehmen	openERP, mobile Interface
7	Rechnung entgegennehmen	openERP, mobile Interface
8	Zahlung senden	openERP

Tabelle 12.2: Ressourcenunterstützung eines OTC aus Nutzersicht

Mit diesem Szenario werden nun die zwei eingangs beschriebenen Evaluationsziele verfolgt.

12.4 Evaluation 1: Adressierung nicht-föderierter Szenarien

Zunächst muss das entwickelte Rahmenwerk in der Lage sein, klassische (nicht-föderierte) Szenarien zu behandeln. Das neue Rahmenwerk muss daher auf den im Geltungsbereich befindlichen Betrachtungsgegenstand, den OTC, angewendet werden. Als Referenz für die Feststellung einer erfolgreichen Behandlung dient hierbei die angewandte Methodik der ISO 27001 und ihrer Liefergegenstände in Bezug auf den OTC aus Kapitel 8.2.

Ausgehend vom Blickwinkel des OTC-Betreibers muss das entwickelte Rahmenwerk analog zur traditionellen Herangehensweise in der Lage sein, Schutzbedarfe zu identifizieren sowie Maßnahmenvorschläge zu unterbreiten. Die durchgeführten Schritte können abweichen, die Ergebnisse müssen identisch sein.

Führt man die Analyse-Phase des entworfenen Rahmenwerks durch, erhält man zunächst eine Bewertung der Schutzbedarfe. Verwendet man anschließend die bereits gezeigte Kontrollen-Anforderungszuordnung (vgl. Tabelle 11.1), lassen sich zunächst allgemeine Kontrollen (vgl. Tabelle 11.2, reduziert auf die Gefährdungen des Betreibers), und im Anschluss spezifische Maßnahmen ableiten.

Das Ergebnis der konkreten Maßnahmen für das zu evaluierende Szenario ist in Tabelle 12.3 dargestellt.

#	Prozessschritt	Schutz-bedarf	Maßnahmen gemäß Anhang A
1	RFQ entgegennehmen	**Normal**	1.1, 1.4, 2.1.1, 2.2.1, 2.3.1, 2.3.2, 2.3.3, 2.4.1, 3.1.1, 3.2.1, 3.3.2
2	Angebot senden	**Hoch**	1.3, 1.5, 1.6, 2.1.3, 2.2.2, 2.4.2, 3.1.2, 3.2.2, 3.2.3, 3.2.4, 3.3.3
3	Auftrag erhalten	**Normal**	1.1, 1.4, 2.1.1, 2.2.1, 2.3.1, 2.3.2, 2.3.3, 2.4.1, 3.1.1, 3.2.1, 3.3.2
4	Bestätigung senden	Normal	1.1, 1.4, 2.1.1, 2.2.1, 2.3.1, 2.3.2, 2.3.3, 2.4.1, 3.1.1, 3.2.1, 3.3.2
5	Verfügbarkeit senden	Normal	1.1, 1.4, 2.1.1, 2.2.1, 2.3.1, 2.3.2, 2.3.3, 2.4.1, 3.1.1, 3.2.1, 3.3.2
6	Lieferschein senden	**Normal**	1.1, 1.4, 2.1.1, 2.2.1, 2.3.1, 2.3.2, 2.3.3, 2.4.1, 3.1.1, 3.2.1, 3.3.2
7	Rechnung senden	Hoch	1.3, 1.5, 1.6, 2.1.3, 2.2.2, 2.4.2, 3.1.2, 3.2.2, 3.2.3, 3.2.4, 3.3.3
8	Zahlung entgegennehmen	Sehr hoch	2.1.2, 2.2.3, 2.4.3, 3.1.3, 3.3.1

Tabelle 12.3: Maßnahmen-Festsetzung für OTC-Betreiber

Vergleicht man diese Aufstellung, wird zunächst deutlich, dass eine Bewertung der Schutzbedarfe identisch zur traditionellen Erfassung mittels ISO 27001 ist, vgl. Tabelle 8.2 aus Kapitel 8.2 (erhobene Risiken eines OTC aus reiner Betreiberperspektive). Ferner ist demonstriert, dass sich mit dem vorgeschlagenen Rahmenwerk konkrete Maßnahmen für das beschriebene

Szenario ableiten lassen. Somit sind nicht-föderierte Fälle durch das Rahmenwerk zunächst effektiv adressierbar.

12.5 Evaluation 2: Adressierung föderierter Szenarien

Nun wird die Analyse-Phase des entwickelten Rahmenwerks bei einem föderierten Szenario durchgeführt, das heißt sowohl die Betreiber- als auch die Nutzer-Perspektive des OTC berücksichtigt.

Tabelle 12.4 verschmilzt erneut die Perspektiven von OTC-Betreiber und OTC-Nutzer, hier hinsichtlich Prozessschritten und Schutzbedarfen, sowie abschließend ergänzt um die konkreten (Extra-)Maßnahmen gemäß Anhang A, welche im zu evaluierenden Föderierungsszenario durch beide Parteien (Betreiber und Nutzer des OTC) zu adressieren sind.

Die ersichtlichen Maßnahmen können nun an den (hier „mobilen“) IT-Systemen aus den Tabellen 12.1 und 12.2 realisiert und mit der beschriebenen Methodik entlang des Lebenszyklus des Geschäftsprozesses verwaltet werden.

Entsprechend konnte gezeigt werden, dass, im Gegensatz zu traditionellen Herangehensweisen, föderierte Fälle adressiert, d.h. Schutzbedarfe für mehrere Seiten erfasst und konkrete Maßnahmen abgeleitet werden können.

Die beschriebene Methodik erlaubt auch mehrschichtigere Föderierungen, beispielsweise Kunden-Lieferanten-Lieferantenbeziehungen. Hier gilt, dass ein weiterer Partner stets als „Nutzer“ des Geschäftsprozesses des nachfolgenden zu betrachten ist. Ein hoher Schutzbedarf an einer Stelle wird sich entsprechend durch die Lieferantenschichten „vererben“.

#	Prozessschritt	Schutzbedarf	Maßnahmen gemäß Anhang A
1	RFQ austauschen	**Hoch**	1.3, 1.5, 1.6, 2.1.3, 2.2.2, 2.4.2, 3.1.2, 3.2.2, 3.2.3, 3.2.4, 3.3.3
2	Angebot austauschen	**Hoch**	1.3, 1.5, 1.6, 2.1.3, 2.2.2, 2.4.2, 3.1.2, 3.2.2, 3.2.3, 3.2.4, 3.3.3
3	Auftrag austauschen	**Sehr hoch**	2.1.2, 2.2.3, 2.4.3, 3.1.3, 3.3.1
4	Bestätigung austauschen	Normal	1.1, 1.4, 2.1.1, 2.2.1, 2.3.1, 2.3.2, 2.3.3, 2.4.1, 3.1.1, 3.2.1, 3.3.2
5	Verfügbarkeit austauschen	Normal	1.1, 1.4, 2.1.1, 2.2.1, 2.3.1, 2.3.2, 2.3.3, 2.4.1, 3.1.1, 3.2.1, 3.3.2
6	Lieferschein austauschen	**Hoch**	1.3, 1.5, 1.6, 2.1.3, 2.2.2, 2.4.2, 3.1.2, 3.2.2, 3.2.3, 3.2.4, 3.3.3
7	Rechnung austauschen	Hoch	1.3, 1.5, 1.6, 2.1.3, 2.2.2, 2.4.2, 3.1.2, 3.2.2, 3.2.3, 3.2.4, 3.3.3
8	Zahlung austauschen	Sehr hoch	2.1.2, 2.2.3, 2.4.3, 3.1.3, 3.3.1

Tabelle 12.4: Vereinheitlichte Maßnahmen-Festsetzung für OTC-Betreiber und OTC-Nutzer

12.6 Akzeptanzprüfung

Abschließend soll die Akzeptanz des neu entwickelten Rahmenwerks überprüft werden. Hierzu sind in der Literatur verschiedene Methoden zu finden.

