Otto-von-Guericke-Universität Magdeburg

Thema:

Information Security Governance

mit COBIT, ITIL und ISO 27002

Masterarbeit

Fakultät für Informatik
Arbeitsgruppe Wirtschaftsinformatik

Themensteller:	Prof. Dr. rer. pol. habil. Hans-Knud Arndt
Betreuer:	Prof. Dr. rer. pol. habil. Hans-Knud Arndt
vorgelegt von:	Ying Zhang
Abgabetermin:	04. März. 2010

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ARIS	Architektur integrierter Informationssysteme
CCTA	Central Computer and Telecommunications Agency
COBIT	Control Objectives for Information and Related Technology
CI	Configuration Items
CMDB	Configuration Management Database
CSI	Continual Service Improvement
EPK	Ereignisgesteuerte Prozesskette
eEPK	erweiterte ereignisgesteuerte Prozesskette
GoM	Grundsätze der ordnungsgemäßen Modellierung
ISACA	Information Systems Audit and Control Association
ISACF	Information Systems Audit and Control Foundation
ISG	Information Security Governance
IT	Informationstechnologie
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
IEC	International Electrotechnical Commission
ISO	International Standards Organization
IS	Informationssicherheit
KPI	Key Performance Indicator
OGC	Office of Government Commerce
OLAs	Operating Level Agreements
RFC	Require for Change
SGML	Standard Generalized Markup Language
SLA	Service Level Agreement
SLR	Service Level Requirements

SRI	Stanford Research Institute
UC	Underpinning Contracts
WSD	Wertschöpfungskettendiagramm
WSK	Wertschöpfungsketten
XML	Extensible Markup Language

Kapitel 1

Einleitung

1.1 Problemstellung

In unserer heutigen modernen Gesellschaft nimmt die Informationstechnologie für beinahe sämtliche Branchen einen immer höheren Stellenwert ein. Insbesondere moderne Unternehmen können ohne Informationstechnologie nur sehr schwer existieren, geschweige denn weiterentwickeln. Aufgrund dieser zunehmenden Abhängigkeit von der Informationstechnologie im Wirtschaftsleben, werden die Informationen einerseits als wichtiges Vermögen bezeichnet, die Ziele des Unternehmens stark unterstützen, aber andererseits auch aufgrund der ansteigenden Komplexität der Informationstechnologie als die Schwäche der Unternehmen, die verheerende Probleme oder gravierende Risiken verursachen könnte. Daher sind Informationen als Vermögen eines Unternehmens im Vergleich zum traditionellen Sachvermögen weitaus sensibler und verletzbarer, welche einer optimalen Verwaltung und einem besonderem Schutz unterliegen müssen.

Für eine lange Zeit wurde die Informationssicherheit lediglich aus der rein technischen Perspektiv betrachtet, die den Fokus auf den Schutz vor einem externen Angriff auf die Informationsinfrastruktur des Unternehmens legt [vgl. ITS 2009 S.7]. Zu Beginn der 80er Jahre verweilten Informationen aufgrund der raschen Entwicklung der Netzwerke, vor allem jedoch in der Internettechnologie, nicht nur in einem Unternehmen, da durch das stark vernetzte Internet Informationen nun überall ausgetauscht werden konnten. Damit veränderte sich auch die Informationssicherheit, die früher lediglich als passiver Schutz vor einem externen Angriff und somit als eine technische Aufgabe angesehen wurde, die der Technikabteilung angehörte, hin zu

einer vollständigen und dynamischen Verwaltung sowie Kontrolle aller Informationsressourcen auf der Organisationsebene, welche eine große Herausforderung einerseits für das gesamte Unternehmen und andererseits für die IT-Governance darstellte [vgl. ITGI2006 S.8].

Deshalb verwenden viele Unternehmen mehrere Standards oder Best Practices, um die effektive und systematische Umsetzung der Informationssicherheit in einer Organisation zu unterstützen. Die Standards bzw. Best Practices bieten jeweils aus ihrer eigenen Sicht Informationssicherheitsprozesse, wobei manche auch ähnlich miteinander verknüpft sind. Wenn alle Informationssicherheitsprozesse von verschiedenen Standards bzw. Best Practices ohne Integration verwendet werden, könnten entweder Ressourcen verschwendet oder gar Sicherheitslücken verursacht werden. Daher ist es wichtig für die Unternehmen, die aus verschiedenen Gründen mehrere dieser Standards oder Best Practices anwenden wollen oder müssen, ein unternehmensweites Framework aufzubauen, die alle Informationssicherheitsprozesse aus verschiedenen Standards und Best Practices möglicherweise miteinander integrieren und noch handhabbar machen.

Diese Masterarbeit soll ein integriertes Framework unter dem Begriff „Information Security Governance“ aufbauen, die den Standard für das Informationssicherheits-managementsystem ISO 27002 und die zwei weiteren bekannten Standards bzw. Best Practices COBIT und ITIL, aus der Perspektive der Informationssicherheit miteinander anpasst. Hier sollen vor allem die Überschneidungen zwischen diesen drei Standards sowie Best Practices klar gezeigt und eine ansprechende Lösung gefunden werden.

1.2 Motivation

Information Security Governance ist zurzeit ein sehr populäres Thema, das viel diskutiert und erforscht wird. Aus diesem Gunde war es meine Motivation, diese Arbeit dem Thema zu widmen. Allerdings ist es oft gar nicht klar gewesen, was nun

genau mit diesem Begriff gemeint wird. Eine exakte Definition oder Beschreibung darüber in Nachschlagwerken wie, „Wirtschaftsinformatik Lexikon“ (Heinrich/ Heinzl/Roithmayr2004), „Einführung in die Wirtschaftinformatik“ (Stahlknecht /Hasenkamp2005) oder „Grundkurs Wirtschaftinformatik“ (Abts/Mülder2004) konnte nicht gefunden werden.

Darüber hinaus beschränken sich die Angaben zur Methodenunterstützung in der vorhandenen Literatur über „Information Security Governance“ zumeist nur auf ein bestimmtes Referenzmodell (beispielsweise nur auf COBIT oder ISO 27002), ein Framework, die alle drei Standards und Best Practices ISO 27002, CobiT und ITIL berücksichtigt, ist derzeitig noch nicht vorhanden.

Aus den oben genannten Gründen soll nun im folgenden Kapitel auf das Thema der Arbeit „Information Security Governance“ eingegangen werden.

1.3 Wissenschaftliche Zielsetzung

Die vorliegende Arbeit beschreibt den gegenwärtigen Stand der Entwicklung von Information Security Governance. Dabei stehen insbesondere die im Rahmen von Information Security Governance anfallenden Aufgaben und die mögliche Unterstützung durch ISO 27002, COBIT und ITIL im Vordergrund.

Weiterhin wird in dieser Arbeit Information Security Governance in geeignete Teilaufgaben aufgegliedert, so dass eine Zuordnung zu Elementen aus den drei Referenzmodellen (ISO 27002, COBIT und ITIL) möglich wird. Wo eine mögliche Überschneidung zwischen den drei Referenzmodellen auftaucht, wird aufgezeigt und die Entscheidung getroffen, welche Lösung, die aus der Überschneidung der drei Referenzmodellen entsteht, die entsprechende Teilaufgabe von Information Security Governance am besten unterstützen kann.

Schließlich soll ein Referenzprozess entwickelt werden, welches ermöglicht, dass bei einer Einführung von Information Security Governance in einem Unternehmen, bereits bestehende Lösungen mit ITIL oder COBIT verwendet bzw. beibehalten werden, und bei der Implementierung handhabbar sein können.

1.4 Lösungsweg

In Kapitel 2 werden zunächst die theoretischen Grundlagen für den weiteren Verlauf der Arbeit beschrieben. Anschließend werden in Kapitel 2.1 die für diese Arbeit nötigen Begriffe definiert, wobei weiterhin in Kapitel 2.2 und 2.3 die Informationssicherheit bzw. dessen Ziele für Unternehmen als Grundlage vorgelegt werden. Darüber hinaus soll in Kapitel 2.4 Information Security Governance definiert werden, um schließlich festzulegen, was sich konkret hinter diesem Begriff verbirgt bzw. wo Grenzen zwischen Corporate Governance und IT-Governance zu setzen sind. Des Weiteren werden Aufgaben dargestellt, die im Rahmen einer Information Security Governance anfallen. In Kapitel 2.5 wird eine theoretische Auseinandersetzung vorgenommen, womit relevante Begriffe der Referenzmodellierung näher erklärt werden sollen. Im vorletzten Kapitel 2.6 werden die in dieser Arbeit verwendeten zwei Werkzeuge, nämlich Topic Maps bzw. ARIS vorgestellt. Schließlich werden im letzten Kapitel 2.7 alle drei Standards bzw. Best Practices detailliert beschrieben.

Auf der vorgelegten Grundlage werden im Praxisteil (Kapitel 3) alle drei Standards bzw. Best Practices der Information Security Governance zugeordnet und zudem geklärt, wie die Prozesse der drei Standards bzw. Best Practices jeweilige Teilaufgaben von Information Security Governance unterstützen.

Darüber hinaus wird in Kapitel 4 mit Hilfe des Modellierungstools ARIS Toolset ein Referenzmodell für Information Security Governance aufgebaut, die in drei Ebenen strukturiert ist und diese wiederum in verschiedene Prozessdetailstufen abgebildet wird.

Zum Schluss der Arbeit wird einerseits in Kapitel 5 eine Zusammenfassung der wichtigsten Ergebnisse bzw. der erreichten Ziele vorgenommen. Im Anschluss daran gibt andererseits einen Ausblick auf die weiteren möglichen Entwicklungen zur Information Security Governance.

1.5 Abgrenzung der Arbeit

Information Security Governance stellt ein äußerst umfangreiches Thema mit vielen wichtigen Bausteinen dar. Auch zu den drei Standards bzw. Best Practices können jeweils wiederum eigene Arbeiten verfasst werden. Aus diesen Gründen können hier nicht alle Teilbereiche und Aspekte aufgriffen werden.

Kapitel 2

Grundlagen

2.1 Grundlegende Begriffe

2.1.1 Funktionen

Unter einer Funktion definiert MERTENS „eine Tätigkeit, die auf die Zustands- oder Lageveränderung eines Objekts ohne Raum- und Zeitbezug abzielt“. Eine Funktionsbezeichnung besteht aus zwei Komponenten, einem Verb (Verrichtung) und einem Substantiv (Objekt), auf das sich dieses Verb bezieht (z.B. „Bestellgrenze ermitteln“)“ [Mertens2007, S. 22]. Ähnlich wird eine Funktion in ARIS auch als eine fachliche Aufgabe bzw. Tätigkeit an einem Objekt zur Unterstätzung eines oder mehrerer Unternehmensziele definiert.

Allerdings kann eine Funktion in ITIL auch aus einer anderen Perspektive definiert werden, und zwar als „ein Team oder eine Gruppe von Personen und die Hilfsmittel, die eingesetzt werden, um einen oder mehrere Prozesse oder Aktivitäten durchzuführen“, damit das Zusammenspiel zwischen den Prozessen und der Aufbauorganisation beschrieben werden kann. Ein Beispiel dafür stellt Service Desk dar [Buchsein2008, S.51].

Aufgrund des Verzichts einer tiefen Bearbeitung des Organisationsaufbaus in dieser Arbeit, repräsentiert eine Funktion im ITIL Kontext nichts anderes als eine Kombination mehrere Prozesse. Deshalb wird hier die Definition einer „Funktion“ grundsätzlich von MERTENS akzeptiert.

2.1.2 Prozesse

Zur Definition von „Prozessen“ bestehen eine ganze Reihe unterschiedlicher Interpretationen. Gemäß DIN EN ISO 9000 ist ein Prozess eine Wertsteigerungstransformation unter Beteiligung von Menschen und anderer Mittel [Binner1997, S. 10].

Etwas konkreter ist die Auffassung vieler Arbeiten bezüglich betrieblich-organisatorischer Prozesse, die die Leistungserstellung der Organisation gewährleisten. In diesem Fall wird ein Prozess beispielsweise als inhaltlich abgeschlossene, zeitliche und sachlogische Folge von Aktivitäten, die zur Bearbeitung eines betriebswirtschaftlich relevanten Objektes notwendig sind, verstanden [vgl. Ros96, S. 9].

In ITIL wird ein Prozess folgendermaßen definiert: „Ein strukturierter Satz an Aktivitäten, mit deren Hilfe ein bestimmtes Ziel erreicht werden soll. Ein Prozess wandelt einen oder mehrere definierte Inputs in definierte Outputs um. Ein Prozess kann beliebige Rollen, Verantwortlichkeiten, Hilfsmittel und Steuerungen für das Management enthalten, die für eine zuverlässige Bereitstellung der Outputs erforderlich sind.“ [Buchsein2008, S.48]. Außerdem soll ein Prozess die folgenden Merkmale aufweisen:

- Messbar: Die Prozesse sind auf einer spezifischen Art und Weise zu messen und müssen zudem leistungsgetrieben sein.

- Spezifizierte Ergebnisse: Prozesse bestehen, damit ein bestimmtes Ergebnis erzeugt wird. Dieses Ergebnis muss individuell identifizierbar und zählbar sein.

- Anforderungen der Kunden: Jeder Prozess liefert einem Kunden oder einer Anspruchsgruppe seine Ergebnisse. Der Prozess muss außerdem mit den Erwartungen der internen oder externen Kunden übereinstimmen.

- Reagieren auf bestimmte Ereignisse: Da ein Prozess einen fortlaufenden oder wechselseitigen Einfluss hinterlassen kann, sollte er zu einem spezifischen Input verfolgbar sein.

2.1.3 Anspruchsgruppe

In den 60er Jahren wurde der Begriff „Stakeholder“, der auf Deutsch mit „Anspruchsgruppe“ übersetzt wird, erstmals vom SRI (Stanford Research Institute) definiert, und bezieht sich auf „jene Gruppen, ohne deren Unterstützung die Unternehmung aufhören würde zu existieren[1]“ [vgl. Gossy2008, S.5]. Der Begriff „Anspruchsgruppe“ findet heute insbesondere in den Wirtschaftswissenschaften breite Verwendung. Darüber hinaus wurde die Grundidee der so genannten Stakeholder-Value-Konzepte entwickelt, damit die Interessen unterschiedlicher für ein Unternehmen wichtige Gruppen, wie z.B. Kunden, Zulieferer und Mitarbeiter sowie übergeordneter Bezugsgruppen, wie z.B. Gesellschaft und Politik bei der Unternehmensführung berücksichtigt werden können [vgl. Siems2008, S.9].

Eine einheitliche Definition für „Anspruchsgruppe“ lässt sich nicht konkret erfassen, da eine Anspruchsgruppe je nach Betrachtungswinkel bzw. Anwendungsbereich sehr unterschiedlich angesehen werden kann. Obwohl viele verschiedene Definitionen dazu bestehen, bezieht sich eine Anspruchsgruppe generell auf einzelne Personen, Gruppen oder Institutionen und ihre Vertreter, die persönliche, gesellschaftliche, politische Interessen verfolgen oder rechtliche Anforderungen an ein Unternehmen stellen. Dadurch unternehmen sie den Versuch zur direkten bzw. indirekten Beeinflussung von Aktivitäten eines Unternehmens und seiner Manager. Dabei können sie im umgekehrten Fall, selbst von den Handlungen des Unternehmens beeinflusst werden. Die Abbildung 2.1 verleiht einen Eindruck über das komplexe Kräfteverhältnis zwischen einem Unternehmen und seinem Umfeld[2].

[1] „those groups without whose support the organization would cease to exist“ Stanford Research Institute, zitiert nach Freeman and Reed, 1983, S.89
[2] Vgl. www.business-wissen.de

Wichtig für Unternehmen ist, die relevanten Anspruchsgruppen zu erkennen und ihre Anforderungen zu analysieren. Obwohl in dieser Arbeit auf eine detaillierte Analyse hinsichtlich der Anspruchsgruppe für die Informationssicherheit in einem Unternehmen verzichtet wird, ist eine klare Erkennung der Anspruchsgruppe bzw. deren Anforderung für den jeweiligen Informationssicherheitsprozess notwendig.

Abbildung 2.1: Modell des Stakeholder-Konzepts (business-wissen.de)

2.2 Informationssicherheit

Informationssicherheit und IT-Sicherheit werden häufig als identifizierte Begriffe verwendet. In dieser Arbeit werden beide Begriffe jedoch unterschiedlich angesehen, Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die IT-Sicherheit hingegen beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff „Informationssicherheit“ ist im Vergleich zu „IT-Sicherheit“ umfassender und findet daher zunehmend an Verwendung [BSI-Standard, S.12]. Die in dieser Arbeit genannten Informationen umfassen nicht nur jene Informationen, die von der IT

unterstützt werden, sondern z.B. auch die Informationen relevanter Geschäftsprozesse. Aus diesem Grunde wird in dieser Arbeit der Begriff „Informations-sicherheit“ verwendet.

Informationen repräsentieren einen wesentlichen Wert für Unternehmen und Behörden [BSI-Standard, S.12]. Bereits seit mehreren Jahrzehnten ist die Abhängigkeit der Unternehmen von Informationen offensichtlich, als Peter Drucker erläutert, dass aufgrund der Verbreitung der Technologie und die Kommodifizierung der Informationen, die Rolle der Informationen als eine Ressource umgewandelt ist, die genauso wichtig als die klassische Ressource wie Land, Labor oder Kapital ist [Drucker1993]. Heutzutage ist die Informations-Technologie (IT) so hoch entwickelt wie niemals zuvor, für moderne Unternehmen sind Informationen eine Art von Vermögen geworden, inklusive sämtlicher Daten und Systeme, Zertifikate, Best Practices, Regelungen und Standards, die einen besonderen Stellenwert besitzen, und entsprechenden Schutz benötigt.