12.6.1 Auswahl eines Prüfverfahrens

Tabelle 12.5 stellt fünf Möglichkeiten zur Akzeptanzmodellierung gemäß [Gmb07] und deren Eignung für die vorliegende Evaluierung gegenüber.

Aufgrund anderweitiger Zielbezüge sind die meisten Modelle vorliegend wenig relevant, setzen teilweise auch ein konkret implementiertes System

	Einflussfaktoren	Zusammenfassung	Eignung
Technology Acceptance Model (TAM) [Dav85]	Wahrgenommener Nutzen, wahrgenommene einfache Anwendbarkeit	Abwägung des Aufwand/Nutzen-Verhältnisses zur Akzeptanzentscheidung.	Hoch
Technology Task Fit Model (TTFM) [GT05]	Technologie, Aufgabe, Menschen	Aufgabenorientierter Ansatz, der die Elemente der Wirtschaftsinformatik berücksichtigt.	Hoch
Degenhardt, 1986 [Deg86]	Aufgaben, System, Anwendermerkmale	Betrachtung der Akzeptanz von Kommunikationsdiensten am Beispiel Bildschirmtext.	Gering
Kollmann, 2000 [Kol00]	Einstellungsakzeptanz, Verhaltensakzeptanz, Nutzungsakzeptanz	Betrachtung der Einführung von Telekommunikations- und Multimediasystemen.	Gering
Herrmann, 1999 [Her99]	Umfassender Kriterienkatalog	Betrachtung der Akzeptanz von Mediendiensten anhand der Kompetenz der Benutzer.	Gering

Tabelle 12.5: Methoden zur Akzeptanzmodellierung [Gmb07], modifiziert

voraus, um effektive Evaluierungsergebnisse zu erzielen. Das TTFM besitzt zwar zur Wirtschaftsinformatik direkt passende Einflussfaktoren, die Faktoren „Individuum“ und „Aufgabe“ werden jedoch nicht miteinander in Verbindung gesetzt, da die Analyse der Verhaltensakzeptanz kein Zielgegenstand des Modells ist [Buc06]. Das TAM fasst den Begriff Technology sehr weit und ist zudem aufgrund seiner Ausrichtung, der Erfassung des Aufwand/Nutzen-Verhältnisses zwar ein pragmatisches, aber auch ein universell einsetzbares Evaluationsinstrument zur Akzeptanzmodellierung. Es soll daher vorliegend Verwendung finden.

Abbildung 12.2 visualisiert das TAM und die Zusammenhänge zwischen Einflussfaktoren und Nutzungswahrscheinlichkeit eines Systems.

Für das vorliegende Modell sollen die „Notwendigkeit zur Adressierung von informationssicherheitsrelevanten Anforderungen“ sowie die „Entscheidungskompetenz innerhalb der Organisation“ als externe Einflussfaktoren genutzt werden. Dies wird dadurch erforderlich, dass die Akzeptanz eines

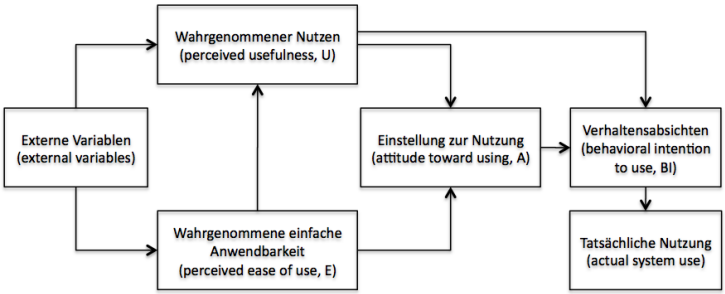

Abbildung 12.2: Technology Acceptance Model [Dav85], modifiziert

jeden Rahmenwerks in direkter Abhängigkeit der organisatorisch zugewiesenen Rolle steht. Diese muss sowohl Notwendigkeit als auch entsprechende Handlungsfreiheit in der Organisation berücksichtigen. Die Notwendigkeit zur Nutzung ist dabei dem Hauptkriterium „Wahrgenommener Nutzen“, die individuelle Handlungsfreiheit dem Hauptkriterium „Wahrgenommene einfache Anwendbarkeit“ zuordenbar.

12.6.2 Vorbereitung der Befragung

Eingangs der Befragung wird die Funktion der befragten Person im Betrieb erfasst. Dies gibt Aufschluss über die Befugnisse der befragten Person im Betrieb, was für wahrgenommenen Nutzen und Anwendbarkeit von entscheidender Bedeutung sein kann.

Es leiten sich folgende Fragen für das Kriterium „Wahrgenommener Nutzen“ ab:

1. Welche allgemeinen Vorteile sehen Sie hinsichtlich des Nutzens des vorliegenden Rahmenwerks in EINEM Betrieb?
2. Welche allgemeinen Nachteile sehen Sie hinsichtlich des Nutzens des vorliegenden Rahmenwerks in EINEM Betrieb?

3. Erachten Sie die Notwendigkeit der Adressierung von informationssicherheitstechnischen und/oder regulatorischen Anforderungen als direkten oder indirekten Bestandteil Ihrer Tätigkeit?
4. Falls ja: welche allgemeinen Vorteile sehen Sie hinsichtlich des Nutzens des vorliegenden Rahmenwerks in IHREM konkreten Betrieb?
5. Falls ja: welche allgemeinen Nachteile sehen Sie hinsichtlich des Nutzens des vorliegenden Rahmenwerks in IHREM konkreten Betrieb?
6. Leistet das vorliegende Modell aus Ihrer Sicht einen positiven/negativen Beitrag zur Adressierung von GRC-Anforderungen in EINEM Betrieb im Allgemeinen? Wenn ja, welchen? Wenn nein, bitte erläutern.
7. Leistet das vorliegende Modell aus Ihrer Sicht einen positiven/negativen Beitrag zur Adressierung von GRC-Anforderungen in IHREM konkreten Betrieb im Allgemeinen? Wenn ja, welchen? Wenn nein, bitte erläutern.

Es leiten sich folgende Fragen für das Kriterium „Wahrgenommene einfache Anwendbarkeit“ ab:

1. Welche allgemeinen Vorteile sehen Sie hinsichtlich der Anwendbarkeit des vorliegenden Rahmenwerks in EINEM Betrieb?
2. Welche allgemeinen Nachteile sehen Sie hinsichtlich der Anwendbarkeit des vorliegenden Rahmenwerks in EINEM Betrieb? (bitte unter „Weitere“ erläutern)
3. Beschreiben Sie kurz die Entscheidungskompetenz die ein Nutzer des vorliegenden Rahmenwerks aus Ihrer Sicht in einem Betrieb benötigt!
4. Verfügen Sie über die entsprechende Entscheidungskompetenz in Ihrem Betrieb?
5. Falls ja: Welche allgemeinen Vorteile sehen Sie hinsichtlich der Anwendbarkeit des vorliegenden Rahmenwerks in IHREM konkreten Betrieb (ggf. auch direkt durch Sie)?
6. Falls ja: Welche allgemeinen Nachteile sehen Sie hinsichtlich der An-

wendbarkeit des vorliegenden Rahmenwerks in IHREM konkreten Betrieb (ggf. auch direkt durch Sie)?