Allerdings hat sich die Art und Weise der Informationssicherheit, wegen der Entwicklung der IT sich verändert. Am Anfang des 20. Jahrhunderts war die Kryptografie ein Beispiel für die Sicherheitskontrolle. Bis dahin wurde die Information als solches jedoch noch nicht als ein wesentliches Vermögen angesehen. Denn während der 60er Jahre lag der Fokus der Informationssicherheit zunächst auf dem Schutz der Informationsinfrastruktur eines Unternehmens gegen externe Bedrohungen. Seit den 80er Jahren wurden Informationen allmählich als ein kritisches Vermögen betrachtet, zumal sensitive Informationen immer häufiger durch das öffentliche Netzwerk ausgetauscht wurden. Deshalb ist insbesondere in dem heutigen modernen Wirtschaftsleben die Informationssicherheit weniger eine Frage der Technik, sondern eher als eine langfristige Herausforderung für das ganze Unternehmen zu betrachten [vgl. ITS 2009 S.7].

Die Informationssicherheit ist nicht eine einfache und einmalige Funktion, sondern ein ganzheitliches Konzept, welche nach Sloms aus mehreren Aspekten oder Dimensionen entsteht. Denn Informationssicherheit kann nur dann erfolgreich und effektiv in einem Unternehmen gewährleistet werden, wenn alle diese Dimensionen berücksichtigt und implementiert werden. Die wesentlichen Aspekte nach Sloms sind Folgende [ISG2009, S.18]:

- (Corporate) Governance Dimension:

  Die Informationssicherheit stellt eine Teilaufgabe der (Corporate) Governance dar und obliegt dem direkten Verantwortlichkeitsbereich vom Firmenvorstand und Operative Manager. (Corporate) Governance Dimension stellt sicher, dass jeder Mitarbeiter im Unternehmen die entsprechende Verantwortlichkeit für die Informationssicherheit trägt [vgl. ISG2009, S.18f.].

- Organisationsdimension:

  Um die Informationssicherheit in einem Unternehmen erfolgreich zu implementieren, wird eine organisatorische Struktur benötigt. In dieser Dimension werden vor allem die Best Practices für das Informationssicherheit Management gefordert, damit eine organisatorische Struktur für die Durchführung der Informationssicherheit geschaffen werden kann. Außerdem werden in der Organisationsdimension auch die Verantwortlichkeiten der Informationssicherheitsrollen bzw. alle Beziehungen und Kommunikationen untereinander definiert [vgl. ISG2009, S.19].

- Managementdimension:

  Die Managementdimension stellt sicher, dass alle definierten Sicherheitskomponenten existieren und verwendet werden können, um alltägliche Sicherheitsmaßnahmen effizient und effektiv durchzuführen. Während die Governance-Dimension auf der strategischen Ebene beginnt, und alle drei Ebenen

berücksichtigt, ist die Managementdimension für die taktische und operative Ebene verantwortlich [vgl. ISG2009, S.22].

- Politikdimension:

  Die Politikdimension legt die Informationssicherheitspolitik fest, welche das Mandat und das Basis-Referenz-Framework bietet, um die Informationssicherheitskontrolle überhaupt zu ermöglichen [vgl. ISG2009, S.20].

- Gesetzliche Dimension:

  Gesetzliche Anforderungen spielen eine entscheidende Rolle bei der Informationssicherheit. Vor allem in europäischen Ländern steht aufgrund der hohen Bedeutung der Datensicherheit diese Dimension unter besonderer Berücksichtigung [vgl. ISG2009, S.21].

- Risikomanagementdimension:

  Das Risiko zu bewerten und zu behandeln, repräsentiert einen Ausgangspunkt für die Informationssicherheit. Die Risikomanagementdimension stellt sicher, dass alle Risiken für IT Assets von dem Unternehmen bewertet und behandelt werden müssen [vgl. ISG2009, S.19].

- Best Practices Dimension:

  Die Informationssicherheit in einem Unternehmen fordert einen nachvollziehbaren und wiederholbaren Referenz-Framework, der dem Informationssicherheitsmanager bei der Feststellung helfen kann, dass alle Informationssicherheitsaspekte abgedeckt werden können. Dafür werden viele Best Practices-Dokumente angeboten. Ein gutes Beispiel dafür ist ISO/IEC 27002, auch bekannt als ISO 27002 (für nähere Details siehe Kapitel 2.7.3).

- Bewusstseinsdimension:

  Diese Dimension bezieht sich auf die Wichtigkeit des Aspekts der „Menschen“, die die Informationssicherheit widerspiegeln. Durch eine Online-Umfrage des IT-Wirtschaftsmagazins "CIO" wurde im Jahr 2007 gezeigt, dass 66% der befragten CIOs das Personal als den ersten Risikofaktor betrachten [vgl. CIO2007]. Ohne Sicherheitsbewusstsein der Mitarbeiter ist die Einrichtung der hohen Informationssicherheitstechnik sinnlos, genauso als ob, der Wachmann eines hoch sicherheitstechnisch eingerichteten Gebäudes vergessen würde, die Tür abzuschließen [vgl. ISG2009, S.21].

- Technik-Dimension:

  Die Technik-Dimension stellt sämtliche technische Mechanismen sicher, um Risiken, die sich durch einen Angriff gegen technische Lücken äußern, zu verhindern [vgl. ISG2009, S.23].

- Messung/Metrik-Dimension:

  Wenn die Informationssicherheitspolitik nicht überwacht oder gemessen werden kann, um zu bewerten, ob die Politik tatsächlich implementiert wird, dann ist die Informationssicherheitspolitik nicht mehr wert als ein Stück Papier, auf dem die Politik niedergeschrieben wurde. Daher wird die Messung/Metrik-Dimension benötigt, die so eine Messungsumgebung erstellt. Darin werden nicht nur die technischen Aspekte überwacht und gemessen, sondern auch die nicht-technischen Aspekte. Z.B. wird hier über das Niveau des Informationssicherheitsbewusstseins in einem Unternehmen oder das Verhalten der Mitarbeiter bei Sicherheitsvorfällen berichtet [vgl. ISG2009, S.21f.].

2.3 Informationssicherheitsziele

Das Ziel der Informationssicherheit stellt die Gewährleistung der Sicherheit von Informationen dar. Was bedeutet jedoch eigentlich Sicherheit für die Informationen? Um die Informationssicherheit zu charakterisieren, werden folgende drei primäre Merkmale benötigt [vgl.ISM2006, S.8; ITS2007, S.12f.]:

- Vertraulichkeit (*engl. Confidentiality*). Die Informationen können nur von berechtigten Prozessen sowie Systemen eingesehen und zugegriffen werden.
- Integrität (*engl. Integrity*). Die Informationen sind nicht manipuliert. Das heißt, dass die Informationen nicht unbefugt und unbeabsichtigt verändert wurden, so wie es beispielsweise *MalWare* tut.
- Verfügbarkeit (*engl. Availability*). Die Informationen stehen gemäß der eigenen Vorgaben zur Verfügung.

Manchmal werden für die Ergänzung von Hauptmerkmalen noch weitere, so genannte Sekundärmerkmale benötigt. Im Folgenden werden häufige sekundäre Merkmale aufgezählt [vgl.ISM2006, S.8; ITS2007, S.12f.]:

- Zurechenbarkeit (*engl*. Accountability),
- Authentizität (*engl. Authenticity*)
- Qualitätsprüfung bzw. –bestätigung (*engl. Assurance*)
- Verbindlichkeit (*engl. Non-Repudiation*)

Normalerweise werden nur die drei primären Merkmale als Informationssicherheitsziele im Unternehmen definiert. Die sekundären Merkmale könnten aber je nach den spezifischen Anforderungen eines Unternehmens als Sicherheitsziele betrachtet werden.

Die Informationen sind für die Unternehmen erst dann sinngemäß sicher, wenn ihre Vertraulichkeit, Integrität, Verfügbarkeit definiert wurde und diese im geforderten Maße gewährleistet werden können [vgl. ISM2006, S.9].

2.4 Information Security Governance

2.4.1 Begriffsdefinition von Information Security Governance

Um den Begriff Information Security Governance (ISG) näher zu beleuchten, müssen an dieser Stelle zunächst zwei andere Begriffe vorgestellt werden, und zwar Corporate Governance und IT Governance.

Die drei Kategorien von „Governance“ beschäftigen sich alle auf der organisatorischen Ebene des Unternehmens, die die gleichen Ziele verfolgen. Um die Realisierung einer langfristigen Wertschöpfung und Steigerung des Unternehmenswertes zu unterstützen, fokussieren sie sich nur jeweils auf den eigenen Bereich.

Corporate Governance entstand dann als eine Disziplin, als der Besitz einer Organisation von der Verwaltung der Organisation getrennt wurde [Rastogi/Solms2006, S.225]. Corporate Governance soll hier gleichzeitig zwei Perspektiven sichern, nämlich die Wahrung der Entscheidungsfähigkeit des Managements und die Berücksichtigung der Interessen aller Anspruchsgruppen. Corporate Governance liefert dabei den strukturellen Rahmen, in dem einerseits die Beziehungen beispielsweise von dem Management der Organisation mit allen möglichen Anspruchsgruppen verbunden sind, und andererseits die Unternehmensziele, die Identifizierung der Mittel und Wege zu ihrer Umsetzung und die Modalitäten der Erfolgskontrolle festlegt [vgl. OECD2004, S.11].

Eine weitere Definition, die einen neuen Trend setzt, zeigt anhand einer zusätzlichen Dimension, dass Corporate Governance die Anforderung aus gesetzlichen

Vorschriften und national sowie international anerkannten Standards für die Unternehmensführung zur guten und verantwortungsvollen Unternehmenssteuerung und –kontrolle gewährleistet [vgl. Kodex 2005, S. 1].

Insgesamt betrachtet, bedeutet Corporate Governance die Festlegung von Methoden und Verantwortung im Unternehmen. Diese sind von der Geschäftsführung zu unterstützen, um der Weiterentwicklung im Sinne der strategischen Ausrichtung zu genügen. Sie muss gewährleisten, dass Ziele erreicht werden, Risiken angemessen gemanagt und Unternehmensressourcen in verantwortungsvoller Weise eingesetzt werden [ITGI2003b, S. 7].

Darüber hinaus ist aufgrund der immer zunehmenden Abhängigkeit und Bedeutung von IT für das Wirtschaftsleben, die systematische Steuerung und Kontrolle der IT in Unternehmen gefragt. Erfolgreiche Unternehmen erkennen den Nutzen der Informationstechnologie und verwenden sie, um den Stakeholder-Value zu erhöhen [ITGI2005, S.6]. Aus diesem Grund wurden die IT Governance Institute (ITGI) 1998 in Anerkennung der zunehmenden Bedeutung der IT auf den Erfolg des Unternehmens gegründet [vgl. ITGI2006 b].

Die Definition der IT Governance lautet nach ITGI folgendermaßen: IT Governance liegt in der Verantwortung des Vorstands und des Managements und ist ein wesentlicher Bestandteil der Unternehmensführung. IT Governance besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die IT die Unternehmensstrategie und –ziele unterstützt [ITGI2003b S.11].

Information Security Governance liegt auch in dem Verantwortungsbereich des Vorstands und des Managements. Während sich Corporate Governance damit beschäftigt, wie der Vorstand und das Management eines Unternehmens betrieben und kontrolliert werden kann, bezieht sich IT Governance auf die Benutzung und Verwaltung der Informationstechnik, damit sie schließlich die Unternehmensziele unterstützen kann. Information Security Governance stellt eine Kontrolleumgebung

sicher, damit die Risiken hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit aller Informationen bzw. ihrer Unterstützungsprozesse und – systeme verwalt werden [vgl. AISG2003, S.580ff.].

Es gibt mehrere professionelle und offizielle Definitionen der Information Security Governance. Eine Definition der Information Security Governance nach ITGI lautet, dass Information Security Governance ein Bestandteil der Corporate Governance ist, welcher von der Geschäftsführung Unterstützung findet, um der Weiterentwicklung im Sinne der strategischen Ausrichtung zu genügen. Sie muss zudem gewährleisten, dass die Ziele erreicht werden, Risiken angemessen gemanagt, Unternehmensressourcen in verantwortungsvoller Weise eingesetzt und den Erfolg bzw. Misserfolg von Unternehmenssicherheitsprogrammen überwacht. [vgl. ITGI2006 a, S. 17].

Eine genauere Erklärung der Information Security Governance von Sloms lautet: Information Security Governance besteht aus der Verantwortung des Managements und der Unternehmensführung, der organisatorischen Struktur, dem Bewusstsein und der Verantwortung der Benutzer, Strategie, Verfahren, Prozesse, Technologien und die Überwachung- und Kontrollemechanismen. Sie setzen sich alle zusammen, um die Vertraulichkeit, Integrität und Verfügbarkeit der elektronische Vermögen (Daten, Informationen, Software, Hardware, Personen usw.) eines Unternehmens sicherzustellen [vgl. ISG2009, S.24].

Information Security Governance ist von Corporate Governance abgeleitet und weist weite Überschneidungen mit der IT Governance auf. Die Abbildung 2.2 zeigt wie Information Security Governance sich positioniert.

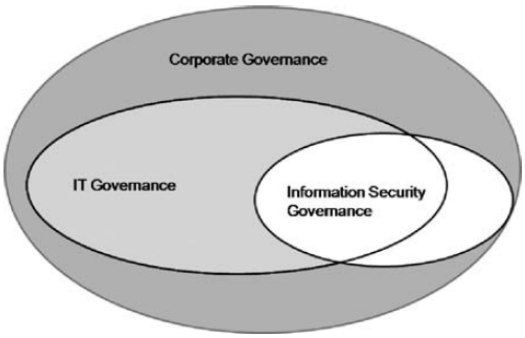

Abbildung 2.2: Position der Information Security Governance (ISG2009)

2.4.2 Bedeutung von Information Security Governance

Im Gegensatz zu unserer heutigen Zeit, hat sich die Gewährleistung der Informationssicherheit früher lediglich auf die Werte der Informationsvermögen sowie auf die Analyse der Risiken konzentriert. Gegenwärtig wird durch die Information Security Governance die Informationssicherheit mit der Auswirkung von Geschäftsabläufen in Verbindung gesetzt [vgl. GIS2007, S.263]. Damit ist die Informationssicherheit nicht mehr als ein reiner Kostenfall vom Vorstand und von Managern des Unternehmens anzusehen, sondern als eine Wettbewerbsstärke, welche die Unternehmensstrategie unterstützt und Profit bringen kann.

Darüber hinaus gewährleistet Information Security Governance auch ein kosteneffizientes Investment für die Informationssicherheit. Ein Null-Risiko soll nicht als Ziel der Implementierung der Informationssicherheit von Unternehmen angestrebt werden. Denn ein unnötiges Investment ist eine Belastung für das Unternehmen, erst durch Information Security Governance werden nach der Risikoanalyse die angemessenen Sicherheitsmaßnahmen angeboten.

Wie bereits in Kapitel 2.2 erläutert, ist Informationssicherheit keinesfalls ein einfacher oder einseitiger Begriff, da sie mehrere Dimensionen impliziert, die alle berücksichtigt und zusammengesetzt werden müssen, damit die Sicherheitsziele des Unternehmens erfüllt werden können. Information Security Governance wirkt als ein

gesamter Framework, welcher sich darum bemüht, dass alle Dimensionen der Informationssicherheit (siehe Kapitel 2.2) berücksichtigt sowie reibungslos und wirksam zusammengesetzt werden können, um eine organisatorische Arbeit zu leiten.

Die Informationssicherheit ist einerseits ein Top-Down und andererseits ein kontinuierlicher Prozess. Es ist unvernünftig zu erwarten, dass die Informationssicherheit von der operativen Ebene aus gut umgesetzt werden kann, ohne das kompetente Verständnis und die Unterstützung von Top-Managern. Ansonsten ist auch festzuhalten, dass ein Bewertungs- und Berichtungsmechanismus bei Informationssicherheitsverfahren eingebettet wird, damit eine kontinuierliche Verbesserung der Aufstellung der Informationssicherheitsstrategie ermöglicht wird. Abbildung 2.3 zeigt das Verfahren der Information Security Governance in begrifflicher Form und die erforderlichen Personen-Komponenten bei der Entwicklung einer Sicherheitsstrategie im Einklang mit den Geschäftszielen. Wie bereits darauf hingewiesen wurde, sichert Information Security Governance einen Top-Down sowie einen kontinuierlichen Prozess und betont vor allem hier die Komponente „Mensch“ beim Informationssicherheitsprozess.