7. Planen Sie, auf Basis Ihrer bisherigen Überlegungen, das Rahmenwerk in Ihrem Betrieb einzusetzen, einsetzen zu lassen oder den Einsatz zu empfehlen? Falls ja und falls nein: würden Sie Anpassungen vornehmen (müssen), falls ja welche?

Ein „Platz für weitere Hinweise“ rundet die Akzeptanzbefragung ab. Hinsichtlich der Teilnehmer der Befragung wurde jeweils eine Person aus dem Bereich des GRC-Managements, der GRC-Beratung und der Geschäftsführung herangezogen.

12.6.3 Durchführung der Befragung

Der Fragebogen wurde als Online-Fragebogen konzipiert und war vom 11. März bis 19. Mai online geschaltet. In dieser Zeit wurden gezielt Personen auf die Umfrage aufmerksam gemacht, welche Stakeholder gemäß Abschnitt 10.1 des GRC-Managements sind und somit sowohl Nutzen als auch Anwendbarkeit des Rahmenwerks einschätzen können. Zusätzlich dazu wurde der Fragebogen der breiten Öffentlichkeit zugänglich gemacht. Der Fragebogen wurde 560 mal ohne jegliche Beantwortung aufgerufen. Aufgrund der speziellen Thematik entspricht dies der Erwartung.

Der Fragebogen wurde insgesamt 12 mal vollständig beantwortet. Acht Beantwortungen gingen mit einer Beantwortungszeit von weniger als 17 Sekunden und diversen Werbelinks ein und wurden ausgesondert. Hierbei handelte es sich um Spamroboter. Die verbleibenden vier Antworten wurden intensiv geprüft. Eine der Beantwortungen enthielt keinerlei inhaltliche Substanz, wurde stets mit „Nein“ und scherzhaft gemeinten Antworten unter „Weiteres“ versehen. Auch diese Beantwortung wurde ausgesondert. Die übrigen drei Beantwortungen entstammten dem GRC-Management, der GRC-Beratung und der Geschäftsführung. Diese wurden verwertet.

12.6.4 Auswertung

Das GRC-Management sieht in sowohl einem als auch dem eigenen Betrieb eine Steigerung der Transparenz, einen Verlust an Einfachheit, d.h. eine Steigerung der Komplexität, eine unveränderte Anzahl von Incidents sowie eine unveränderte Adressierbarkeit von Incidents. Begründet wurden die negativen Punkte einerseits damit, dass ein erhöhter Geschäftsführungs-Aufwand im eigenen Betrieb als gesteigerte Bürokratie wahrgenommen und damit die Vorteile aufheben würde. Zudem sah man sich andererseits nicht mit den Entscheidungskompetenzen ausgestattet, die notwendig sind, um die erforderlichen Einschnitte in den Geschäftsprozessen vorzunehmen.

GRC-Beratung und Geschäftsführung sehen ebenfalls eine Steigerung der Transparenz sowie zusätzlich auch eine Steigerung der Effektivität in einem und ihrem Betrieb. Gleichzeitig wird ein Verlust von Effizienz und ein Verlust an Einfachheit, d.h. auch hier eine Steigerung der Komplexität erwartet. Beides gilt sowohl für einen als auch für ihren eigenen Betrieb. In einem Betrieb im Allgemeinen wird aufgrund der steigenden Transparenz von mehr erfassten GRC-relevanten Incidents ausgegangen. Weiterhin wird davon ausgegangen, dass sich GRC-Anforderungen besser adressieren lassen. Letzteres gilt ebenfalls für den eigenen Betrieb. Man erwartet eine Vereinfachung der Aufgaben des Compliance-Managers, des Informationssicherheitsbeauftragten und des IT-Managers. Es wird jedoch auch eine erschwerte Arbeit der Geschäftsführung angenommen.

Alle drei Anwortenden geben als notwendige Entscheidungskompetenz an, dass sowohl die Gestaltung von Geschäftsprozessen, als auch Richtlinien-Erstellung mitsamt der Autorität zu deren Durchsetzbarkeit gegeben sein muss. Lediglich die Geschäftsführung gibt an, über diese Kompetenz zu verfügen. Die GRC-Beratung merkt zudem an, dass, auch wenn eine Person allein über diese Kompetenz verfüge, noch immer ein Management-System für das Monitoring notwendig sei. Die Geschäftsführung sieht als Problem

lediglich die operative Einbeziehung in den Betrieb, die nicht immer garantiert werden kann.

Geschäftsführung und Beratung geben an, dass sie die Anwendbarkeit in ihrem Betrieb sehen und „vielleicht“ planen, die Beratung merkt zudem an, dass hierzu zu politischen Zwecken eine internationale Norm aus dem Rahmenwerk entstehen sollte, um eine Zertifizierung als Nachweis führen zu können.

12.7 Zusammenfassung

Tabelle 12.6 zeigt die durch Entwicklung des Rahmenwerks sowie der durchgeführten Evaluation adressierten Anforderungen.

#	Adressiert?	Kommentar
A1	Ja	Einbeziehung betriebswirtschaftlicher Entscheidungsfaktoren
A2	Ja	Einbeziehung von Schutzbedarfen, Gefährdungen und Risikobetrachtungen
A3	Ja	Einbeziehung von Entscheidungsgrundlagen für IT-Konfiguration
A4	Ja	Modell zur Ableitung von konkreten Maßnahmen über allgemeine GRC-Kontrollen
A5	Ja	Evaluation siehe aktuelles Kapitel
A6	Ja	Evaluation siehe aktuelles Kapitel
A7	Ja	Verflochtene Integration von A1, A2 und A3 entlang eines GRC-Prozessrahmens entlang des Geschäftsprozess-Lebenszyklus
A8	Ja	GRC-Phasen bauen auf PDCA-Zyklus auf
A9	Nein	Noch unbetrachtet, in Ausblick erläutert

Tabelle 12.6: Adressierte Anforderungen nach Evaluation

Das vorliegende Modell wurde für den Geltungsbereich föderierter und nicht-föderierter Szenarien konzipiert und evaluiert. Aufgrund verschiede-

ner Erschwernisfaktoren wurde eine Evaluierung an einem konkreten technischen Szenario mit anschließender Akzeptanzprüfung durchgeführt.

Das Szenario besteht aus einer OTC-Instanziierung mittels mobiler Unterstützung auf belegempfangender Seite. Für sowohl den nicht-föderierten als auch den föderierten Fall konnten der Erhalt von Schutzbedarfen für kritische Geschäftsinformationen und die Herleitbarkeit von konkreten technischen Maßnahmen demonstriert werden.