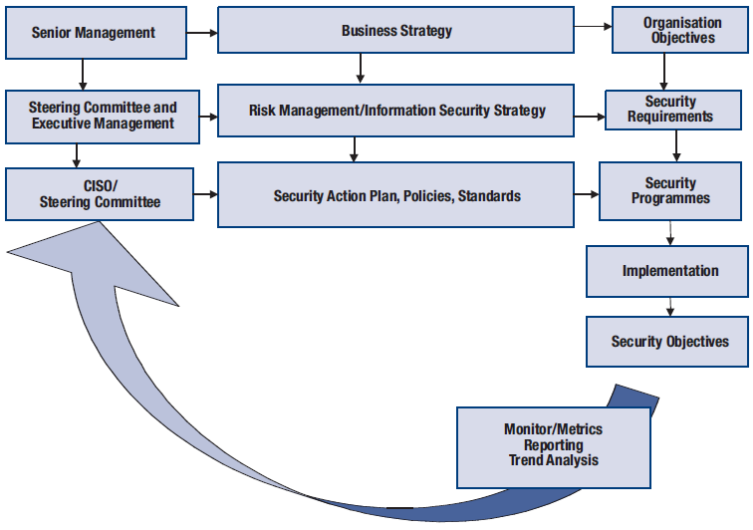

Abbildung 2.3: Konzeptionelle Information Security Governance (ITGI 2006)

2.4.3 Aufgaben der Information Security Governance

Eine wirkungsvolle Information Security Governance soll folgende fünf Ergebnisse ausliefern:

- Strategische Ausrichtung (Strategic Alignment)
- Wertgenerierung (Value Delivery)
- Management von Risiken (Risk Management)
- Management von Ressourcen (Resource Management)
- Leistungsmessung (Performance Measurement)

In den nachfolgenden Unterpunkten werden die einzelnen Aufgaben näher beschrieben.

- **Strategische Ausrichtung (Strategic Alignment)**

Die strategische Ausrichtung impliziert die Bestimmung von Sicherheitsanforderungen mit den Anforderungen des Unternehmens sowie die Integration von Sicherheitslösungen in jeweilige Geschäftsprozesse [ITGI2006a, S.11].

- **Schaffung von Werten (Value Delivery)**

Die Wertgenerierung fokussiert sich auf die Optimierung des Investments in der Informationssicherheit zur Unterstützung der Geschäftsziele [ITGI2006a, S.12]. Ein Wert wird erst dann generiert, wenn die strategischen Ziele durch Sicherheitspraktiken erreicht werden, wie zum Beispiel die Erfüllung der drei primären Ziele der Informationssicherheit, nämlich die Gewährleistung der Vertraulichkeit, der Integrität sowie der Verfügbarkeit. Informationssicherheitsaktivitäten verbrauchen jedoch Ressourcen, deshalb ist ein optimales Investment gefragt, was konkret bedeutet, mit dem geringstmöglichen Einsatz finanzieller Mittel einen akzeptablen Risikorahmen zu schaffen und kontrollierbar zu halten [vgl. ITGI2006a, S.30].

- **Risikomanagement (Risk Management)**

Das Risikomanagement bezieht sich auf den Schutz der Informationsressourcen, wobei Rücksichtnahme zum einen auf den Wiederanlauf nach Katastrophen und zum anderen auf die Fortsetzung der Unternehmensprozesse im Krisenfall gelegt wird. Durch das Risikomanagement wird zunächst sichergestellt, dass die Risiken der Informationsverarbeitung erkannt, verstanden, bewertet und gemäß dem vereinbarten Risikobehandlungsplan behandelt werden. Bei den Risiken, die nicht zu dem vordefinierten Risikobehandlungsplan passen, müssen zwingend gemeldet und erklärt werden. Schließlich sollen mit Hilfe des Risikomanagements geeignete Maßnahmen ausgeführt werden, damit die Risiken gesteuert und gemildert werden bzw. um die zukünftige Auswirkung auf Informationsressourcen auf ein akzeptables Niveau verringern zu können [vgl. ITGI2006a, S.11].

- **Management von Ressourcen (Resource Management)**

Das Ressourcen-Management nimmt sich als Ziel, das Wissen und die Infrastruktur der Informationssicherheit effizient und effektiv zu verwenden [vgl. ITGI2006a, S.11]. Die Gewährleistung der Sicherheit der IT Ressourcen (Menschen, Anwendungen, Technologien, Einrichtungen, Daten) stellen den Schlüsselfaktor für eine erfolgreiche Performance der Informationssicherheit dar [vgl. Sewera2005, S.13].

- **Leistungsmessung (Performance Measurement)**

Die Leistungsmessung stellt durch die regelmäßige Überwachung und Berichtung der Informationssicherheitsprozesse bzw. die Messung der Performance sicher, dass die organisatorischen Ziele erreicht werden [vgl. ITGI2006a, S.30]. Keine Informationssicherheitsziele können erreicht werden, ohne dass die Performance der Informationssicherheit regelmäßig überprüft wird. Die Prüfungen können von einer inneren oder externen unabhängigen Instanz durchgeführt werden, damit die Wirksamkeit und Fortschritte des etablierten Sicherheitsprogramms nach vordefinierten Indikatoren und Metriken beurteilt werden können.

Die Beziehung der obig dargestellten fünf Aufgaben ist aus der Abbildung 2.4 zu entnehmen. Information Security Governance bewegt sich innerhalb einer bestimmten Abfolge, wobei die Festsetzung einer Strategie und ihre Ausrichtung im Unternehmen zunächst im Vordergrund stehen. Die Ergebnisse leisten zudem eine Unterstützung zur Implementierung der Strategie. Dies kann durch die Schaffung von Werten realisiert werden, die einerseits durch die Strategie bestimmt wurden und andererseits durch die Aufklärung von Risiken, die zu minimieren sind, zustande kamen. Zu bestimmten Zeitabständen müssen die Strategie überwacht sowie die Ergebnisse gemessen und berichtet werden. Darüber hinaus müssen die jeweiligen Maßnahmen festgesetzt werden. Die Strategie wird zudem jedes Jahr neu erstellt, beurteilt und ausgerichtet [vgl. ITGI2003b, S.27].

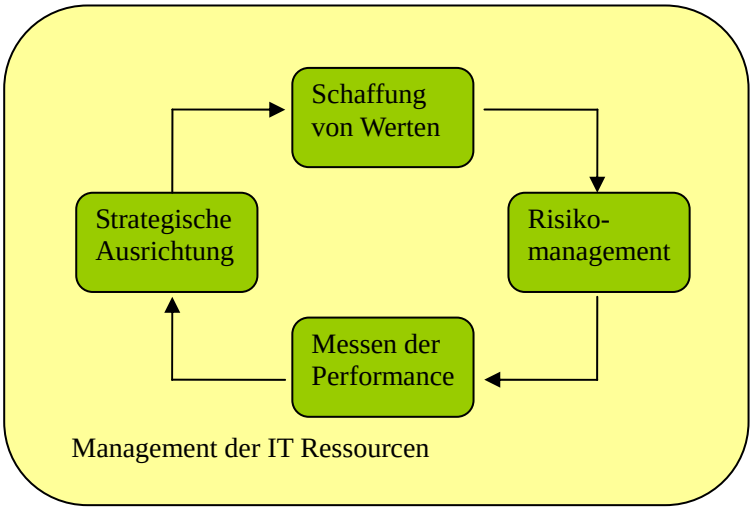

Abbildung 2.4: Aufgaben der Information Security Governance
(eigene Darstellung)

2.5 Referenzmodellierung

2.5.1 Referenzmodell

Ziel dieser Arbeit ist es letztendlich ein Referenzmodell für Information Security Governance zu erstellen, damit die Aktivitäten der Referenzmodelle COBIT, ITIL und ISO 27002 darin zugeordnet werden können. Im weiteren Verlauf der Arbeit wird öfters auf ein zu konzipierendes bzw. zu erstellendes Information Security Governance Referenzmodell verwiesen, deshalb ist es nötig zuerst festzulegen, was genau ein Referenzmodell ist und ob es sich hier überhaupt um ein Referenzmodell handelt. Daher wird an dieser Stelle die Definition des Referenzmodells eingeführt.

Die Definition nach SCHÜTTE besagt, dass ein Referenzmodell eine vom Modellierer hergestellte Konstruktion darstellt, die universellen Elemente und Beziehungen eines Systems als eine Empfehlung erklärt [vgl. Schütte 98, S.69].

Eine weitere Definition nach P. Fettke und J. vom Brocke hat die intendierte bzw. faktische Wiederverwendung als zentrales Charakteristikum betont, das folgendermaßen lautet: Ein Referenzmodell ist ein Modell, das mindestens eine der beiden folgenden Eigenschaften genügt, nämlich die Allgemeingültigkeit und der Empfehlungscharakter. Bei Allgemeingültigkeit heißt es, das Referenzmodell wird beispielsweise nicht nur nach der spezifischen Anforderung von den einzelnen Unternehmen hergestellt, sondern gültig für eine Klasse des Unternehmens (z.B. eine Branche oder ein Konzern).[3] Darüber hinaus wird bei dem Empfehlungscharakter das Referenzmodell gefordert, das zunächst als Basis für die Entwicklung eines unternehmensspezifischen Modells verwendet werden kann, jedoch stets Erweiterungen und Anpassungen an die tatsächliche Unternehmenssituation

[3] Vgl. IT –Vorgehens – und Referenzmodelle: Eine Einführung: http://www.iwi.uni-hannover.de/lv/seminar_ws06_07_de/Koenig_Chr/22wasisteinreferenzmodell.html

vorzunehmen sind.[4]

Dabei ist ein Referenzmodell beispielsweise als ein idealtypisches Fachkonzept zu betrachten, das betriebliche Informationssysteme nach einem bestimmen Integrationsansatz branchenahhängig oder für eine bestimme Betriebsklasse schildert. Ein solches Referenzmodell kann von einem Betrieb dieser Branche verwendet werden, um sein eigenes Fach- sowie DV-Konzept daran anlehnen zu können [Han/Neu, S.332].

Gemäß den oben angegebenen Definitionen, kann Information Security Governance tatsächlich als ein Referenzmodell für die Informationssicherheit konzipiert werden. So wie vorher schon erklärt wurde, enthält Information Security Governance Haupt- sowie Teilaufgaben und Aktivitäten mehrerer Elemente, welche auch miteinander über die Zuordnung in Beziehung stehen. Außerdem ist das Information Security Governance Referenzmodell nicht nur für ein Unternehmen geeignet, sondern für alle Unternehmen, die Sicherheitsanforderungen benötigen. Es bietet daher eine Grundlage für die weitere Entwicklung und ermöglicht auch Anpassungen und Erweitungen je nach der spezifischen Unternehmenssituation.

2.5.2 Modellierungsanforderungen

Die Regeln für eine korrekte angemessene Modellierung wurden im Jahre 1995 zum ersten Mal von Becker, Rosemann und Schütte aufgestellt, damit die Komplexität, die bei der Modellierung entsteht, zu reduzieren bzw. zu beherrschen. Zudem soll dadurch die Qualität von Informationsmodellen gesteigert und gewährleistet werden. Demnach sollen die Richtlinien einer ordnungsgemäßen Modellierung stets weiterentwickelt und vollständig ausgeführt werden. Zurzeit besteht eine Sechs-Grundsätze-Struktur, die als wesentliche Qualitätskriterien bzw. Anforderungen im Rahmen der Modellierung gelten [vgl. Bec97, S.1]. Diese sechs Grundsätze werden mit Hilfe der Abbildung 2.5 dargestellt und näher beleuchtet.

[4] Vgl. http://www.bpm-akademie.de/bpmakademie/opencms/de/Glossar/

Weiterhin werden hier alle sechs Grundsätze kurz vorgestellt, wobei eine genaue Erklärung über die Umsetzung dieser unten dargestellten sechs Grundsätze der Modellierung in Kapitel 4 vorgenommen wird.

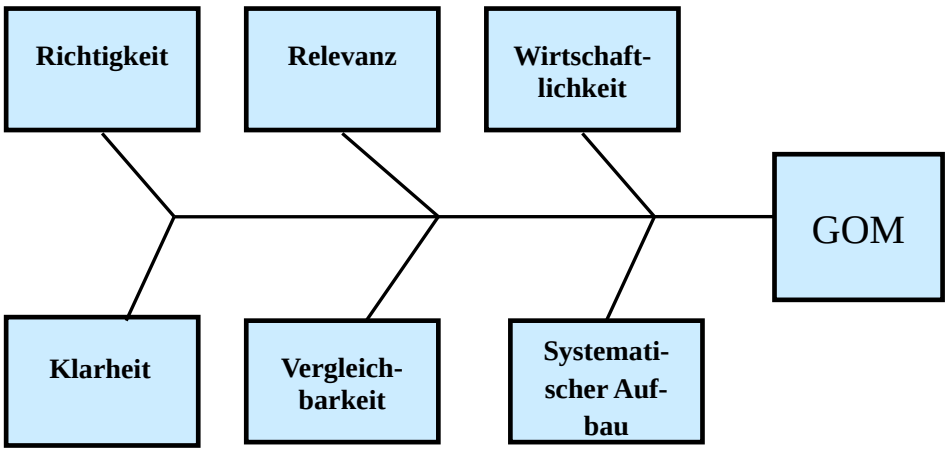

Abbildung 2.5: Grundsätze einer ordnungsmäßigen Modellierung
(Bec97, S.2)

Grundsatz der Richtigkeit

Der Grundsatz der Richtigkeit entspricht der semantischen sowie syntaktischen Korrektheit. In dieser Arbeit geht es insbesondere um die Vollständigkeit der syntaktischen Richtigkeit bzw. der Konsistenz, die der semantischen Richtigkeit zugeordnet wurde.[5] Diese Konsistenz wird hier zudem als Widerspruchsfreiheit verstanden [vgl. Ros96, S.98]. Darüber hinaus muss unter Berücksichtigung der Vollständigkeit, die Modellsyntax, die im Metamodell definiert wurde, auch im Referenzmodell gefordert werden [vgl. Ros96, S.94].

[5] Dabei ist ausdrücklich zwischen der Konsistenz des Modellsystems gegenüber dem Metamodell als Anforderung des Grundsatzes der syntaktischen Richtigkeit und der Konsistenz zu anderen Modellsystemen als Anforderung des Grundsatzes der semantischen Richtigkeit zu differenzieren [Ros96. S. 96].

Grundsatz der Relevanz

Bei der Modellierung ist es unabdingbar, dass die für die Modellierungszwecke relevanten Tatbestände auch tatsächlich im Modell wieder zu erkennen sind [Bec98], das heißt, „das Modell sollte“ nach dem Ziel der Modellierung „so viel Informationen wie nötig und so wenig wie möglich enthalten“ [Ros96, S. 96].

Grundsatz der Wirtschaftlichkeit

Dieser Grundsatz stellt eine wirtschaftliche Modellerstellung sicher, welche vor allem durch die Nutzung von Referenzmodellen oder Maßnahmen zur Wiederverwendung gefördert werden kann [Bec98, S. 4]. Dies spiegelt sich durch die Anpassungs-fähigkeit und Erweiterbarkeit des Modells wider [Ros96, S.96].

Grundsatz der Klarheit

Neben der Richtigkeitsanforderung der Syntax und Semantik, betrifft der Grundsatz der Klarheit die pragmatische Anforderung bezüglich der Beziehung zwischen Modell und Modellnutzer, welche die Anforderungen wie Strukturiertheit, Verständlichkeit, Übersichtlichkeit erfüllen soll [vgl.Ros96, S.99f.].

Hauptsächlich wird die Klarheit eines Modells durch die Erstellung einer Vorschrift für die graphische Darstellung von Elementen bzw. die graphische Anordnung ihrer Beziehungen bestimmt [vgl.Ros96, S.101].

Grundsatz der Vergleichbarkeit

Der Grundsatz der Vergleichbarkeit ist besonders wichtig, weil es eine übergreifende Modellierung ermöglicht, die durch unterschiedliche Modellierer, sogar unterschiedlichen Methoden durchgeführt werden [vgl. Ros96, S.102]. Ein Gesamtmodell, das arbeitsteilig auf Basis unterschiedlicher Metamodelle realisiert wird, kann nur hergestellt werden, wenn die zugrunde liegenden Metamodelle ineinander überführbar sind. Eine weitere Möglichkeit ist, dass der Vergleich von

Modellen auf einem Metamodell beruht, denn dadurch wird eine Modellkonformität durch die Einhaltung bestimmter Richtlinien bezüglich der Verwendung von Bezeichnern und Modellkonstrukten erreicht [vgl. Rau/Sch03, S. 256].

Grundsatz des systematischen Aufbaus

Für eine Modellierung, die auf verschiedene Sichten geht, ist der Grundsatz des systematischen Aufbaus notwendig für die Sichtintegration. Damit eine solche Forderung realisiert werden kann, wird ein sichtenübergreifendes Metamodell benötigt, das die jeweiligen Modelle zum einen klar voneinander abgrenzt und zum anderen Informationsobjekte, die in mehreren Sichten verwendet werden, integriert [vgl. Ros96, S.103].

2.6 Verwendete Werkzuge

2.6.1 Topic Maps

Topic Maps stellen einerseits ein abstraktes Modell und andererseits ein dazugehöriges SGML- bzw. XML-basiertes Datenformat zur Formulierung von Wissensstrukturen dar[6]. Mit Topic Maps ist es möglich, über ein semantisches Netzwerk auf Wissen zuzugreifen [Widhalm2002, S.5].

Erstmalige Ideen zur Erstellung von Topic Maps sind auf die frühen 90er Jahre zu datieren, als Versuche unternommen wurden, Indexe und Indexstrukturen zusammenzuführen. Im Laufe der Zeit gab es jedoch auch Bestrebungen, nicht allein das Zusammenführen von literarischen Indexen in den Vordergrund zu stellen, sondern Glossare, Thesauri, Kreuzverweise, etc. auszuweiten. Erst nach einigen Jahren hat der Begriff Topic Maps für die Konzepte und Bemühungen der ISO-Arbeitsgruppe zum ersten Mal Verwendung gefunden. Im Jahr 1999 wurden Topic Maps als ISO-Standard ISO/IEC 13250 normiert und später als XML Topic Maps (XTM) in XML formuliert [vgl. Widhalm2002, S.5].