Zur Prüfung der Akzeptanz des Rahmenwerks wurde das Technology Acceptance Model (TAM) aufgrund seiner universellen Einsetzbarkeit ausgewählt, ein Fragebogen entwickelt und drei Zielpersonen unterschiedlicher betrieblicher Positionen befragt. Das Ergebnis der Befragung ist eine hinsichtlich Effektivität und Transparenz positive, hinsichtlich Effizienz bei der Geschäftsführung negative Einschätzung.

13 Fazit

Dieses Kapitel fasst die Untersuchungsergebnisse dieser Dissertation zusammen und liefert einen Ausblick für weitere Forschungsvorhaben.

13.1 Ausblick

Weitere Arbeiten können zunächst Augenmerk auf die Erarbeitung eines Leitfadens zur Operationalisierung der vorgeschlagenen Methodik legen. Hier könnten mehrere Handbücher entstehen, welche den verschiedenen Stakeholdern als Leitlinie dienen können. Ein übergreifendes Handbuch, welches die übrigen in Relation zueinander setzt, wäre hierbei empfehlenswert, um die Aufgabenverteilung auf Ebene der Geschäftsleitung(en) verständlich zu machen.

Höherwertigere Arbeit kann in einer weiterführenden Evaluation gegen andere Föderierungsfälle dienen. Vorliegend wurde der komplexe und verbreitete OTC ausgewählt, die These, dass hierdurch auch andere Geschäftsprozesse, insbesondere in föderierter Form adressiert werden können, verdient nähere Untersuchung. Gleiches gilt für die Evaluierung gegen weitere technische Instanziierungen der jeweiligen Geschäftsprozesse. Auch der OTC selbst kann noch in anderen technischen Realisierungsformen als der mobilen Unterstützung evaluiert werden.

Ferner ließe sich die Integraton in Landschaften, welche bereits andere Rahmenwerke einsetzen, untersuchen. Hierbei sind Hinweise auf Praktikabili-

tät und Best Practices zur Integration und Abgrenzung der Aufgaben der GRC-Prozesse in Relation zu den jeweiligen Rahmenwerken zu erwarten.

Schließlich wäre es sinnvoll, das vorgeschlagene Modell, möglicherweise in weiter optimierter Form, als Standard zu etablieren. Hierzu sind insbesondere viele formale Herausforderungen zu erwarten. Für eine Zertifizierbarkeit des vorgeschlagenen Modells wäre dieser Schritt jedoch unabdingbar. Hierfür wäre zudem zu kären, inweit sich Föderierungen im Allgemeinen, und der Einsatz des Modells im Speziellen realisieren lassen.

13.2 Zusammenfassung

Es wurde eine Methodik zur Unterstützung der Etablierung und Aufrechterhaltung von Informationssicherheit für föderierte Geschäftsprozesslandschaften entwickelt und evaluiert. Vorhandene relevante Rahmenwerke wurden analysiert und dienten als Grundlage zur Erweiterung. Es wurde versucht, die organisatorischen Grenzen traditioneller Ansätze zu entfernen, indem ein neues Rahmenwerk entwickelt wurde, welches die Geschäftsprozesse und die darin transportierten Informationen vor den mit den Aufgaben in Verbindung stehenden Ressourcen zentralisiert und somit zur Ursachenbehandlung von Sicherheitsvorfällen beiträgt. Tabelle 13.1 zeigt die nach Durchführung der Untersuchung adressierten Anforderungen.

Geschäftsprozesse werden durch verschiedene Ressourcen unterstützt und unterliegen zeitgleich verschiedenen sicherheitstechnischen und regulatorischen Anforderungen. Diesen Anforderungen wird traditionell mit verschiedenen Rahmenwerken begegnet, welche der jeweiligen Organisation helfen, zu bestimmten Maßnahmen zu gelangen, um die jeweiligen Anforderungen nachhaltig zu adressieren. Bereits im Rahmen isolierter Organisationen behandeln diese klassischen Rahmenwerke die Symptome mangelhaften Geschäftsprozessdesigns. Ohne offene Grenzen bieten die resultierenden Maßnahmen einen gewissen Schutz vor verschiedenen Gefährdun-

#	Adressiert?	Kommentar
A1	Ja	Einbeziehung betriebswirtschaftlicher Entscheidungsfaktoren
A2	Ja	Einbeziehung von Schutzbedarfen, Gefährdungen und Risikobetrachtungen
A3	Ja	Einbeziehung von Entscheidungsgrundlagen für IT-Konfiguration
A4	Ja	Modell zur Ableitung von konkreten Maßnahmen über allgemeine GRC-Kontrollen
A5	Ja	Evaluation auf Basis eines mobil unterstützten Order-to-Cash Geschäftsprozesses aus Betreiberperspektive
A6	Ja	Evaluation auf Basis eines mobil unterstützten Order-to-Cash Geschäftsprozesses aus Betreiber- und Nutzerperspektive
A7	Ja	Verflochtene Integration von A1, A2 und A3 entlang eines GRC-Prozessrahmens entlang des Geschäftsprozess-Lebenszyklus
A8	Ja	GRC-Phasen bauen auf PDCA-Zyklus auf
A9	(Ja)	Benötigt reale Anwendung des Rahmenwerks und separate Untersuchung

Tabelle 13.1: Adressierte Anforderungen

gen in Abhängigkeit des in der Organisation identifizierten Schutzbedarfs und des individuellen Risikos.

Betrachtet man jedoch Föderierungen, beispielsweise Unternehmenskooperationen oder langfristige Kunden-Lieferanten-Beziehungen, so stellte sich die Frage nach dem Element, welches als Referenz für den Erhalt eines einheitlichen, d.h. organisationsübergreifenden, Verständnisses des Schutzbedarfs führen kann. Hier manifestierte sich die Kritikalität der zu einem bestimmten Arbeitsschritt gehörenden, transportierten Informationen. Der Schutzbedarf dieser Informationen ist für jede an der Föderation beteiligten Organisation unterschiedlich. Um ein für das Gesamtsystem konsistentes Schutzniveau zu ermöglichen, müssen diese abgeglichen und bestimmte

Entscheidungen und Maßnahmen vor Beginn der Etablierung der Zusammenarbeit getroffen und realisiert werden. Entsprechend wurde vorliegend ein Modell anvisiert, welches die Entwicklung gemeinsamer Geschäftsprozesskonfigurationen unterstützt.

Traditionelle Ansätze zur Ausrichtung der IT an den Geschäftszielen (wie COBIT), für das IT-Management (wie ITIL) und/oder die Etablierung und Aufrechterhaltung von Informationssicherheit (wie die ISO 27001) adressieren die Entwicklung von Geschäftsprozessen nicht. Gleichzeitig ist die Adressierung von informationssicherheitstechnischen Anforderungen von traditionellen Rahmenwerken zum Geschäftsprozess-Management (wie ARIS) ebenfalls nicht hinreichend gegeben.

Das resultierende Rahmenwerk etabliert eine Erweiterung der traditionellen Geschäftsprozess-Sichten (auf Ressourcen, Geschäftsinformationen, Geschäftsfunktionen, resultierende Prozesse und erhaltbare Dienstleistungen und Produkte) um informationssicherheitstechnische Informationen, Funktionen und Prozesse, welche als Input für die Entwicklung und/oder der informationssicherheitstechnischen Optimierung von Geschäftsprozessen dienen können. Tabelle 13.2 zeigt das entwickelte, GRC-optimierte Geschäftsprozess-Rahmenwerk („GRCGPM“) in Relation zu den untersuchten.