[6] http://de.wikipedia.org/wiki/Topic_Maps

Topic Maps stellen ein flexibles Datenmodell dar, das wesentliche 19 Elemente beinhaltet. Dieses Konzept umfasst folgende wichtige Bestandteile[7]:

Topics: Ein Topic repräsentiert ein elementares Subjekt im Kontext des modellierten Wissens, eine Entität. Normalerweise kann es alles Beschreibbare sein, eine Person, ein Gegenstand, eine Zahl, etc [Widhalm2002, S.6]. In dieser Arbeit werden alle Prozesse bzw. Maßnahmen von COBIT, ITIL und ISO 27002 als Topics definiert.

Associations: Associations schildern Beziehungen zwischen Topics. Dabei können beliebig viele Topics an einer Assoziation teilhaben [Widhalm2002, S.11]. In dieser Arbeit werden zwei Assoziationstypen definiert, nämlich die „Korrelation“ und „Überschneidung“, die mögliche Beziehungen zwischen sämtlichen Prozessen bzw. Maßnahmen der drei Standards und Best Practices darstellen.

Occurrences: Topic Occurrences sind Instanzen von oder Dokumente zu Topics. Ein Topic kann zudem beliebig viele Occurrences aufweisen, die Verbindungen zu externen Web-Ressourcen bzw. Dokumenten darstellen [Widhalm2002, S.9]. In dieser Arbeit wird die Beschreibung über die jeweiligen Prozesse bzw. Maßnahmen von COBIT, ITIL und ISO 27002 als Topic Occurrences festgelegt.

In dieser Arbeit werden mit Hilfe von Topic Maps bzw. anhand theoretischer Grundlagen aus den verwendeten Literaturen „Aligning CobiT 4.1, ITIL, V3 and ISO/IEC 27002 für Business Benefit“, „CobiT Mapping, Mapping of ISO/IEC 17799: 2005 with CobiT 4.0“ und „CobiT Mapping, Mapping of ITIL v3 with CObiT 4.1“, die Zuordnungen zwischen den drei Standards bzw. Best Practices, nämlich COBIT, ITIL und ISO 27002 aufgebaut. Dadurch können die Zuorderungen untereinander klar dargestellt werden, wobei auch ein flexibler Zugriff darauf erlaubt ist. Dies schafft eine solide Basis und gute Übersicht für eine weitere strukturierte sowie analytische Arbeit hinsichtlich der Überschneidung und Ergänzung zwischen allen drei Standards und Best Practices unter Berücksichtigung der Informationssicherheit in einem Unternehmen.

[7] http://www.topicmaps.org/xtm/index.html

Im Folgenden werden die Beispieldarstellungen bezüglich der Zuordnung der drei Standards bzw. Best Practices dargestellt. In Abbildung 2.6 wird als Beispiel der Prozess „5.1.1 Leitlinie zur Informationssicherheit“ von ISO 27002 ausgewählt, der dessen Prozesse bzw. sämtliche Prozesse anderer Standards oder Best Practices, die Beziehungen mit ersterem aufweisen, zeigt. Die Beziehungskanten stellen deutlich dar, mit welchen Prozessen der Prozess 5.1.1 von ISO 27002 eine Überschneidung oder aber eine Korrelation aufzeigt.

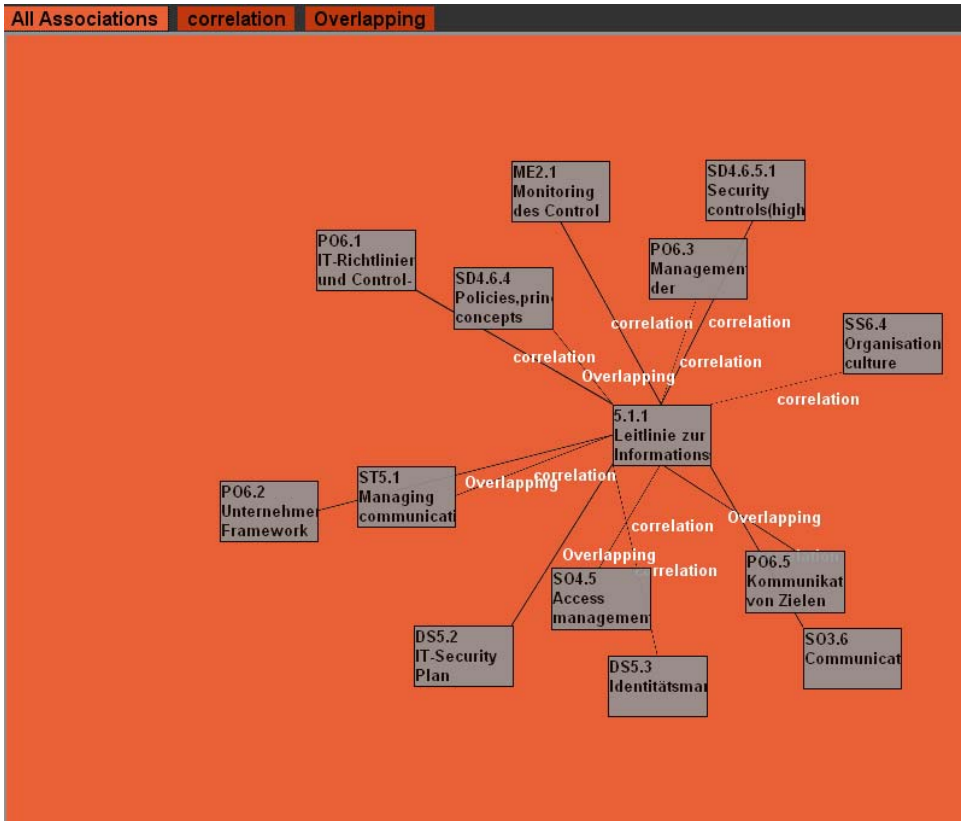

Abbildung 2.6: Beispieldarstellung von Topic Maps (1)

Abbildung 2.7 visualisiert, dass durch das Auswählen der Funktion „Overlapping“ lediglich die Prozesse dargestellt werden, die eine Überschneidung mit dem Prozess 5.1.1 von ISO 27002 aufweisen. Außerdem gibt es eine genaue Beschreibung für jeden Prozess, damit die Eigenschaft bzw. Aufgaben von jedem Prozess eindeutig und übersichtlich angezeigt werden können.

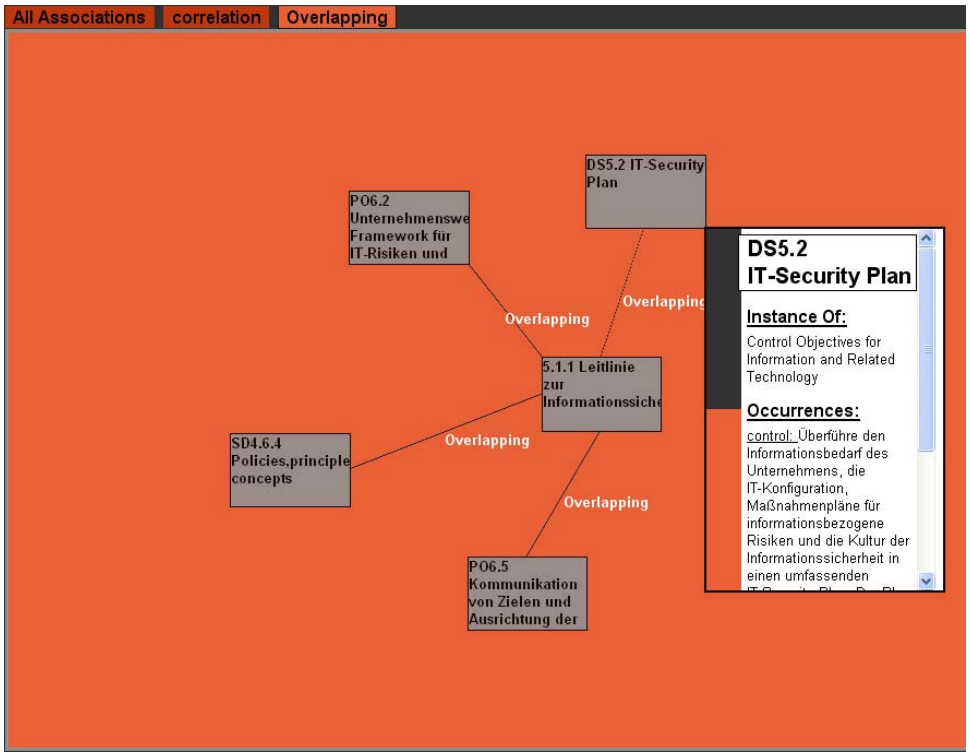

Abbildung 2.7: Beispieldarstellung von Topic Maps (2)

2.6.2 ARIS

Um die Realisierung des Information Security Governance Referenzmodells schaffen zu können, wird in dieser Arbeit der von IDS Scheer entwickelte Ansatz, ARIS (ARchitektur integrierter InformationsSysteme) als Konzept bzw. Softwarewerkzeug ausgewählt, welches eines der bekanntesten und verbreitesten Lösungen für den Bereich der Modellierung und Gestaltung von Geschäftsprozessen darstellt. Es unterstützt die Anforderung zur ganzheitlichen Beschreibung des Informationssystems einer Organisation.

Bei ARIS handelt es sich einerseits um ein Konzept und andererseits um ein Softwarewerkzeug. Als Konzept ist ARIS ein Rahmenwerk zur Beschreibung von Unternehmen und betriebswirtschaftlichen Anwendungssystemen. Dieses Konzept wird in Form eines Softwarewerkzeugs umgesetzt [Sei 2006, S11f.].

2.6.2.1 ARIS – Konzept

Als Konzept ist ARIS ein Rahmenwerk zur Beschreibung von Unternehmen und betriebswirtschaftlichen Anwendungssystemen. Dieses Konzept wird in Form eines Softwarewerkzeugs umgesetzt [Sei 2006, S11f.].

Das ARIS-Konzept wurde von A.W. Scheer entwickelt und in seinem Buch „ARIS – Vom Geschäftsprozess zum Anwendungssystem 1998“ veröffentlich, das zur Reduktion der Komplexität der Geschäftsprozessbeschreibung durch die Strukturierung in Beschreibungssichten und Phasen eines Lebenszyklus-Modells dient. In Abbildung 2.8 wird das Konzept als ARIS-Haus dargestellt. Die Modellierungsmethoden werden zudem in Sichten und Ebenen des ARIS-Hauses eingeordnet [vgl. Scheer 2001, S. 2].

Um die Komplexität des Geschäftsprozesses zu reduzieren, stützt ARIS sich hauptsächlich auf seine eigene Fünf-Sichten-Architektur, welche den dargestellten Gesamtzusammenhang in einzelne Sichten zerlegt. Diese fünf einzelnen Sichten sind

die Organisations-, Daten-, Leistungs-, Funktions- und Steuerungssicht auf einen Prozess. Im Folgenden werden die fünf Sichten kurz vorgestellt:

- **Die Funktionssicht**

Eine Funktion repräsentiert eine fachliche Aufgabe bzw. Tätigkeit an einem Objekt, um ein bzw. mehrere Ziele einer Unternehmung zu unterstützen. Die Funktionssicht enthält zudem sämtliche durchzuführende Funktionen. Damit eine eindeutige Darstellung der Objekte der Funktionssicht und deren Beziehungen gewährleistet werden kann, werden in ARIS die Modelle Funktionsbaum und Zieldiagramm eingesetzt [vgl. Sei 2006, S.15].

- **Die Datensicht**

Die logische Datenstruktur des jeweiligen Anwendungsfalles wird in der Datensicht dargestellt. Dabei muss zumeist eine komplexe Struktur aus Entity-, Attribut- und Beziehungstypen erzeugt werden.

Im Falle von komplexen Zusammenhängen mit hohen formalen Ansprüchen, verwendet die Datensicht das Model „Erweitertes Entity-Relationship-Modell (eERM)“ und deren Varianten. Des Weiteren werden für vergleichsweise einfache Datenstrukturen, das spezifische ARIS-Fachbegriffsmodell benutzt [vgl. Sei 2006, S.18].

- **Die Organisationssicht**

Unternehmen stellen vielschichtige soziotechnische Gebilde dar, die in übersichtliche Einheiten aufgeteilt sind. Dabei werden bestimmte Regeln festgelegt und Ordnungsmuster definiert. Das Ergebnis dieses Ordnungsprozesses wird als Organisation bezeichnet, die sich zum einen in Aufbauorganisation und zum anderen in Ablauforganisation gliedert. Die Aufbauorganisation behandelt die Strukturierung der Aufgaben, der Aufgabenträger und deren Beziehungen, die als Organisationsobjekte in der Organisationssicht gekennzeichnet sind. Das in der Organisationssicht verwendete Modell ist das Organigramm [vgl. Sei 2006, S.19].

- **Steuerungssicht**

Mit der Aufteilung der Prozesse in separate oben genannte Sichten, wird zwar die Komplexität verringert, jedoch werden dadurch auch die Zusammenhänge der Prozesselemente innerhalb der Sichten undeutlich. Um dem entgegenwirken zu können, wird eine zusätzliche Sicht, nämlich die Steuerungssicht eingefügt, in der die Verbindungen zwischen den Sichten nochmal deutlich hervorgehoben werden. Somit können alle Beziehungen systematisch und redundanzfrei festgestellt werden. In der Steuerungssicht können Modelle, wie eEPK (ereiterte ereignisgesteuerte Prozesskette), Funktionszuordnungsdiagramm und Wertschöpfungskettendiagram dargestellt werden [vgl. Sei 2006, S.20].

- **Leistungssicht**

Die Leistungssicht enthält die Ergebnisse der Prozesse und umfasst alle Dienst-, Sach- und finanzielle Leistungen. In der Leistungssicht werden alle materiellen und immateriellen Leistungen eines Unternehmens strukturiert. Als häufig benutztes Modell zur Leistungssicht wird der Produktbaum verwendet.

Weiterhin enthalten alle fünf Sichten drei so genannte „Beschreibungsebenen“, nämlich Fachkonzept, DV-Konzept und Implementierung. Im Fachkonzept werden der Ist- sowie der Soll-Zustand in Modellen formalisiert dargestellt. Es dient als Ausgangspunkt für eine konsistente Umsetzung in eine informationstechnische Anwendung. Die oben genannten Modelle, wie z.B. eEPK, das Organigramm oder Wertschöpfungskettendiagramm, werden je nach genutzter Sicht auf diesen Ebenen beschrieben. In dem DV-Konzept werden die Inhalte des Fachkonzeptes in die Welt der Datenverarbeitung übertragen. Dabei wird die organisatorische Beschreibung der Zustände in die Sprache der Informationstechnik übersetzt. Bei der Implementierung wird das DV-Konzept durch Hardware- und Software-Komponenten verwirklicht [vgl. Sei 2006, S.23f.]. In dieser Arbeit wird eine Beschreibung auf die Ebenen DV-Konzept und Implementierung verzichtet, denn hierbei handelt es sich lediglich um die Modellierung auf der Fachkonzept-Ebene.

2.6.2.2 ARIS – Toolset

Das ARIS-Toolset ist ein international erfolgreiches Softwaresystem zur Analyse, Modellierung und Navigation von Geschäftsprozessen [Scheer 96, S.1]. Darunter werden zwei Softwarewerkzeuge von IDS Scheer AG entwickelt, diese sind einerseits die Vollversion ARIS Toolset und andererseits die einfachere Version mit dem Namen ARIS Easy Design. Damit kann das ARIS-Konzept umgesetzt werden.

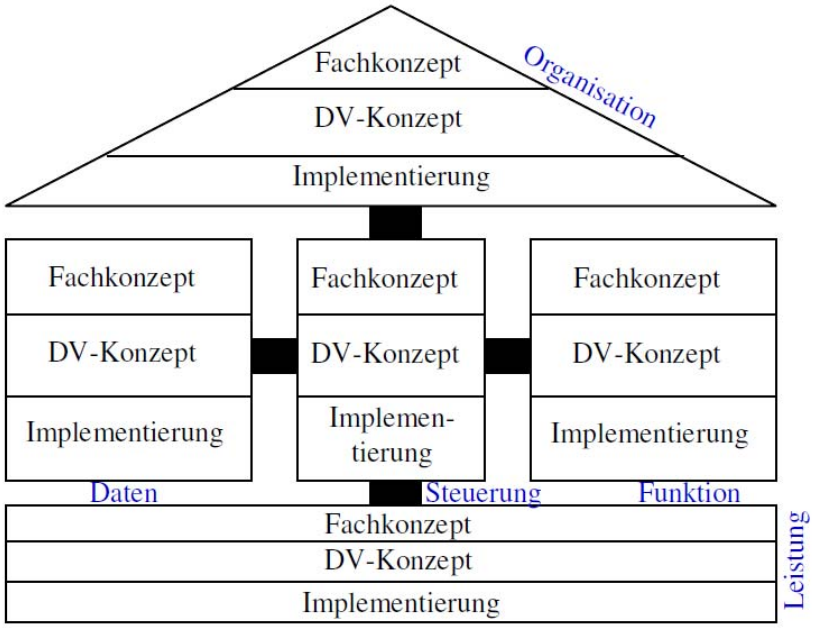

Abbildung 2.8: ARIS-Haus (Scheer, 1998)

2.6.2.3 Verwendete Symbole

In diesem Abschnitt werden die in dieser Arbeit verwendeten Symbole grafisch dargestellt und kurz erläutert [vgl. Sei2006, S26ff.].