Es entstanden Phasen zur Analyse, der Konzeption, der Implementierung, dem Monitoring und der fortwährenden Verbesserung der resultierenden Geschäftsprozesse, inklusive der eingesetzten technischen Komponenten. Dabei werden Aussagen über zu realisierende Maßnahmen an beteiligten Ressourcen auf Basis der identifizierten Schutzbedarfe der Informationen der beteiligten Kooperationspartner möglich. Das Modell wurde an einem konkreten Anwendungsfall, aufgrund von Komplexität und Verbreitung dem Order-to-Cash Ende-zu-Ende Geschäfts-prozess, mit einer konkreten technischen Instanziierung, einer teilweisen mobilen Unterstützung, validiert. Hierbei wurde einerseits gezeigt, dass auch die Behandlung nicht föderierter Szenarien deckungsgleiche Ergebnisse zu denen der ISO 27001 liefert. Andererseits wurde gezeigt, dass das Problem unterschiedlicher Schutz-

Kriterium	COBIT	ITIL	ISO 27001	BSI IT-GS	GRCGPM
Föderierbarkeit	Mittel	Mittel	Mittel	Gering	Hoch
GRC-Prozesse	Teilweise	Hoch	Vollst.	Vollst.	Vollst.
PDCA-Konformität	Ja	Nein	Ja	Ja	Ja
Operationalisierbarkeit	Gering	Hoch	Mittel	Hoch	Hoch
Dokumentationsaufwand	Gering	Gering	Gering	Hoch	Mittel
Konkretisierung	Gering	Mittel	Mittel	Hoch	Mittel
Implementierungskosten	Gering	Mittel	Mittel	Hoch	Mittel
Zertifizierbarkeit	Nein	Ja	Ja	Ja	(Potenz.)

Tabelle 13.2: Einordnung des entwickelten Rahmenwerks

bedarfe, und somit inkompatibler Schutzniveaus der in der Föderation transportierten Informationen, unter Anwendung des entwickelten Rahmenwerks nicht mehr auftreten. Abschließend wurde das Modell einer Akzeptanzprüfung unterzogen. Hierzu wurde das Technology Acceptance Model (TAM) aufgrund seiner universellen Einsetzbarkeit ausgewählt, ein Fragebogen entwickelt und drei Zielpersonen unterschiedlicher betrieblicher Positionen befragt. Das Ergebnis der Befragung ist eine hinsichtlich Effektivität und Transparenz positive, hinsichtlich Effizienz bei der Geschäftsführung negative Einschätzung.

Dies schließt die vorliegende Untersuchung.

Literaturverzeichnis

[AA06] Marco Maratea Serena Elisa Ponta Alessandro Armando, Enrico Giunchiglia. *An action-based approach to the formal specification and automated analysis of business processes under authorization constraints*. Journal of Computer and Systems Sciences: Special issue on Knowledge Representation and Reasoning, 2006.

[AG14] SAP AG. Sap ui5 architektur, online `http://sap.github.io/openui5/`, Zugriff am 10.03.2014.

[All14] Cloud Security Alliance. Open certification framework. *Online verfügbar unter `https://cloudsecurityalliance.org/research/ocf/`*, zuletzt besucht am 21. Juli 2014.

[APQ14] APQC. *APQC's Process Classification Framework*. APQC, 2014.

[BCN92] C. Batini, S. Ceri, and S. B. Navathe. Conceptual database design. an entity-relationship-approach. *Benjamin Cummings, Redwood City, California*, 1992.

[BFN03] C. Batini, L. Furlani, and E. Nardelli. What is a good diagram? a pragmatic approach. *Chen, P. P.-S. (ed.): Proceedings of the 4th International Conference on the Entity- Relationship Approach: The Use of ER Concept in Knowledge Representation. Elsevier, North-Holland*, pages 312 – 319, 2003.

[BfSidI09] BSI and Bundesamt für Sicherheit in der Informationstechnik. Leitfaden informationssicherheit - it-grundschutz kompakt, 2009. Online verfügbar unter `https://www.bsi.bund.de/cae/servlet/contentblob/540280/publicationFile/34672/GS-Leitfaden_pdf.pdf`; besucht am 10. Januar 2010.

[Bha03] USA ; Raj Rajagopalan S. ; Rao P. Bhatt, S. ; Telcordia Technol. Federated security management for dynamic coalitions. *DARPA Information Survivability Conference and Exposition, Proceedings (Volume:2)*, April 2003.

[BJMU11] K. Bernsmed, M.G. Jaatun, P.H. Meland, and A Undheim. Security slas for federated cloud services. In *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, pages 202–209, Aug 2011.

[Boo95] Grady Booch. *Objektorientierte Analyse und Design*. Addison-Wesley; Auflage: 6. Aufl., 1995.

[BSI09a] Bundesamt für Sicherheit in der Informationstechnik BSI. Bsi-standard 100-1, 100-2, 100-3, 100-4, 2009.

[BSI09b] Bundesamt für Sicherheit in der Informationstechnik BSI. *Informationssicherheit – Ein Vergleich von Standards und Rahmenwerken*. BSI, Bonn, 2009.

[Buc06] Kay Alexander Buck. *Entwicklungs eines Modells zur Integration von Akzeptanz und Motivation in mediengestützte Lehrveranstaltungen an der Hochschule Furtwangen*. Hochschule Furtwangen, 2006.

[Cou08] PCI Security Standards Council. *Payment Card Industry Data Security Standard (PCI DSS)*. PCI SSC, 2008.

[Cou14] Supply Chain Council. *Supply Chain Operations Reference (SCOR)*. Supply Chain Council, 2014.

[CS11] Dieter Bartmann Christian Senk. *Starke Authentifizierung für den sicheren Zugriff auf IT-Ressourcen in Föderationen*. In: Sinz, Elmar J. und Bartmann, Dieter und Bodendorf, Freimut und Ferstl, Otto K., (eds.) Dienstorientierte IT-Systeme für hochflexible Geschäftsprozesse. Schriften aus der Fakultät Wirtschaftsinformatik und Angewandte Informatik der Otto-Friedrich-Universität Bamberg, 9 (16). University of Bamberg Press, Bamberg, Deutschland, 2011.

[CWA08] L. Michelle Bobbitt Chad W. Autry. Supply chain security orientation: conceptual development and a proposed framework. *International Journal of Logistics Management, The, Vol. 19 Iss: 1*, pages 42 – 64, 2008.

[Dav85] F. Davis. *A technology acceptance model for empirically testing new end-user information systems - theory and results (PhD thesis*. Massachusetts Inst. of Technology, 1985.

[Deg86] Werner Degenhardt. Akzeptanzforschung zu bildschirmtext: Methoden und ergebnisse. *München*, 1986.

[DJC04] Edmund F. McGarrell David J. Closs. Enhancing security throughout the supply chain. *IBM SPECIAL REPORT SERIES*, 2004.

[dWiDeH13] Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.). Das idw, 2013.

[ea11] Becher et al. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. *IEEE Symposium on Security and Privacy*, 2011.

[EI08] Inc. Enterprise Integration. Aris for dodaf. *Whitepaper*, 2008.

[EN13] Ute Riemann Erik Neitzel. Grc monitoring of federated end-to-end business processes. *Heilongjiang University National Science Foundation of China (Hrsg.): Proc. of 2013 International Conference on Sensor Network Security Technology and Privacy Communication System;*, pages 44–47, 2013.