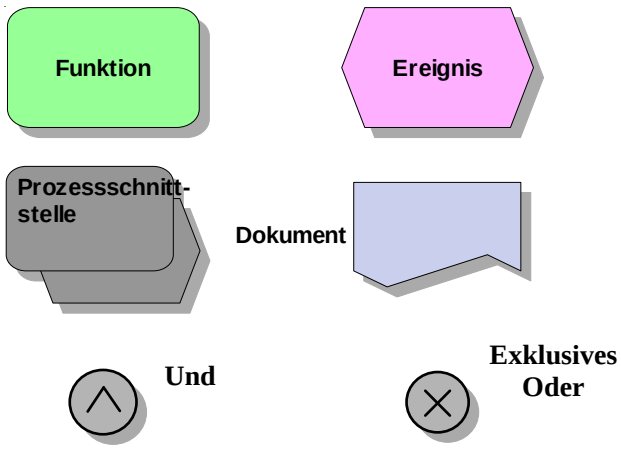

Abbildung 2.9: Häufig verwendete ARIS Symbole zur Funktions- und Prozessmodellierung

Funktion: Eine Funktion (in ARIS) ist eine fachliche Aufgabe bzw. Tätigkeit an einem Objekt zur Unterstätzung eines oder mehrerer Unternehmensziele.

Ereignis: Ein Ereignis (In ARIS) beschreibt einen eingetretenen Zustand.

Prozessschnittstelle: Verweis auf andere Prozesse

Dokument: Ein Dokument ist eine für den menschlichen Gebrauch aufbereitete Einheit an gespeicherter Information, die entweder von dem Prozess selber erzeugt wird oder die Verarbeitung des Prozesses als Informations- bzw. Wissensquelle unterstützt.

Und: Die Ereignisse bzw. Funktion treffen alle ein

Exklusives Oder: Nur ein Ereignis darf zutreffen, sich gegenseitig ausschließende Alternativen können modelliert werden

2.6.2.4 Verwendete Modelle

Um das Information Security Governance Referenzmodell bzw. die Zuordnung der drei Standards und Best Practices in ARIS umsetzen und darstellen zu können, werden hier hauptsächlich zwei Modelltypen verwendet, diese sind Wertschöpfungskettendiagramm (WSD) und ereignisgesteuerte Prozesskette (EPK).

Im Folgenden werden die zwei Modelltypen näher erläutert.

Wertschöpfungskettendiagramm

Das Wertschöpfungskettendiagramm (WSD) stellt die Prozesse der oberen bzw. strategischen Unternehmensebenen dar, und dient zur Veranschaulichung der Kern- und Unterstützungsprozesse einer Organisation. Kernprozesse stellen die Prozesse dar, die eine hohe Wertschöpfung für den Kunden besitzen. Unterstützungsprozesse hingegen repräsentieren die Prozesse, die entweder keine oder lediglich eine geringe kundenbezogene Wertschöpfung aufweisen, jedoch zur Verwirklichung der Kernprozesse unabdingbar sind [vgl. Sei 2006, S.71]. In dieser Arbeit werden die Kernprozesse als Prozesse verstanden, die Informationssicherheitsanforderungen von Kunden direkt gewährleisten können.

Weiterhin wird das WSD zum Einstieg in die Geschäftsprozessmodellierung genutzt, um die relevanten Sachverhalte zu bestimmen. Außerdem ist es mit Hilfe von Hinterlegungen möglich, eine detaillierte Darstellung von Wertschöpfungsketten (WSK) oder ereignisgesteuerten Prozessketten (EPK) zu modellieren.

Ereignisgesteuerte Prozesskette

Anhand von Wertschöpfungskettendiagrammen lassen sich große Zusammenhänge oder Prozesse gut modellieren, jedoch ist für eine detaillierte Ansicht eine ereignisgesteuerte Prozesskette (EPK) effizienter. Ein EPK besteht prinzipiell aus Funktionen, Ereignissen und Verknüpfungsoperatoren. Falls die EPK von den Elementen aus der Organisations-, Daten- und Leistungssicht erweitertet werden muss, benötigt es die so genannte erweiterte ereignisgesteuerte Prozesskette (eEPK), auf die jedoch in dieser Arbeit verzichtet werden soll.

Die Erstellung von EPKs erfordert folgende Regeln [Rau/Sch 2003, S. 246]:

- Funktionen dürfen nicht direkt mit Funktionen verknüpft werden.
- Ereignisse dürfen nicht direkt mit Ereignissen verknüpft werden.
- Konnektoren dürfen nicht mit Konnektoren verknüpft werden.

- Konnektoren, Ereignisse und Funktionen werden über Kontrollflüsse miteinander verbunden.
- Jede Prozesskette muss mit mindestens einem Ereignis beginnen und enden.
- Einem Ereignis darf weder eine disjunktive noch adjunktive Verknüpfung folgen, da Ereignisse keine Entscheidungskompetenz haben und Modelle ohne exogene Informationen erklärbar sein müssen.

2.7 Standards und Best Practices

Standards oder Best Practices sind normalerweise Dokumentationen, welche die optimale Lösung oder Verfahrensweise erhält, die zu Spitzenleistung führen und als Modell für eine Übernahme in Betracht kommt [Lektion 2009].

Wie bereits in Kapitel 2.2 erläutert, erhält die Informationssicherheit die Best Practices-Dimension. Das heißt, es wird ein Referenzmodell für die Informationssicherheit gefordert, um dem Sicherheitsmanager dabei zu helfen, dass sie einerseits eine Übersicht über sämtliche Sicherheitselemente des Unternehmens schaffen, und andererseits auch nach einer Rechtlinie für die Informationssicherheit nachfolgen können. Deshalb sind mehrere Referenzmodelle für die Information Security Governance verfügbar, damit die Informationssicherheit gewährleistet werden kann. Eine der international anerkannten Best Practices repräsentiert ISO 27002 (*code of practice for information security*).

Darüber hinaus wird aufgrund der zunehmenden Bedeutung der IT für den Unternehmenserfolg das IT-Governance-Modell von vielen Unternehmen übernommen, um eine umfassende Steuerung und Kontrolle des Unternehmens zu gewährleisten. Dadurch könnte auch das volle Potential seiner Informationen ausgeschöpft werden. Damit dieser Ansatz weiter unterstützt und konkretisiert werden kann, wurden mit Hilfe verschiedener Institutionen Modelle mit differenzierten Schwerpunkten entwickelt: COBIT als Referenzmodell für die Implementierung von

IT Governance, und ITIL als Best Practices für das IT-Service-Management [vgl. Sewera2005, S.2].

Information Security Governance zeigt viele weite Überschneidungen mit IT Governance auf (siehe Kapitel 2.4.1), das heißt, obwohl die vorgelegten drei Referenzmodelle, also ISO 27002, COBIT und ITIL alle über ihre eigenen Anforderungen und Perspektiven verfügen, haben viele Prozesse der drei Referenzmodelle jedoch ähnliche oder sogar identische Prozesse oder Ziele. Sie besitzen beispielsweise all jene Prozesse, die sich mit der Behandlung von Sicherheitsvorfällen, dem Management der Änderungen oder der kontinuierlichen Verbesserung beschäftigen. Es stellt eine große Herausforderung für die Unternehmen, denn sofern ISO 27002 als Referenzmodell für Information Security Governance in das Unternehmen eingefügt wird, müssen die bereits im Unternehmen eingesetzten Referenzmodelle, die die Implementierung der IT Governance ermöglichen, integriert werden. Schließlich soll ein Referenzmodell als gemeinsamer Rahmen für die Informationssicherheit hergestellt werden, das einerseits mögliche Anforderungen mehrerer Standards und Best Practices erfüllt, aber anderseits auch Überschneidungen und unnötige Wiederholungen mehrerer Referenzmodelle vermeiden soll.

Im Folgenden werden zunächst die drei ausgewählten Referenzmodelle, nämlich COBIT, ITIL, und ISO 27002 inhaltlich näher beschrieben. Im Kapitel 3 erfolgt anschließend eine Zuordnung zu den Aufgaben der Information Security Governance.

2.7.1 COBIT

2.7.1.1 Eine allgemeine Einführung

COBIT als Begriff steht dabei für **C**ontrol **Ob**jectives of **I**nformation and related **T**echnology, welche die Entwicklung von allgemein akzeptierten Kontrollzielen für die Information und die damit verbundene Technologie als Ziel setzt [vgl. Goltsche 2006. S.11].

COBIT liegt mittlerweile in der vierten Version vor, die eine Sammlung von Dokumentationen darstellt, und vom internationalen Prüfungsverband ISACA (Information Systems Audit and Control Association) seit dem Jahr 1993 stets weiterentwickelt wurde. Die erste Version von COBIT wurde 1996 von der ISACF (Information Systems Audit and Control Foundation), dem Forschungsinstitut der ISACA veröffentlicht. Im Mai 1998 erschien die zweite Version, welche eine komplett überarbeitete und erweiterte Version mit 34 IT-Prozeesen und 300 Kontrollzielen darstellte. Seit der dritten Version (veröffentlicht im Juli 2000) wird COBIT vom IT Governance Institut herausgegeben. In dieser Version wurde COBIT im Wesentlichen um relevante Aspekte der IT Governance erweitert. Die letzte Version ist derzeit V4.0 (Jan. 2006), wobei das aktuellste Update COBIT 4.1 (Mai 2007) darstellt [vgl. Goltsche 2006, S.12; vgl. AISG 2003, S.20].

COBIT wurde ursprünglich als eine Methode zur Auditierung gedacht, welche nur von Auditoren, Endanwendern und dem Management angewandt werden konnte. Heute stellt COBIT eine Sammlung von Veröffentlichungen dar, die als allgemein anerkanntes internes Kontroll-Rahmenwerk für die IT bezeichnet werden kann. Die Zielgruppen sind somit alle betroffenen Anspruchsgruppen wie Direktoren, das obere Management, die Eigner von Prozessen, Anwender, IT-Lieferanten, Auditoren, etc. [vgl. Goltsche2006, S.12; vgl. AISG2003, S.20].

COBIT ist auf der strategischen Ebene anzusiedeln, und stellt ein international anerkanntes Kontroll-Framework bzw. unterstützendes Werkzeug dar, welche die Implementierung der IT Governance unterstützt, um sicherzustellen, dass die benutzte Informationstechnologie die Geschäftsziele abdeckt, die die Ressourcen verantwortungsvoll einsetzt und die Risiken entsprechend überwacht [vgl. Sewera 2005, S. 20].

Außerdem wurde COBIT durch Forschungsprojekte an andere IT Standards und Best Practices angepasst und mit diesen harmonisiert (z.B. ITIL). Unter COBIT werden diese unterschiedlichen Standards und Best Practices in einem gemeinsamen Rahmen

integriert [vgl. ITGI 2005, S.8].

2.7.1.2 Inhaltliche Beschreibung

Das Hauptthema von COBIT bezieht sich auf die Unternehmensorientierung, deswegen lautet das Prinzip des COBIT-Frameworks folgendermaßen: Alle IT-Aktivitäten zielen auf die Unterstützung der Geschäftsziele mit Hilfe von IT-Ressourcen [vgl. ITGI 2005, S.14].

Das COBIT-Framework richtet sich nach Prozessen. Dabei wird nicht nur jeder IT-Prozess definiert, sondern sowohl die Geschäftsziele, die durch diesen Prozess unterstützt werden sollen, als auch die Kontrollziele für diesen Prozess. Folgende sieben Kategorien von Geschäftsanforderungen werden für die Festlegung der Kontrollziele aufgestellt: Die klassischen Sicherheitsanforderungen Vertraulichkeit, Verfügbarkeit, Integrität, Effektivität (Wirksamkeit), Effizienz (Wirtschaftlichkeit) sowie Ordnungsmäßigkeit (Einhaltung rechtlicher Erfordernisse) und Zuverlässigkeit (Ordnungsmäßigkeit der Berichterstattung) [vgl. Sewera2005, S. 23].

Die Struktur der Kontrollziele stützt sich auf ein prozessorientiertes Geschäftsmodell. Geschäftprozesse wiederum basieren laut COBIT auf IT-Ressourcen, Daten, Anwendungen, Technologien, Anlagen und auf das Personal [vgl. Sewera 2005, S. 23].

Die für die Geschäftsprozesse notwendigen Mitarbeiter, Daten, Anwendungen, Technologien und Anlagen müssen kontrolliert geplant, entwickelt, implementiert, betrieben und überwacht werden. COBIT definiert dazu 34 kritische Prozesse mit derzeit insgesamt 210 Aktivitäten, die in vier Domänen aufgliedert werden. Diese Domänen sind [vgl. Sewera 2005, S. 23]:

1. „Plan and Organize“ (Plane und Organisiere: PO), diese Domäne enthält 10 Prozesse und umfasst die Strategie und Taktik und betrifft die Bestimmung der Art, wie die Informationstechnologie am besten zur Erreichung der Geschäftsziele

beitragen kann. Weiterhin muss die Realisierung der strategischen Vision für unterschiedliche Aspekte geplant, kommuniziert und geleitet werden. Schließlich muss eine geeignete Organisation wie auch eine technologische Infrastruktur bereitstehen [vgl. Sewera 2005, S. 23].

2. „Acquire and Implement“ (Beschaffe und Implementiere: AI), diese Domäne enthält 7 Prozesse, die IT-Lösungen identifizieren, entwickeln, beschaffen und implementieren, aber auch Veränderungen und die Wartung von bestehenden Systemen abdecken [vgl. Sewera 2005, S. 23].

3. „Deliver and Support“ (Erbringe und Unterstütze: DS), diese Domäne enthält 13 Prozesse und betrifft die effektive Bereitstellung der gewünschten Dienstleistungen, die vom traditionellen Betrieb über Sicherheits- und Kontinuitätsfragen bis hin zur Ausbildung reichen. Zum Betrieb von Dienstleistungen müssen die notwendigen Unterstützungsprozesse etabliert werden. Diese Domäne beinhaltet auch die eigentliche Datenverarbeitung durch Anwendungen [vgl. Sewera 2005, S. 24].

4. „Monitor and Evaluate“ (Überwache und Beurteile: ME), die Domäne enthält 4 Prozesse, welche die Anforderungen der regelmäßigen Überprüfung aller Kontrolleprozesse auf ihre Qualität und auf die Erreichung der Kontrollziele erreichen können [vgl. Sewera 2005, S. 24].

Zusammen mit den oben angegebenen COBIT-Elementen lässt sich folgender Kreislauf des gesamten COBIT-Referenzmodells darstellen. Eine Übersicht über sämtliche COBIT-Prozesse und die dazugehörigen detaillierten Kontrollziele befinden sich im Anhang A.

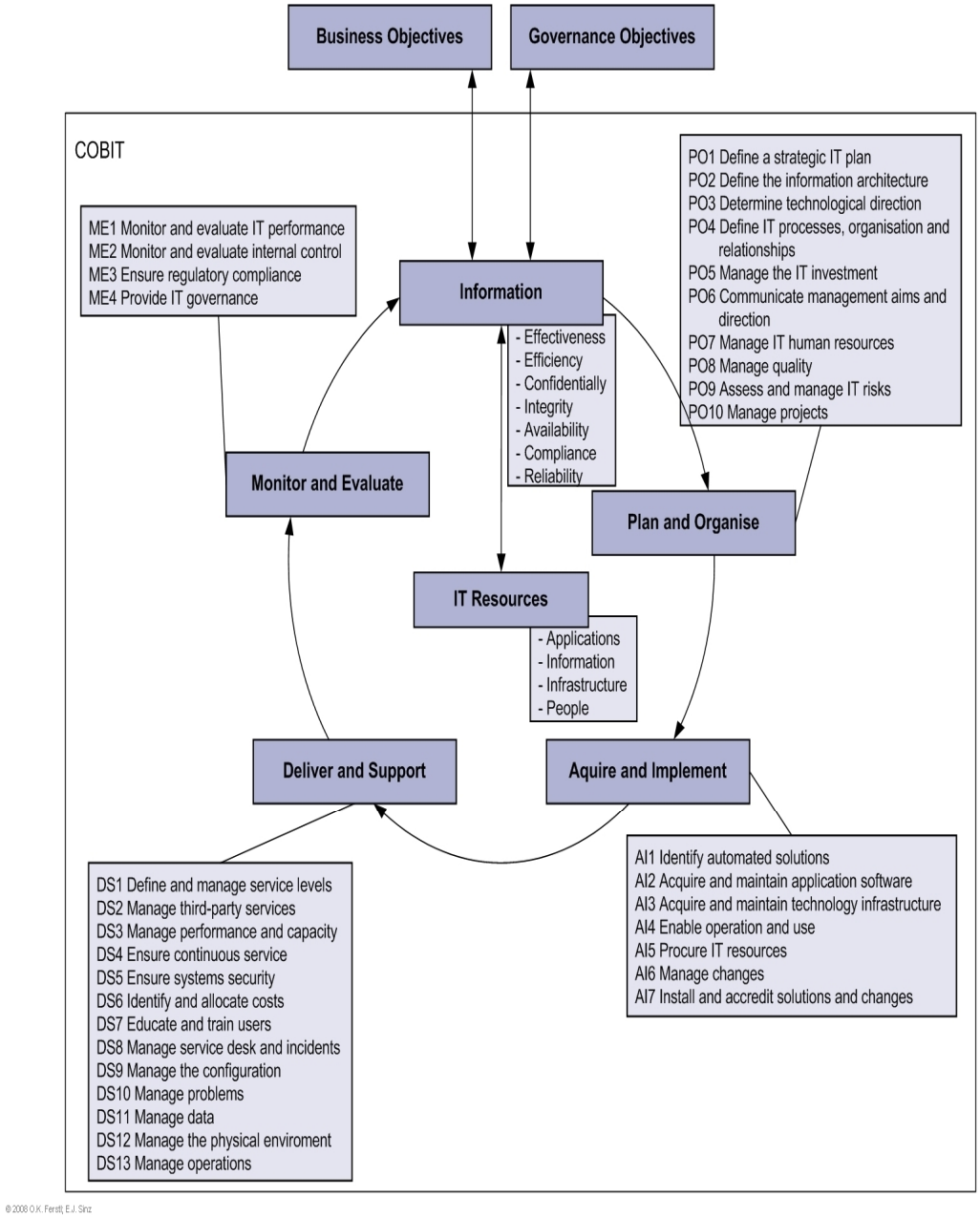

Abbildung 2.10: Vollständiges COBIT-Referenzmodell
(ITGI 2007b)

2.7.2 ITIL

2.7.2.1 Allgemein

ITIL steht für **I**nformation **T**echnology **I**nfrastructure **L**ibrary und ist ein öffentlich zugänglicher und herstellerunabhängiger Best Pracitces-Leitfaden, der durch die Praxis gewonnene Erkenntnisse, Architekturen und Modelle darstellt, die wiederum als Richtlinie für den systematischen Aufbau sowie den Betrieb einer durchgängig abgestimmten professionellen IT-Servciestruktur verwendet werden können. Von zentraler Bedeutung sind dabei die Serviceorientierung und die Kundenzufriedenheit [vgl. Olbrich 2008, S.1ff.].

ITIL wurde in den 80er Jahren durch die „Central Computer and Telecommunications Agency“ (CCTA) von der britischen Regierung, welche im Laufe der Jahre in OGC (Office of Government Commerce) umbenannt wurde, entwickelt, um die eigenen IT-Ressourcen des öffentlichen Sektors effizienter und kosteneffektiver nutzen zu können. Die Vereinheitlichung der Ergebnisse der Analysen wurde ITIL genannt und in verschiedenen Büchern definiert [vgl. Stych/Zeppenfeld 2008, S.11].

Die erste Version bzw. Revision der Bibliothek oder Büchersammlung wurde im Jahre 1995 abgeschlossen. Die zweite Version wurde im Jahr 1999 veröffentlicht, die aus sieben Kernpublikationen und einem ergänzenden Teil besteht, welche das IT-Service-Management hauptsächlich als Service Support und Service Delivery betrachtet. Seit Ende 2007 existiert ITIL in der dritten Revision, in der ITIL insgesamt fünf Kernelemente, und eine umfangreiche Einführung beinhaltet. Eine der wesentlichen Unterschiede zur Version 2.0 ist die deutlich stärkere Fokussierung auf den Service-Lebenszyklus. An dieser Stelle ist besonders zu betonen, dass unter einem Service-Lebenszyklus nicht verstanden wird, dass der Service selbst einen Lebenszyklus besitzt, sondern die Verwaltung des Services unendlich ist und kontinuierlich verbessert werden soll.

ITIL wird heute weltweit als de-facto-Standard für IT-Service-Management angesehen, der Prozesse, Aufgaben, Rollen und Abhängigkeiten in einem Unternehmen klar festlegt, aber nicht deren Umsetzung genauer definiert. ITIL liefert weder Implementierungsvorschriften oder Formularvorlagen, noch werden irgendwelche Tools von bestimmten Herstellern bevorzugt [vgl. Olbrich 2008, S.1].

2.7.2.2 Inhaltliche Beschreibung

Den Kern des neuen ITIL V3 Frameworks bilden fünf Kerngebiete, denen jeweils ein eigener, einheitlich strukturierter Band gewidmet ist [Olbrich 2008, S.144]. Diese Kerngebiete sind:

- Service Strategie (*engl. Service Strategy*, SS) befasst sich mit der Konzeption und Strategie von Service-Prozessen, die Definition, Spezifikation, Logistik und finanzielle Aspekte aus der Geschäftsperspektive umfassen, und sich durch den gesamten Lebenszyklus des IT-Service-Managements von ITIL vollzieht.[8]

- Modelle für den Betrieb (*engl. Service Design*, SD) befassen sich mit den architektonischen Rahmenbedingungen zur Entwicklung, die Definition, Spezifikation, Logistik und Sicherheitsaspekte aus der operativen Perspektive umfassen.[9]

- Service Implementierung bzw. Einführung (*engl. Service Transition*, ST) behandelt die praktische und faktische Umsetzung und Übertragung der geschäftlichen Anforderungen in konkrete IT-Dienstleistungen.[2]

- Operativer Betrieb (*engl. Service Operation*, SO) beschreibt den operativen Teil, der notwendig ist, um die vereinbarte Leistung beim alltäglichen Betrieb möglichst störungsfrei aufrecht zu erhalten und zu sichern.[2]

[8] http://de.wikipedia.org/wiki/ITIL
[9] http://de.wikipedia.org/wiki/ITIL

- Die kontinuierliche Verbesserung von Services (*engl. Continual Service Improvement,* CSI) beschäftigt sich mit der Optimierung der Servicequalität und umfasst Methoden der Festlegung und Einführung von Leistungsparametern sowie Messgrößen, die Überwachung von Zielvereinbarungen, die Identifikation von Schwachpunkten und die Umsetzung von Service-Verbesserungen.[2]

Zusammenfassend lässt sich festhalten, dass „Service Strategy“ die Achse definiert, um die der Lebenszyklus sich bewegt. Dabei werden die Richtlinien und Ziele festgelegt, die mit „Service Design“, „Service Transition“ und „Service Operation“ von der Planung über die Änderung bis hin zur Inbetriebnahme realisiert werden. Das „Continual Service Improvement“ impliziert ein konstantes Lernen und eine ständige Verbesserung und hilft zudem Verbesserungsprogramme und –projekte auf Basis der strategischen Ziele zu platzieren und zu priorisieren.[10] Die Abbildung 2.11 zeigt die Beziehung innerhalb der fünf Kernelemente bzw. den Service-Lebenszyklus.

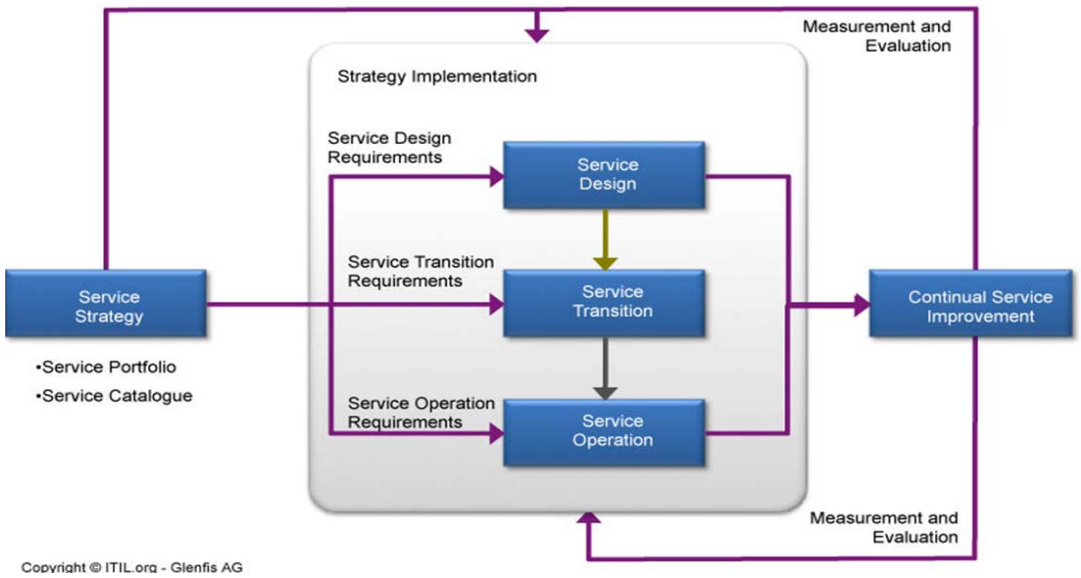

Abbildung 2.11: Service-Lebenszyklus (www.itil.org)

[10] www.itil.org

2.7.3 ISO 27002

2.7.3.1 Allgemein

Die ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management ist eine Überarbeitung der ISO/IEC 17799:2000, die aus dem British Standard BS 7799-1:2000 hervorging. Um eine einheitliche Namensgebung zu verwenden, wurde im Juli 2007 der Standard in ISO/IEC 27002:2005 umbenannt [Müller 2008, S28]. In dieser Arbeit werden diese Bezeichnungen deshalb als Synonym verwendet und abgekürzt (ISO/IEC 27002 oder ISO 27002).

Der weltweit akzeptierte Standard ISO 27002 gehört zur Normenreihe ISO 2700x und beschäftigt sich mit den Kontrollmechanismen, deren Methoden und Verfahren, die sich in der IT-Sicherheit bewährt haben. Viele Unternehmen verwenden ISO 27002 als eine allgemeine Richtlinie oder ein Rahmen für ihr Information Security Management. Jedoch werden in dem Standard keine konkreten Sicherheitslösungen empfohlen, allerdings sollten Unternehmen und Organisationen aller Branchen die im Standard aufgeführten Richtlinien beachten und umsetzen.[11]

Zu Beginn der 90er Jahre wurde eine Arbeitsgruppe eingerichtet, die aus Informationssicherheits-Praktikern mehrerer großer Unternehmen bestanden und aus Großbritannien stammen, um die Anforderung der Erstellung einer Art von Leitfaden für das Management der Informationssicherheit zu reaktiveren. Im Jahre 1993 wurde das erste Dokument „A Code of Practice for Information Security Management“ von der Arbeitsgruppe erstellt. Dieses Dokument wurde im Jahr 1995 durch das British Standards Institute (BSI) als Standard mit dem Namen BS 7799 angenommen. Daraufhin fand dieses Dokument im Bereich Informationssicherheitsmanagement eine sehr schnelle und weite Verbreitung [vgl. ISG 2009, S.43ff.].

[11] IT Wissen, Das große Online-Lexikon für Informationstechnologie: http://www.itwissen.info/definition/lexikon/ISO-27002-ISO-27002.html

Gegen Ende der 90er Jahre wurde ein weiteres Dokument erstellt, das als BS 7799-2 bezeichnet wird, und den spezifischen Anforderungen gemäß der Zertifizierung des originalen BS 7799 entspricht. Daher wurde das Original BS 7799 in BS 7799-1 umbenannt [vgl. ISG 2009, S.43ff.].

Aufgrund der breiteren Nutzung von BS 7799-1 wurde das Dokument an die International Standards Organization (ISO) weitergeführt. Durch den so genannten „Fast Tracking“ - Prozess wurde BS 7799-1 im Jahr 2000 als ISO 17799 akzeptiert. Zu der Zeit wurde BS 7799-2 noch nicht zu einem ISO-Standard. Im Jahr 2005 wurde ISO 17799 überarbeitet und ist derzeit die neueste Version. Im Jahr 2007 wurde ISO 17799 in ISO 27002 umbenannt, wobei der Inhalt identisch geblieben ist [vgl. ISG 2009, S.43ff.].

Im gleichen Zeitraum wurde BS 7799-2 auch der International Standards Organization (ISO) vorgelegt, das schließlich als ISO 27001 anerkannt wurde [vgl. ISG 2009, S.43ff.].

Eine Zertifizierung entsprechend dem ISO-Standard zur Informationssicherheit kann nur auf der Basis von ISO 27001 stattfinden. Da dieser Standard auf den ISO 27002 Standard Bezug nimmt, muss ISO 27002 bei einer Zertifizierung unbedingt beachtet werden. Eine ausschließlich auf den ISO 27002 Standard ausgerichtete Zertifizierung, kann ohne Berücksichtigung des ISO 27001 Standards nicht realisiert werden.

2.7.3.2 Inhaltliche Beschreibung

Der Standard ISO 27002 besteht aus 11 Überwachungsbereichen mit insgesamt 39 Sicherheitskategorien, zu jeder Sicherheitskategorie ist ein Kontrollziel angegeben. Diese sind mit insgesamt 133 Sicherheitsmaßnahmen untersetzt, deren Anwendung die Erreichung der Kontrollziele unterstützt.[12]

[12] http://de.wikipedia.org/wiki/ISO/IEC_27002

Im Folgenden werden die 11 Überwachungsbereiche dargestellt, die weiteren zugeordneten Sicherheitskategorien bzw. Sicherheitsmaßnahmen jeweiliger Bereiche befinden sich im Anhang C [ITSM2008]:

1. Sicherheitsleitlinie (*Information Security Policy*)
2. Organisation der Informationssicherheit (*Organization of information security*)
3. Management von organisationseigenen Werten (*Asset management*)
4. Personalsicherheit (*Human resources security*)
5. Physische und umgebungsbezogene Sicherheit (*Physical and Environmental Security*)
6. Betriebs- und Kommunikationsmanagement (*Communications and Operations Management*)
7. Zugangskontrolle (*Access Control*)
8. Beschaffung, Entwicklung und Wartung von Informationssystemen (*Information systems acquisition, development and maintenance*)
9. Umgang mit Informationssicherheitsvorfällen (*Information security Incident management*)
10. Sicherstellung des Geschäftsbetriebs (*Business Continuity Management*)
11. Einhaltung von Vorgaben (*Compliance*)

Kapitel 3

Ist-Analyse

Im folgenden Kapitel wird zunächst erläutert, auf welcher Basis die Standards bzw. Best Practices nämlich COBIT, ITIL und ISO 27001 sich miteinander zuordnen lassen, und gleichzeitig Information Security Governance unterstützen können. Weiterhin wird die Zuordnung von COBIT, ITIL und ISO 27002 unter Information Security Governance tabellarisch dargestellt, um anschließend eine Grundlage für den Aufbau eines Referenzmodells für Information Security Governance mit ARIS zu erstellen.

3.1 Grundlagen der Zuordnung

In dieser Arbeit wird Information Security Governance, wie bereits in Kapitel 2.4.1 erwähnt, als ein Framework für Informationssicherheit betrachtet. Framework bedeutet hier, eine Struktur, die etwas unterstützen oder enthalten kann.[13] Information Security Governance soll hier eine einheitliche Struktur anbieten, welche darin alle drei Referenzmodelle, nämlich COBIT, ITIL, ISO 27002 einfügt und auf dieser Basis miteinander vergleichen und zuordnen kann. Um so eine Struktur deutlich zu machen, muss zunächst der Aufbau der drei Referenzmodelle näher beleuchtet werden. Nach der Analyse der drei Referenzmodelle ist festzustellen, dass COBIT, ITIL und ISO 27002 ähnlich aufgebaut sind. Sie unterteilen sich alle in drei Ebenen:

- Hauptaufgaben
- Teilaufgaben
- Aktivitäten

Um die Einheitlichkeit und Vergleichbarkeit zwischen Information Security

[13] http://wordnet.princeton.edu/

Governance Framework und allen drei Referenzmodellen zu ermöglichen, wird in dieser Arbeit ebenfalls eine Drei-Ebenen-Struktur für Information Security Governance Framework benutzt.

Darüber hinaus ist bereits bekannt, dass Information Security Governance fünf Hauptaufgaben verfolgt. Obwohl die genauen Teilaufgaben unter diesen fünf Hauptaufgaben noch nicht in der einschlägigen Literatur anhand von Tabellen oder einer Listenform übersichtlich vorhanden sind, werden hier die Teilaufgaben zu den einzelnen Hauptaufgaben der Information Security Governance wie folgt hergeleitet:

- Als Vorschläge werden in der Literatur „Information Security Governance: Guidance for Boards of Directors and Executive Management 2nd Edition“ von ITGI die Aufgaben für jede einzelne Hauptaufgabe gestellt.

- Die Teilaufgaben können von den 44 Schritten zur Informationssicherheit aus der Literatur „COBIT Security Baseline“ von ITGI herangezogen werden. Die 44 Sicherheitsschritte basieren auf den Standard COBIT und für jeden Schritt wird eine Zuordnung mit dem Standard ISO 27002 angeboten, welche als zwei weltweit akzeptierte Referenzmodelle für die Information Security Governance anerkannt sind.

Die Aktivitäten der Information Security Governance werden nach der Zuordnung, der Analyse von Überschneidungen bzw. die Entscheidung über die Anpassung der Aktivitäten mit Hilfe von drei Referenzmodellen dargestellt.

Die folgende Abbildung verdeutlicht, inwiefern die Elemente der drei Ebenen-Struktur von Information Security Governance (ISG), COBIT; ITIL, ISO 27002 miteinander in Beziehung stehen. Darüber hinaus stellt die Abbildung auch dar, wie im Einzelnen weiter vorgegangen wird, um die Aktivitäten der Information Security Governance aus den entsprechenden Aktivitäten von COBIT, ITIL und ISO 27002 zuzuordnen. Das heißt, die sicherheitsrelevanten Aktivitäten aus COBIT, ITIL und ISO 27002 werden zuerst gemischt und nach Anforderungen jeder Teilaufgabe

von ISG redundanzfrei zugeordnet, um die Teilaufgaben von ISG unterstützen zu können.