[Est03] W. A. Estrem. *An Evaluation Framework for Deploying Web Services in the Next Generation Manufacturing Enterprise*. Robitics and Computer-Integrated Manufacturing, 2003.

[Fau02] D.A. Faust. *Effektive Sicherheit: Analyse Des Systems Kollektiver Sicherheit Der Vereinten Nationen Und Entwurf Eines Alternativen Sicherheitssystems*. VS Verlag für Sozialwissenschaften, 2002.

[fdDudI10] Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Bundesdatenschutzgesetz (bdsg), 2010.

[Fie00] T. R. Fielding. *Dissertation: Architectural Styles and the Design of Network-based Software Architecture*. University of California, Irvine, 2000.

[fNe05] DIN Deutsches Institut für Normung e.V. *Informationstechnik – IT-Sicherheitverfahren – Leitfaden für das Informationssicherheits-Management (ISO/IEC 27002:2005)*. Beuth Verlag, Berlin, 2005.

[Fro11] Network Frontiers. Unified compliance framework. *Online verfügbar unter* `http://www.unifiedcompliance.com/sites/default/files/RSA%20Archer.UCF_Data_Sheet.pdf`, Januar 2011.

[fS14] International Organization for Standardization. Entwurf: Information technology - security techniques - information security management for inter-sector and inter-organizational communications. *ISO/IEC 27010:2012(en), onli-*

ne verfügbar unter `https://www.iso.org/obp/ui/#iso:std:iso-iec:27010:ed-1:v1:en`, 2014.

[fSidI08] BSI Bundesamt für Sicherheit in der Informationstechnik. *Informationssicherheit und IT-Grundschutz: BSI-Standards 100-1, 100-2 und 100-3*. Bundesanzeiger; Auflage: 2., überarbeitete Auflage., 20. Juni 2008.

[Gab12] Wirtschaftslexikon Gabler. *Definition Informationssystem*. Gabler Verlag (Herausgeber), 2012.

[GG04] Karin Grossmann and Klaus E. Grossmann. *Bindungen: das Gefüge psychischer Sicherheit*. Klett-Cotta, Stuttgart, 2004.

[Glo09] Boris Gloger. *Scrum - Produkte zuverlässig und schnell entwickeln*. Carl Hanser Verlag München, Seite 31, 2009.

[Gmb07] Safari GmbH. Ein modell zur akzeptanzanalyse für die entwicklung situationsabhängiger mobiler dienste im compass ansatz – fachvortrag auf der konferenz mc3 in augsburg, 2007.

[GMN05] Martin Gaedke, Johannes Meinecke, and Martin Nussbaumer. A modeling approach to federated identity and access management. In *Special Interest Tracks and Posters of the 14th International Conference on World Wide Web*, WWW '05, pages 1156–1157, New York, NY, USA, 2005. ACM.

[Goe06a] Matthias Goeken. *IT-Governance – neue Aufgaben des IT-Managements*. In: HMD 250, August 2006. Herausgegeben von Hans-Peter Fröschle, Susanne Strahringer. (Gemeinsam mit Wolfgang Johannsen), 2006.

[Goe06b] Matthias Goeken. Referenzmodelle für betrieb und entwicklung von anwendungssystemen. *In: Vorgehensmodelle und Projektmanagement - Assessment, Zertifizierung, Akkreditierung*

(Höhn, R. et al.), Proceedings of 14th Workshop of WI-VM Symposium GI, Aachen, 2006.

[Gro14] Value Chain Group. *Value Chain Reference Model (VRM)*. Value Chain Group, 2014.

[GT05] Dale L. Goodhue and Ronald L. Thompson. Task-technology fit and individual performance. *MIS Quarterly Vol. 19, No. 2*, 2005.

[Hat05] Simon Fraser Univ. Surrey BC Canada ; Ty Mey Eap ; Ashok Shah Hatala, M. ; Sch. of Interactive Arts Technol. Federated security: lightweight security infrastructure for object repositories and web services. *Conference: Next Generation Web Services Practices*, 2005.

[Her99] T. Herrmann. Perspektiven der medienwirtschaft. kompetenz - akzeptanz - geschäftsfelder. *Szyperski, N. (Hrsg.): Perspektiven der Medienwirtschaft*, 1999.

[Hev04] Alan R. Hevner. *Design Science in Information Systems Research*. MIS Quarterly Vol. 28 No. 1, Seiten 75 - 105, 2004.

[HF10] Torsten Till Erik Neitzel Holger Friedrich, Torsten Kempa. Konzeption eines isms-tools zur unterstützung der rahmenwerke cobit, itil, iso 27001/02 & bsi it-grundschutz. *Projektbereicht, entstanden im Rahmen des Masters Security Management*, Juni 2010.

[HR06] Carsten Dorrhauer Haio Röckle. *Messbarkeit der Sicherheitsqualität im Lebenszyklus betrieblicher Anwendungssysteme*. In: Betriebliche Anwendungssysteme (Thomas Bartin, Burkhard Erdlenbruch, Frank Herrmann, Christian Müller (Herausgeber)), Tagungsband zur AKWI-Fachtagung, September 2011, Worms, 2006.

[IDW11] Institut der Wirtschaftsprüfer IDW. *IDW PS 980 – Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen*. WPg Supplement, 2011.

[Ins07] IT Governance Institute. *Cobit 4.1*. ISA, 2007.

[Ins12] IT Governance Institute. *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT*. ISACA, 2012.

[ISO13] ISO/IEC. 27002:2013(en): Information technology - security techniques - code of practice for information security controls, 2013.

[Jos08] Nicolai Josuttis. *SOA in der Praxis: System-Design für verteilte Geschäftsprozesse*. Dpunkt Verlag; Auflage: 1., Aufl., 2008.

[Kei04] Detlef Keitsch. *Risikomanagement*. Schäffer-Poeschel Verlag, 2. Auflage, 2004.

[Klo08] Larry Klosterboer. *Implementing ITIL Change and Release Management*. IBM Press, 2008.

[KMW00] Michael Koch, Kathrin Möslein, and Michael Wagner. Vertrauen und reputation in online-anwendungen und virtuellen gemeinschaften - trust and reputation in online applications and virtual communities. *Proc. Workshop 'GeNeMe2000 - Gemeinschaften in Neuen Medien' (Gemeinschaften in Neuen Medien, Martin Engelien; Detlef Neumann (Herausgeber))*, 2000.

[Kol00] Tobias Kollmann. Die messung der akzeptanz bei telekommunikationssystemen. *Journalbibliothek Universität Duisburg-Essen*, 2000.

[Kri01] Nico Krisch. *Selbstverteidigung und kollektive Sicherheit*. Springer Verlag, 2001.

[LDL03] Ann Lindsay, Denise Downs, and Ken Lunn. Business processes – attempts to find a definition. *Information and Software Technology, Volume 45, Issue 15*, pages 1015–1019, 2003.

[LJH07] Friedrich Roithmayr Lutz Jürgen Heinrich, Armin Heinzl. *Wirtschaftsinformatik: Einführung und Grundlegung*. Oldenbourg Verlag, 4. Auflage, 2007.

[LL08] Hongtao Zhang Lode Li. Confidentiality and information sharing in supply chain coordination. *Management Science, Volume 54 Issue 8*, pages 1467 – 1481, 2008.

[LRD03] Avraham Leff, James T. Rayfield, and Daniel M. Dias. Service-level agreements and commercial grids. *IEEE Internet Computing, 7(4)*, pages 44–55, 2003.

[Mee11] Ioana Ciuciu; Yan Tang; Robert Meersman. Towards retrieving and recommending security annotations for business process models using an ontology-based data matching strategy. *Symposium on Data-Driven Process Discovery and Analysis (SIMPDA), Volume 1, Seiten 71-81*, 2011.

[MF07] Matthias Goeken Wolfgang Johannsen Martin Fröhlich, Kurt Glasner. *Sichten der IT-Governance*. IT Governance (ISACA Germany Chapter e.V.), dpunkt.verlag, 2007.

[MG09] Peter Mell and Tim Grance. The nist definition of cloud computing. *National Institute of Standards and Technology, Information Technology Laboratory*, 2009.

[MM08] Ila Manuj and John T. Mentzer. Global supply chain risk management. *Journal of Business Logistics*, 29(1):133–155, 2008.

[MNF06] Ravi Shankar Mohd Nishat Faisal, D.K. Banwet. Supply chain risk mitigation: modeling the enablers. *Business Process Management Journal, Vol. 12 Iss: 4*, pages 535 – 552, 2006.

[Mor04] Scott; Carmody Steven; Hoehn Walter; Klingenstein Ken Morgan, R. L.; Cantor. *Federated Security: The Shibboleth Approach*. EDUCAUSE Quarterly, v27 n4, Seiten 12-17, 2004.

[MS98a] D. L. Moddy and G. Shanks. Improving the quality of entity relationship models: An action research programme. *Edmundson, B., Wilson, D. (eds.): Proceedings of the 9th Australiasian Conference on Information Systems. Vol. II, Sydney*, pages 433 – 448, 1998.

[MS98b] D. L. Moody and G. G. Shanks. What makes a good data model? a framework for evaluating and improving the quality of entity relationship models. *The Australian Computer Journal, 30*, pages 97 – 110, 1998.

[Mül10] Klaus-Reiner Müller. *Handbuch Unternehmenssicherheit*. Vieweg+Teubner Verlag, 2. überarbeitete Auflage, 2010.

[NF12] Erik Neitzel and Robert U. Franz. Sicherheit in erp-konfigurationen. *In: ERP Management 4/2012*, pages 47–49, 2012.

[oD14] Department of Defence. Dod, online `http://dcmo.defense.gov/products-and-services/business-enterprise-architecture/10.0/classic/htm/end2end.htm`, Zugriff am 02.05.2014.

[Ora12] Oracle. *An Oracle White Paper in Enterprise Architecture December 2012: Oracle Enterprise Architecture Framework: Information Architecture Domain, Version 2.0*. Oracle Whitepaper, 2012.

[Org09] OPEN Process Framework Repository Organization. *OPEN Process Framework (OPF)*. OPFRO, 2009.

[oT03] Massachusetts Institute of Technology. *MIT Process Handbook*. MIT, 2003.

[Por08] Michael E. Porter. *Competitive Advantage: Creating and Sustaining Superior Performance*. Simon and Schuster, 2008.

[Pro14] FP7 European Project. Trusted architecture for securely shared services. *Online verfügbar unter http://www.tas3.eu*, Zuletzt besucht am 1. Juli 2014.

[PRW03] Arnold Picot, Ralf Reichwald, and Rolf T. Wigand. *Die grenzenlose Unternehmung: Information, Organisation und Management: Lehrbuch zur Unternehmensführung im Informationszeitalter*. Gabler Verlag, 2003.

[QMC14] VDA QMC. *Automotive Spice*. VDA QMC, 2014.

[Ran06] D.S. Ransom. System and method for federated security in an energy management system, October 24 2006. US Patent 7,127,328.

[RC70] Anatol Rapoport and Albert M. Chammah. *Prisoner's Dilemma*. University of Michigan, 1970.

[RM97] Ralf Reichwald and Kathrin Möslein. Organisation: Strukturen und gestaltung. `http://www.aib.wiso.tu-muenchen.de`, 1997.

[RP02] Ralf Reichwald and Frank Thomas Piller. *Customer integration: Formen und Prinzipien einer Integration der Kunden in die unternehmerische Wertschöpfung*. Lehrstuhl für Allg. und Industrielle Betriebswirtschaftslehre an der TU München, 2002.

[SAP13] SAP. Process management lifecycle. *http://scn.sap.com/docs/DOC-23472*, besucht am 29.03.2013.

[Sch00] A.W. Scheer. *ARIS-Business Process Modelling*. Springer, 2000.

[Sch04] Alexandra Schwerin. *Staatsaufgabe Sicherheit*. GRIN Verlag, 2004.

[Sch06] Michaela Schütt. *Informationsmanagement auf elektronischen B2B-Marktplätzen*. In Markt- und Unternehmensentwicklung, Hrsg.: Arnold Picot, Ralf Reichwald, Egon Franck, Dissertation Universität München, Gabler Edition Wissenschaft, 2006.

[Sey02] P.B. Seybold. *The Five Waves of Customer Relationship Management*. Business Briefing: Data Management & Storage Technology, 2002.

[SH00] Thomas M. Siebel and Pat House. *Cyber Rules.: Die neuen Regeln für Spitzenerfolg im e-Business*. Verlag Moderne Industrie, 2000.

[SJ05] Ravi Shankar Sanjay Jharkharia. It-enablement of supply chains: understanding the barriers. *Journal of Enterprise Information Management, Vol. 18 Iss: 1*, pages 11 – 27, 2005.

[Spr07] Reinhard K. Sprenger. *Vertrauen führt: Worauf es im Unternehmen wirklich ankommt*. Campus Verlag, 2007.

[Spr12] Reinhard K. Sprenger. *Radikal führen*. Campus Verlag, 2012.

[SS06] Thoams Nowey Sabrina Sitzberger. *Lernen vom Business Engineering - Ansätze für ein systematisches, modellgestütztes Vorgehensmodell zum Sicherheitsmanagement*. In: Multikonferenz Wirtschaftsinformatik 2006 (Lehner, Franz und Nösekabel, Holger und Kleinschmidt, Peter (Herausgeber)). Tagungsband 2. Gito, Berlin, 2006.

[SS11] V. Kavitha S. Subashini. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications Volume 34, Issue 1*, pages 1–11, Januar 2011.

[Ste06] Paul Stephenson. Ensuring consistent security implementation within a distributed and federated environment. *Computer*

Fraud & Security, Volume 2006, Issue 11, Seiten 12-14, November 2006.

[T84] Peters R.H. Watermann T, J. *In search of Excellence: Lessons from America's Best-run companies*. Warner Books, 1984.

[TMF14] TMForum. *Business Process Framework (eTOM)*. TMForum, 2014.

[WA11] Samuel Paul Kaluvuri Serena Elisa Ponta Wihem Arsac, Luca Compagna. *Security validation tool for business processes*. In Proceedings of the 16th ACM symposium on Access control models and technologies, SACMAT '11, pages 143-144, New York, NY, USA. 2011, ACM, 2011.

[Wal88] Mary Walton. *Deming management method*. Perigee Trade, 1988.