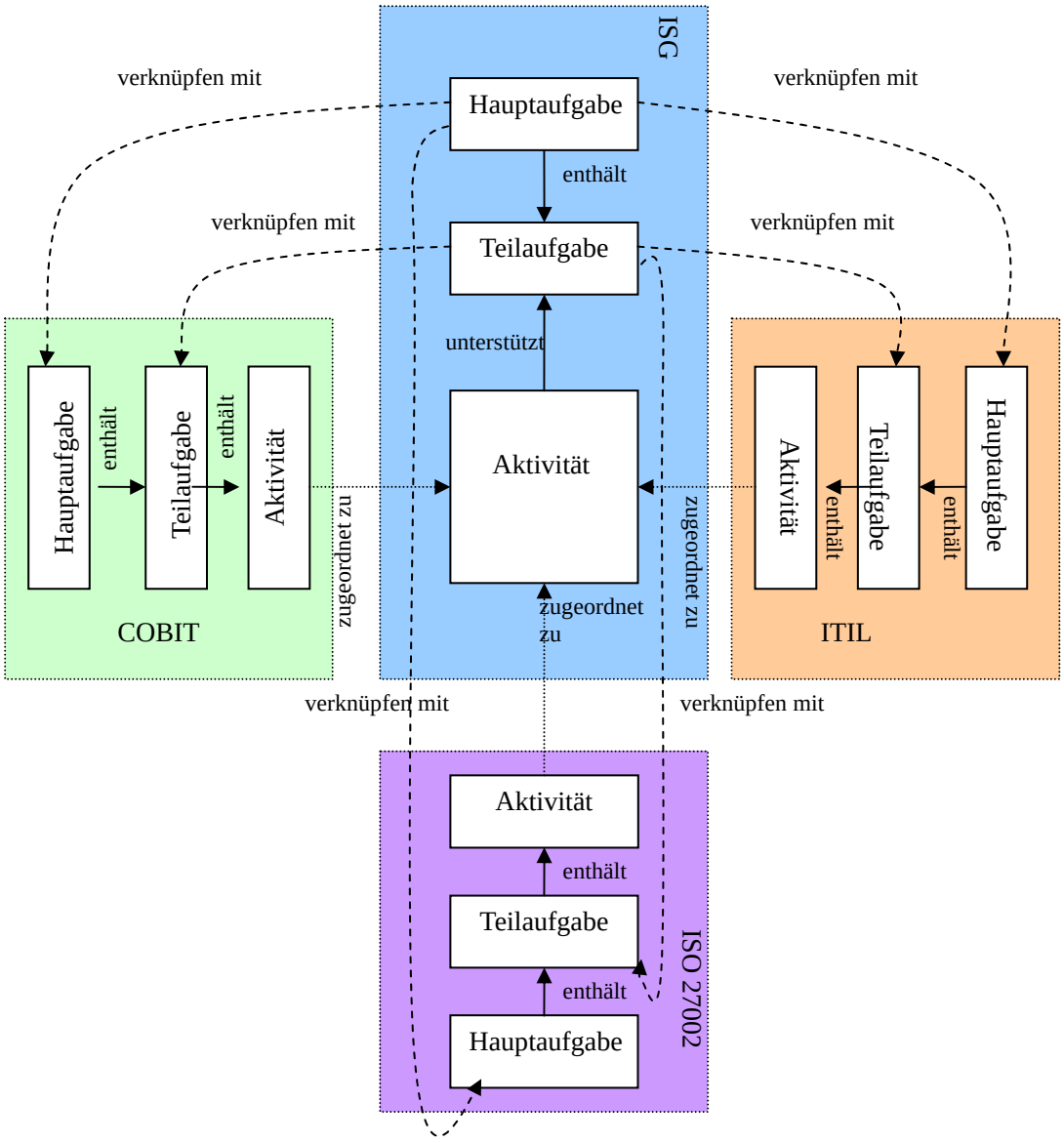

Abbildung 3.1: Beziehung zwischen den Elementen von ISG, COBIT, ITIL und ISO 27002 (eigene Darstellung)

Aus den oben vorgelegten Gründen werden die Teilaufgaben unter jeder Hauptaufgabe der Information Security Governance in der folgenden Tabelle dargestellt:

Strategische Ausrichtung
Definiere die Informationssicherheitsstrategie
Definiere Informationsarchitektur
Bestimme die technologische Richtung
Entwerfe Informationssicherheitspolitik
Definiere IT Organisation und Beziehung
Kommuniziere Ziele und Richtung des Managements
Schaffen von Wert
Definiere und verwalte Service Levels
Identifiziere automatisierte Lösung
Installiere und akkreditiere Lösungen und Änderungen
Manage Leistung von Dritten
Risikomanagement
Stelle den kontinuierlichen Betrieb sicher
Manage IT Risiko
Manage Access
Manage Änderung
Identifiziere, überwache und berichte die Schwachstellen und Störungen
Stelle Ordnungsmäßigkeit mit Vorgaben sicher
Management von Ressourcen
Manage IT Human Resources
Beschaffe und warte Anwendung
Beschaffe und warte Technologie Infrastruktur

Manage Konfiguration
Ermögliche Betrieb und Verwendung
Manage Daten
Manage die physische Umgebung
Leistungsmessung
Monitore und evaluiere IT-Performance
Monitore und evaluiere Internal Controls
Unabhängige Bestätigung

Tabelle 3.1: Haupt- und Teilaufgaben der ISG

Weiterhin werden die Struktur und Bezeichnungsregelung der Haupt-, Teilaufgaben und Aktivitäten der Referenzmodelle COBIT, ISO 27002 sowie ITIL kurz erläutert und in tabellarischer Form dargestellt.

Wie bereits in Kapitel 2.7.1 verdeutlicht wurde, besitzt der Standard COBIT 4 Domänen, die hier als 4 Hauptaufgaben angesehen werden. Unter diesen 4 Domänen gibt es insgesamt 34 IT-Prozesse, hier werden diese als Teilaufgaben für die jeweilige Hautaufgabe aufgenommen. Schließlich werden alle IT-Prozesse von 300 Kontrollzielen unterstützt, die in diesem Falle als Aktivitäten verstanden werden. Tabelle 3.2 zeigt eine Beispiel-struktur und -bezeichnung von COBIT.

COBIT	
Hauptaufgabe	Planung und Organisation (PO)
Teilaufgabe	PO1 Definiere einen strategischen IT-Plan
Aktivität	PO1.2 Ausrichtung Kerngeschäft und IT

Tabelle 3.2: Beispiel-struktur und -bezeichnung von COBIT

Aus Kapitel 2.7.2 wurde erkannt, dass der Standard ITIL V3 über 5 Kerngebiete verfügt, wobei diese zwar fünf Publikationen darstellen, jedoch hier als 5 Hauptaufgaben von ITIL betrachtet werden. Für jedes Kerngebiet gibt es mehrere Prozesse, die das jeweilige Kerngebiet hauptsächlich unterstützen können, sie werden

hier als Teilaufgabe von ITIL aufgenommen. Unter jeden Prozess von ITIL werden zwar mehrere Aktivitäten oder Komponenten beschrieben, jedoch besteht nur unter den Komponenten „Prozess, Aktivitäten, Methoden und Technik“ eine Verbindung mit COBIT und dann also auch mit ISO 27002 [vgl. ITGI 2006 d, S22]. Deshalb werden hier die Aktivitäten von ITIL genau wie die Teilaufgaben bezeichnet, damit der Inhalt der Aktivitäten klarer durch die Bezeichnung dargestellt werden kann. Tabelle 3.3 zeigt eine Beispiel-struktur und -bezeichnung von ITIL.

ITIL	
Hauptaufgabe	Service Design (SD)
Teilaufgabe	SD4.6 Information Security Management
Aktivität	SD4.6 Information Security Management

Tabelle 3.3: Beispiel-struktur und -bezeichnung von ITIL

Wie bereits in Kapitel 2.7.3 dargestellt, verfügt der Standard ISO 27002 über 11 Überwachungsbereiche, die für die Informationssicherheit notwendig sind, sie werden hier jedoch als 11 Hauptaufgaben von ISO 27002 angenommen. Unter jedem Überwachungsbereich bestehen insgesamt 41 Sicherheitskategorien, diese Sicherheitskategorien werden hier als Teilaufgaben für die jeweilige Hauptaufgabe aufgenommen. Weiterhin werden zur Umsetzung der Sicherheitskategorien insgesamt 133 Sicherheitsmaßnahmen des Standards ISO 27002 angeboten, die hier als Aktivitäten von ISO 27002 gezeichnet werden. Tabelle 3.4 zeigt eine Beispiel-struktur und -bezeichnung von ISO 27002.

ISO 27002	
Hauptaufgabe	6.0 Organisatorische Sicherheitsmaßnahmen und Managementprozess
Teilaufgabe	6.1 Interne Organisation
Aktivität	6.1.1 Engagement des Managements für Informationssicherheit

Tabelle 3.4: Beispiel-struktur und -bezeichnung von ISO 27002

3.4 Gesamt-Referenzmodell

In diesem Kapitel wird das gesamte Referenzmodell für Information Security Governance beschrieben bzw. die Zuordnungsergebnisse von COBIT, ITIL und ISO 27002 in tabellarischer Form dargestellt. Für jeden Sicherheitsprozess wird erklärt, wie die jeweiligen Aktivitäten von COBIT, ITIL und ISO 27002 diesen Sicherheitsprozess unterstützen.

Um angepasste Prozesse aus den drei Standards und Best Practices übersichtlich verdeutlichen zu können, werden solche Prozesse, die durch COBIT, ITIL oder ISO 27002 zustande kommen und auch Überschneidungen mit anderen Prozessen aufzeigen, farbig gekennzeichnet.

3.4.1 Strategische Ausrichtung

Definiere die Informationssicherheitsstrategie		
COBIT	**ISO/IEC 27002**	**ITIL**
PO1.2 Ausrichtung Kerngeschäft und IT		**SS4.1 Define the market**
PO1.4 Strategischer IT-Plan		**SS4.2 Develop the offerings**
		SS4.3 Develop strategic assets
		SS4.4 Prepare for execution
		SS5.1 Financial Management
		SS5.5 Demand management
PO1.6 IT - Portfoliomanagement		**SS5.3 Service portfolio management**

Tabelle 3.5: Definiere die Informationssicherheitsstrategie

Um die Sicherheitsstrategie auszurichten, soll zunächst die Definition der Sicherheitsstrategie erklärt werden. Sicherheitsstrategie ist eine Teilstrategie der IT-Strategie, die Aussagen darüber macht, mit welcher Handlung, die als strategisches Formalziel geplante Sicherheit erricht werden soll. Die Sicherheitsstrategie bestimmt den Handlungsspielraum, in dem sich die administrativen und operativen Entscheidungen zur Realisierung der geplanten Sicherheit vollziehen sollen

[Heinrich2004].

Die IT-Strategie hängt stark von der Art der Unternehmung ab, denn um eine IT-Strategie auszuarbeiten, die die Unternehmensstrategie wirkungsvoll unterstützt, ist es zuerst wichtig, die Ziele der Unternehmen genau festzulegen. Eine IT-Strategie ist nur dann sinnvoll, wenn sie mit der Geschäftsstrategie integriert werden. Das heißt, die IT-Strategie soll nur nach den Erfordernissen des Kerngeschäfts ausgerichtet werden. Durch den Prozess „PO1.2 Ausrichtung Kerngeschäft und IT“ von COBIT wird eine klare Verbindung zwischen Unternehmenszielen und den IT–Zielen erstellt, damit die Bereiche, in denen die Geschäftsstrategie von der IT kritisch abhängt, identifiziert werden können [vgl. ITGI2005, S.34]. Diese Bereiche spiegeln zudem den Handlungsspielraum der Informationssicherheit wider.

Nach dem Abstimmen, wo IT eine Unterstützung der strategischen Ziele des Unternehmens leisten kann, soll auch festgelegt werden, inwieweit die IT zu den strategischen Zielen des Unternehmens beiträgt und der die damit verbundenen Kosten und Risiken aufzeigt [vgl. ITGI2005, S.34]. Deshalb ist ein strategischer IT-Plan, der durch den Prozess „PO1.4 strategischer IT-Plan“ ausgerichtet wird, nötig. Der Plan sollte das Investitions- und operative Budget, Finanzierungsquellen, die Sourcing-Strategie, die Beschaffungsstrategie sowie rechtliche und regulatorische Anforderungen abdecken [vgl. ITGI2005, S.34]. Für die Sicherheitsstrategie ist auch wichtig, den finanziellen Aspekt während der strategischen Planungsphase zu berücksichtigen, weil einerseits ohne die benötigen finanziellen Mittel das Sicherheitssystem keine Maßnahmen ergreifen kann, um die Sicherheitsziele zu erledigen. Anderseits bedeuten unnötige hohe Budgets auch nicht zwangsläufig einen hohen Grad an Unterstützung bei der Informationssicherheit [vgl. ISM2006, S.67].

Bei der Ausrichtung einer Sicherheitsstrategie spielen das Demand Management und das Service Portfolio Management eine große Rolle. Durch das Demand Management bzw. das Service Portfolio Management wird der Service, der nach den Anforderungen der Kunden bereitgestellt wird bzw. der für die Erreichung der

strategischen Unternehmensziele erforderlich ist, identifiziert. Die Sicherheitsanforderungen sämtlicher Services werden in der Sicherheitsstrategie beschlossen. Damit werden beispielsweise folgende Fragen beantwortet: Wie lauten die Anforderungen für die Verfügbarkeit eines Services. Wie sehen die Anforderungen hinsichtlich der Vertraulichkeit und Integrität elektronischer Transaktionen und ähnlichem aus.

Definiere Informationsarchitektur		
COBIT	**ISO/IEC 27002**	**ITIL**
PO2.2 Unternehmensweites Data Dictionary und Datensyntaxregeln		
PO4.9 Daten- und Systemeignerschaft	**6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit**	
PO2.3 Datenklassifikationsschema	**7.2.1 Regelungen für die Klassifizierung**	
	7.2.2 Kennzeichnung von und Umgang mit Informationen	

Tabelle 3.6: Definiere Informationsarchitektur

Die Informationsarchitektur ist das Ergebnis der im Idealfall unternehmensweit erfassten, evaluierten und gegliederten Informationsnachfrage bzw. der zu ihrer Befriedigung erforderlichen Informationsversorgung [Heinrich2004, S.319]. Um die Informationsarchitektur zu definieren, wird ein unternehmensweites Data Dictionary aufgebaut, welches die Datensyntaxregeln der Organisation enthält. Damit wird ein gemeinsames Datenverständnis zwischen IT- und Businessanwendern ermöglicht [vgl. ITGI2005, S.38]. Außerdem soll der Eigentümerschaft spezifische Daten- und Informationssysteme durch den Prozess „PO4.9 Daten- und Systemeignerschaft“ zugeordnet werden, damit über die Klassifikation von Informationen und den entsprechenden Schutz von Dateneigentum entschieden werden kann [vgl. ITGI2005, S.46]. Auf der Basis von Data Dictionary, wird durch den Prozess „PO2.3 Datenklassifikationsschema“ ein im gesamten Unternehmen anwendbares Klassifikationsschema eingerichtet, das die Kritikalität und Sensitivität

der Unternehmensdaten zugrunde legt [vgl. ITGI2005, S.38]. Dieses Schema beinhaltet Details über die Dateneigentümerschaft, die Festlegung von angemessenen Sicherheitsstufen sowie Schutzmechanismen, eine kurze Beschreibung der Vorgaben für die Datenaufbewahrung und -zerstörung, und die Kritikalität sowie Sensitivität. Dieses Schema stellt die Grundlage für die Informationssicherheitskontrolle dar.

Nach dem Teilprozess „Definiere Informationsarchitektur“ sollen alle kritischen Daten, die eine große Auswirkung auf Business-Prozesse ausüben, identifiziert werden. Sie sollen auf keinen Fall verloren oder verletzt werden. Ansonsten soll die Eigentümerschaft für die entsprechenden Daten festgelegt werden, wobei nur diejenigen auf ihre vertraulichen Daten zugreifen können, denen sie das ausdrücklich gestatten.

Bestimme die technologische Richtung		
COBIT	**ISO/IEC 27002**	**ITIL**
PO3.4 Technologische Standards		

Tabelle 3.7: Bestimme die technologische Richtung

Um Informationssicherheitsziele zu schaffen, wird eine effektive technologische Unterstützung benötigt. Das Ziel des Teilprozesses „Bestimme die technologische Richtung“ ist, die angemessenen technologischen Standards für sicherheitsrelevante Hardware und Software zu definieren [vgl. ITGI2007a, S.16]. Durch den Prozess „PO3.4 Technologische Standards“ wird ein technologisches Forum etabliert, das Technologierichtlinien und eine Anleitung zur Auswahl von Technologien bereitstellt. Diese sicherheitsrelevanten technologischen Standards basieren auf die Geschäftsrelevanz und berücksichtigen rechtliche sowie regulatorische Rahmenbedingungen, um konsistente, effektive und sichere technische Lösungen für die unternehmensweite Sicherheit einzurichten [vgl. ITGI2005, S.42]

Entwerfe Informationssicherheitspolitik		
COBIT	**ISO/IEC 27002**	**ITIL**
DS5.1 Management der IT-Sicherheit	**6.1.1 Engagement des Managements für Informationssicherheit**	**SD4.6 Information security management**
DS5.2 IT-Security Plan	**5.1.1 Leitlinie zur Informationssicherheit**	**SD4.6 Information security management**
	5.1.2 Überprüfung der Informationssicherheitsleitlinie	

Tabelle 3.8: Entwerfe Informationssicherheitspolitik

Der Begriff Sicherheitspolitik bzw. Sicherheitsleitlinie definiert verschiedene Normen, Standards und Publikationen. In diesem Fall wird die Sicherheitspolitik nach ISO 27002:2005 als überblicksartige Unternehmens- oder Managementvorgaben gewählt. Ziel der Informationssicherheitspolitik ist es, dass das Management die Ausrichtung im Hinblick auf die Informationssicherheit vorgibt und sie unterstützt [vgl. Müller2008, S.53].