[Wie14] Sandra Wiesbeck. Arbeitskreis: Industrial it security. *Bayerischer IT-Sicherheitscluster e.V., online verfügbar unter* `http://www.it-sicherheit-bayern.de/IT-Sicherheitscluster/117362-666,1,0.html`, 2014.

[Wir12] Wirtschaftsinformatiklexikon. *Definition Informationssystem*. Seite 325, 7. Auflage, 2012.

[WS04] Johann Wagner and Kurt Schwarzenbacher. *Föderative Unternehmensprozesse*. Publicis Corporate Publishing, Erlangen, 2004.

[WS13] Lawrie Brown William Stallings. *Computer Security Principles and Practice*. Pearson Education, Inc., 2013.

[Wör08] Johann-Dietrich Wörner. Sicherheit und forschung. *DLR Magazin 128, Seite 7*, 2008.

[Zar09] Panos Zarkadakis. *Managementorientiertes Audit der Informationssicherheit: Beschreibung eines mehrdimensionalen Verfahrens zur Analyse der Informationssicherheit in Unternehmen (Taschenbuch)*. VDM Verlag Dr. Müller, 16. Dezember 2009.

[ZLR93] A. Zamperoni and P. Löhr-Richter. Enhancing the quality of conceptual database specifications through validation. *In: Elmasri, R. A., Kouramajian, V., Thalheim, B. (eds.): Proceedings of the 12th International Conference on the Entity-Relationship Approach - ER '93. Springer-Verlag, Berlin et al.*, pages 85 – 98, 1993.

A Zuordnung von Maßnahmen, Kontrollen und Schutzbedarfen

Maßnahme	Kontrolle	Schutzbedarfe
1 Organisatorisch		
1.1 Errichtung und Durchsetzung mobiler Device-Policy (unterstützte Geräte, Nutzungsrichtlinien, Rollen und Verantwortlichkeiten, etc.)	1	normal
Verwendung von Acces-Control-Listen (Autorisierung, Rollen und Privilegien für Zugriff über Mobilgeräte)	1	hoch
1.2 Errichtung von Informationssicherheitskompetenz (Schulungen für Awareness, Bedienung und Prozesse, insbesondere Notfallprozesse)	8	normal
1.3 Errichtung und Wartung eines Verschlüsselungsmanagements	9	hoch
1.4 Aufnahme von Sicherheitsaudits von Web- und mobilen Anwendungen	8	hoch
2 Gerätespezifisch (Hardware/Software)		
2.1 Verschlüsselung		
2.1.1 Verwendung von Datenverschlüsselungsverfahren bei Transport von Daten über öffentliche Netze	2	normal
2.1.2 Verwendung von starken Datenverschlüsselungsverfahren bei Transport von Daten über öffentliche Netze	2	sehr hoch
2.1.3 Verwendung von sicheren Zugriffsschichten für lokale Datenablage	2	hoch
2.2 Persistenz		
2.2.1 Verwendung einer lokalen Persistenzschicht (Offline-Modus)	4	normal
2.2.2 Verwendung von hybriden Persistenzschichten (offline und online)	4	hoch
2.2.3 Verwendung einer entfernten Persistenzschicht (Online-Modus)	4	sehr hoch
2.3 Administration		
2.3.1 Etablierung von Prozessen und Werkzeugen zur Verhinderung von Malicious-Code-Attacken (Viren, Spam, Malware, Trojaner, etc.)	5	normal
2.3.2 Installation und Konfiguration von Firewalls auf allen mobilen Geräten	5	normal
– Fortsetzung auf Folgeseite –		

Tabelle A.1: Maßnahmen, Kontrollen und adressierte Schutzbedarfe

Maßnahme	Kontrolle	Schutzbedarfe
2.3.3 Durchsetzung sicherer Gerätekonfiguration (Netzwerkports, Protokolle, Dienste, Gerätesensoren, Kennwortstärken)	5	normal
2.4 Authentisierung und Autorisierung		
2.4.1 Bereitstellung eines zentralen ID-Managements	1	normal
2.4.2 Erzwingen von PIN-Codes	1	hoch
2.4.3 Erzwingen einer Multi-Factor-Authentisierung	1	sehr hoch
3 Infrastrukturell		
3.1 Mobile Device Management		
3.1.1 Errichtung und Aufrechterhaltung eines Geräteinventars	5	normal
3.1.2 Errichtung und Aufrechterhaltung eines Geräteinventars mit Durchsetzung dedizierter Informationssicherheitsrichtlinie	5	hoch
3.1.3 Errichtung und Aufrechterhaltung eines zentralen plattformübergreifenden Gerätemanagements (Gerätekonfigurationskontrolle, Fernlöschung, Lokalisierung, Passwortrücksetzung, Betriebssystemupdates, etc.)	5	sehr hoch
3.2 Loggin, Monitoring, Testing		
3.2.1 Zugriff und Nutzung loggen (Performance- und Nutzungsmetriken)	3	normal
3.2.2 Überprüfung digitaler Signaturen von Anwendungen (inklusive Updates)	3	hoch
3.2.3 Systematische Aufzeichnung und Analyse von Sicherheitsvorfällen	3	hoch
3.2.4 Regelmäßige Durchführung von Penetrationstests der Infrastruktur, Dienste und Anwendungen	7	hoch
3.3 Netzwerk und Drittanbieter		
3.3.1 Segmentierung des Unternehmensnetzwerks zur Isolierung mobiler Anfragen	7	sehr hoch
3.3.2 Bereitstellung von Mechanismen für sicheren Mobilzugriff (VPN, IPsec, SSL)	7	normal
3.3.3 Monitoring von Service-Level-Agreements und Sicherheitsleveln Dritter (Cloud-Storage, Webservices, mobile Middleware, etc.)	7	hoch

Tabelle A.2: Maßnahmen, Kontrollen und adressierte Schutzbedarfe (Fortsetzung)

Akademischer Werdegang

1998 - 2005 :	Abitur am Theodor–Fontane–Gymnasium Strausberg, Leistungskurse Physik und Englisch
2006 - 2009 :	Studium der Wirtschaftsinformatik an der FH Brandenburg, Abschluss zum Bachelor of Science mit Prädikat „sehr gut“
2007 - 2009 :	Studentischer Mitarbeiter der FH Brandenburg, Tutor für Datenbanken I, II, III und Programmierungstechnik
2007 :	Gewinner des Programmierwettbewerbs 2007
2007 - 2008 :	Mitglied des akademischen Senats der FH Brandenburg
2008 - 2009 :	Mitglied des Prüfungsausschusses des Fachbereichs Wirtschaft der FH Brandenburg
2008 - 2009 :	Stipendiat der SysTree AG Berlin
2009 - 2015 :	Akademischer Mitarbeiter der FH Brandenburg
2009 :	Nominierung für den Nachwuchswissenschaftlerpreis des Ministeriums für Wissenschaft, Forschung und Kultur, Land Brandenburg
2009 - 2010 :	Studium des Security Managements an der FH Brandenburg, Abschluss zum Master of Science mit Prädikat „sehr gut“
2010 :	Auszeichnung als bester Absolvent der FH Brandenburg Studiengang Wirtschaftsinformatik Abschlussjahrgang 2008/09
2011 - 2015 :	Promotion zum Doktor-Ingenieur (Dr.-Ing.) an der Otto-von-Guericke-Universität Magdeburg