Durch den Prozess „DS5.1 Management der „IT-Sicherheit“ wird die IT-Sicherheit auf der höchstmöglichen organisatorischen Ebene beachtet, und damit sichergestellt, dass das Management von sicherheitsrelevanten Aktivitäten mit den Unternehmensanforderungen bestimmt wird [vgl. ITGI2005, S.132]. Auf diese Basis soll eine Leitlinie zur Informationssicherheit festgelegt werden. Diese Informationssicherheitsleitlinie muss von dem Management genehmigt und veröffentlicht werden, wobei alle Angestellten und relevanten externen Positionen darüber in Kenntnis zu setzen sind. Außerdem ist es auch sehr wichtig, die Informationssicherheitsleitlinie in regelmäßigen Abständen zu überprüfen, damit wesentliche Änderungen schnell erfahren werden, und ihre Eignung, Angemessenheit und Wirksamkeit auf Dauer sicherzustellen. Diese Aufgaben werden durch den Prozess „5.1.1 Leitlinie zur Informationssicherheit“ bzw. “5.1.2 Überprüfung der Informationssicherheitsleitlinie“ ständig durchgeführt [vgl. ITSM2008, SS. 132].

Definiere IT Organisation und Beziehung		
COBIT	**ISO/IEC 27002**	**ITIL**
PO4.8 Verantwortung für Risiko, Sicherheit und Ordnungsmäßigkeit	**6.1.1 Engagement des Managements für Informationssicherheit**	
	6.1.2 Koordination der Informationssicherheit	
	6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit	
	6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen	
PO4.10 Beaufsichtigung	**6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit**	
PO4.11 Funktionstrennung	**10.1.3 Aufteilung von Verantwortlichkeiten**	
PO4.13 Schlüsselpersonal der IT		
PO4.14 Policies und Verfahren für beigezogenes Personal	**6.1.5 Vertraulichkeitsvereinbarungen**	
PO4.15 Beziehung	**6.1.6 Kontakt zu Behörden**	
	6.1.7 Kontakt zu speziellen Interessengruppen	

Tabelle 3.9: Definiere IT Organisation und Beziehung

In diesem Teilprozess geht es einerseits um die Definition und Kommunikation von Verantwortlichkeiten der Informationssicherheit innerhalb einer Organisation, und andererseits um den Aufbau von Beziehungen mit informationssicherheitsrelevanten Behörden bzw. Interessengruppen außerhalb einer Organisation.

Um die Informationssicherheitsverantwortlichkeiten definieren zu können, muss zunächst durch den Prozess „6.1.1 Engagement des Managements für Informationssicherheit“ die Informationssicherheit innerhalb der Organisation aktiv vom Management unterstützt werden. Dabei sollen alle Verantwortlichkeiten für die Informationssicherheit anerkannt werden. Weiterhin soll durch den Prozess „6.1.2 Koordination der Informationssicherheit“ auch ein Koordinationsverfahren von den

Vertretern verschiedener Organisationsbereiche stattfinden, damit die Inkompatibilität zwischen den Informationssicherheitsaktivitäten und den Funktionen sowie Aufgaben von Organisationsbereichen zu vermeiden.

Innerhalb des Teilprozesses sollen die Informationssicherheitsverantwortlichkeiten eindeutig definiert und korrekt an die entsprechenden Rollen verteilt werden. Besonderes entscheidend ist, dass das Schlüsselpersonal der IT durch den Prozess „PO4.13 Schlüsselpersonal der IT“ von COBIT bestimmt und identifiziert wird, damit im Notfall mit ihnen Kontakt aufgenommen werden kann. Für jede neue informationsverarbeitende Einrichtung muss durch den Prozess „6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen“ ein Verantwortlicher zugeordnet werden. Hier muss auch beachtet werden, dass nicht zu viele Sicherheitsrollen oder Verantwortlichkeiten auf einen Person vergeben werden (10.1.3 Aufteilung von Verantwortlichkeiten), auch ein Verfahren zur Beaufsichtigung ist nötig, um sicherzustellen, dass Rollen und Verantwortlichkeiten korrekt ausgeführt werden [vgl. ITGI2005, S.46]. Die vertraulichen Inhalte innerhalb der Organisation sollen auf jeden Fall geschützt und geheim gehalten werden. Diese Anforderungen werden durch eine Vertraulichkeitsvereinbarung identifiziert und regelmäßig überprüft (6.1.5 Vertraulichkeitsvereinbarung) [vgl. ITSM2008, S.134].

Kontakte mit sicherheitsrelevanten Behörden als Aufsichts- oder Prüforgane sollen bereits frühzeitig aufgebaut werden, damit deren Anforderungen an die Informationssicherheit kennengelernt und berücksichtigt werden können. Die Aufgabe wird durch den Prozess „6.1.6 Kontakt zu Behörden“ gefordert [vgl. ITSM2008, SS.135f.]. Auch geeignete Kontakte, wie beispielsweise Experten-Sicherheitsforen und professionelle Verbände verhelfen der Organisation den Bedarf nach Beratung, Expertise und Branchenrichtlinien zu erfüllen.

Kommuniziere Ziele und Richtung des Managements		
COBIT	**ISO/IEC 27002**	**ITIL**
PO6.4 Kommunikation der IT-Richtlinien	**6.1.1Engagement des Managements für Informationssicherheit**	
	6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten	
	8.2.2 Sensibilisierung, Ausbildung und Schulung für Informationssicherheit	
PO6.5 Kommunikation von Zielen und Ausrichtung der IT	**5.1.1 Leitlinie zur Informationssicherheit**	
	6.1.1 Engagement des Managements für Informationssicherheit	
	6.1.2 Koordination der Informationssicherheit	

Tabelle 3.10: Kommuniziere Ziele und Richtung des Managements

Die Informationssicherheitspolitik soll ständig an alle relevanten Mitarbeiter kommuniziert und in Kraft gesetzt werden. Damit das Bewusstsein für das Sicherheitsrisiko und die eigenen Sicherheitsverantwortlichkeiten bzw. das Verständnis für Informationssicherheitsmaßnahmen im gesamten Unternehmen durchgeführt werden. Damit eine effiziente und effektive Kommunikation stattfinden kann, wird ein kontinuierliches Kommunikationsprogramm benötigt, in dem alle kommunizierten Informationen in verständlicher Form eingebettet werden.

3.4.2 Schaffen von Werten

Definiere und verwalte Service Levels		
COBIT	**ISO/IEC 27002**	**ITIL**
DS1.3 Service Level Agreements		**SD4.2 Service Level Management**
DS1.5 Monitoring und Berichterstattung der Erreichung von Service Levels		
DS1.6 Review von Service Level Agreement und Underpinning Contracts		

Tabelle 3.11: Definiere und verwalte Service Levels

Das Service Level Management von ITIL stellt zuerst sicher, dass alle Anforderungen an die Informationssicherheit und Service Level Requirements (SLR) für die Sicherheit aufgenommen werden. Auf Basis der Informationssicherheits-anforderungen werden Service Level Agreements (SLA) definiert und vereinbart, die die Maßnahmen zur Erreichung der Informationssicherheitsziele festgelegt haben. Um die im SLA vereinbarten Sicherheitsziele in spezifizierte technische Prozesse umzusetzen und dem Anbieter auf eine verständliche Art und Weise beizubringen, werden in Operating Level Agreements (OLAs) pro Sicherheitsziel aus dem SLA eine genauere Anweisung gegeben, und festgestellt, welche Aufgaben damit verbunden sind [vgl. ISM2006, S.44]. Außerdem muss der Service, der nur mit Hilfe von Dritten erbracht werden kann, in Underpinning Contracts (UC) definiert werden.

Die Erreichung der Informationssicherheitsziele muss überwacht, gemessen und bewertet werden. Dazu bietet ITIL Kennzahlen, die so genannten Key Performance Indicator (KPI). Damit spiegelt sich die Leistung der Erreichung des Informationssicherheitsziels wider. Auf Basis der KPIs soll regelmäßig eine Berichtung stattfinden, um das Optimierungspotential zu identifizieren, auf mögliche Trends aufmerksam zu machen und eine Lösung dafür zu finden [vgl. ISM2006, S.44].

Durch den Teilprozess „Definiere und verwalte Service Levels“ werden die Anforderungen des Informationssicherheitsziels von Kunden hergestellt, und dadurch gewährleistet, dass die Informationssicherheitsanforderungen immer mit den Geschäftsanforderungen übereinstimmen.

Identifiziere automatisierte Lösungen		
COBIT	**ISO/IEC 27002**	**ITIL**
AI1.1 Festlegung und Aktualisierung von funktionalen Geschäfts- und technischen Erfordernissen	**12.1.1 Analyse und Spezifikation von Sicherheitsanforderungen**	**SD4.5 IT Service Continuity Management**
AI1.2 Risikoanalyse-Bericht		

Tabelle 3.12: Identifiziere automatisierte Lösungen

Der Bedarf an neuen Anwendungen oder Funktionen erfordert vor einer Beschaffung oder Entwicklung eine Analyse, um sicherzustellen, dass die Unternehmensanforderungen an Sicherheitsmaßnahmen spezifiziert werden. Das heißt, die Sicherheitsanforderung soll schon in der Beschaffungsanforderung integriert werden und für jede Anforderung einen Testfall erzeugen, damit der beschaffende Gegenstand nach einem bestimmten Abnahmekriterium kontrolliert und somit nachgeprüft werden kann, ob bestimmte Sicherheitsanforderungen erfüllt oder spezifische Sicherheitseigenschaften erhalten werden können [vgl. ITSM2008, SS.189]. Diese Aufgabe wird von dem Prozess „12.1.1 Analyse und Spezifikation von Sicherheitsanforderungen“ von ISO 27002 übernommen.

Installiere und akkreditiere Lösungen und Änderungen		
COBIT	**ISO/IEC 27002**	**ITIL**
PO8.3 Entwicklungs- und Beschaffungs-Standards		**ST4.1 Transition Planning and Support**
AI7.3 Implementierungsplan		**ST4.4 Release and Deployment**
AI7.2 Testplan		**ST4.5 Service Validation and Testing**
AI7.4 Testumgebung	**10.1.4 Aufteilung von Entwicklungs-, Test- und Produktiveinrichtungen**	
	12.4.2 Schutz von Test-Daten	
AI7.6 Test von Änderungen	**12.5.2 Technische Kontrolle von Anwendungen nach Änderungen am Betriebssystem**	
AI7.8 Produktivstellung		
AI7.7 Abschließender Akzeptanztest	**10.3.2 System-Abnahme**	**ST 4.6 Evaluation**
AI7.9 Post-Implementation Review		

Tabelle 3.13: Installiere und akkreditiere Lösungen und Änderungen

Der Teilprozess „Installiere und akkreditiere Lösungen und Änderungen“ stellt sicher, dass alle autorisierten Veränderungen nur nach ausreichender Sicherheitsüberprüfung in Produktion vollzogen und ausgeliefert werden dürfen.

Der Prozess “Transition Planning and Support“ behandelt hingegen die strukturierte Planung von angemessenen Ressourcen für die Überführung von technischen Komponenten und Services in den Betrieb. Dies impliziert zum einen die Zusammenstellung von Release-Ständen, und zum anderen den Test und die Installation [vgl. Olbrich2008, S.152].

Weiterhin wird der Prozess „Release und Deployment Management“ für die Planung, den zeitlichen Ablauf und die Steuerung des Übergangs von Releases in Test- und Live-Umgebungen verantwortlich sein. Das wichtigste Ziel dieses Prozesses liegt darin, sicherzustellen, dass die Integrität der Live-Umgebung aufrecht erhalten wird und dass die richtigen Komponenten im Release enthalten sind. Die Hauptaufgabe in

Bezug auf die Informationssicherheit ist, dass Informationssicherheits-Grundsätze definiert und während einer Rollout-Phase sichergestellt werden [vgl. ISM2006, SS.91].

Eine wichtige Forderung des Teilprozesses “Installiere und akkreditiere Lösungen und Änderungen“ ist eine produktionsidentische Testumgebung, auf der die unterschiedlichen Releases in der jeweils zu einer Rollout gültigen Version durchgängig gegeneinander getestet werden können. Diese Durchgängigkeit muss sowohl durch das Testsystem als auch für die Vorhaltung konsistenter Testdaten ermöglicht werden [vgl. ISM2006, SS.91]. Außerdem ist es aus Sicherheitsgründen wichtig, dass die Test-Daten sorgfältig ausgewählt, geschützt und kontrolliert werden. Falls Änderungen am Betriebsystem erfolgten, werden eine Überprüfung und Tests auf geschäftskritische Anwendungen gefordert, um zu garantieren, dass keine negativen Auswirkungen für den Betrieb und die Sicherheit der Organisation vorhanden sind [vgl. ITSM2008, S.194f.]. Diese Aufgabe wird vom Prozess „Service Validation und Testing“ übernommen.

Am Ende des Teilprozesses sollen sämtliche Änderungen bewertet, und akzeptierte Kriterien von dem SLA geliefert werden. Durch die Bewertung der erwarteten und tatsächlichen Performance der Änderung, erzeugt der Prozess “Evaluation“ dann jeweils einen so genannten Evaluation Report, damit vor der Betriebsfreigabe jene Änderungen festgestellt werden, wo und welche Probleme oder Risiken es eventuell geben könnte und ob mit den Änderungen überhaupt fortgefahren werden soll.

Manage Leistung von Dritten		
COBIT	**ISO/IEC 27002**	**ITIL**
DS2.3 Lieferanten-Risikomanagement	**6.2.1 Identifizierung von Risiken in Zusammenhang mit Externen**	**SD4.7 Supplier Management**
AI5.2 Vertragsmanagement für Lieferanten	**6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten**	
	8.1.1 Aufgaben und Verantwortlichkeiten	
	8.1.2 Überprüfung	
	8.1.3 Arbeitsvertragsklauseln	
	10.2.1 Erbringung von Dienstleistungen	
DS2.4 Monitoring der Performance von Lieferanten	**10.2.2 Überwachung und Überprüfung der Dienstleistungen von Dritten**	
	10.2.3 Management von Änderungen an Dienstleistungen von Dritten	

Tabelle 3.14: Manage Leistung von Dritten

Einbindungen mit externen Parteien sollen alle identifiziert, überwacht, gesichert und überprüft werden. Die folgenden Aspekte werden berücksichtigt, sofern Daten und Systeme von Externen genutzt und verwaltet oder Daten an Externe kommuniziert werden. Zunächst müssen alle möglichen Risiken für Informationen und informationsverarbeitende Einrichtungen der Organisation, die durch Geschäftsprozesse unter Beteiligung Externer verursacht werden, identifizieren und angemessene Maßnahmen einleiten, bevor diesen der Zugang erteilt wird [vgl. ITSM2008, S.138]. Daraufhin müssen sämtliche Sicherheitsanforderungen mit Externen abgedeckt bzw. in der Vertragsform vereinbart werden.

Außerdem müssen die Sicherheitsaufgaben und –verantwortung der Benutzer von Externen definiert sowie dokumentiert und in Form eines Vertrags niedergeschrieben werden. Die Vergangenheit externer Benutzer muss in Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen überprüft werden, damit nur zuverlässige und vertrauenswürdige Personen an eine informationssicherheits-

relevante Position eingestellt werden.

Sämtliche von Dritten erbrachten Dienstleistungen müssen gemäß der Sicherheitsmaßnahmen, Leistungsbeschreibungen und dem Grad der Lieferungen einer Liefervereinbarung mit Dritten genau definiert, und die Einhaltung der Vereinbarung regelmäßig überwacht und überprüft werden. Damit kann die Verpflichtung von Dritten nachgewiesen bzw. kontrolliert werden. Wenn es Veränderungen der Dienstleistungen durch Dritte geben sollte, muss vor der Zustimmung der neuen Liefervereinbarung die Auswirkung auf die Sicherheit der Organisation berücksichtigt werden.

3.4.3 Risikomanagement

Stelle den kontinuierlichen Betrieb sicher		
COBIT	**ISO/IEC 27002**	**ITIL**
DS3.1 Planung von Performance und Kapazität	10.3.1 Kapazitätsplanung	SD4.3 Capacity management
DS3.2 Gegenwärtige Kapazität und Performance		
DS3.3 Künftige Kapazität und Performance		
DS3.4 Verfügbarkeit der IT-Ressourcen		SD4.4 Availability Management
DS3.5 Monitoring und Reporting		
DS4.1 Framework für IT-Kontinuität	14.1.1 Einbeziehen von Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs	SD4.5 IT service continuity management
DS4.3 Kritische IT-Ressourcen	14.1.2 Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung	
DS4.2 IT - Kontinuitätspläne	14.1.3 Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten	
DS4.1 Framework für IT-Kontinuität	14.1.4 Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs	
DS4.4 Wartung des IT-Kontinuitätsplans	14.1.5 Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung des Geschäftsbetriebs	
DS4.5 Test des IT-Kontinuitätsplans		
DS4.6 IT Continuity plan Training		
DS4.7 Verteilung des IT-Kontinuitätsplans		

Tabelle 3.15: Stelle den kontinuierlichen Betrieb sicher

Der Teilprozess “Stelle den kontinuierlichen Betrieb sicher“ gewährleistet, dass der Betrieb die Fähigkeit besitzt, dass kontinuierliche Geschäftsprozesse unterstützt

werden können. Außerdem soll durch den Teilprozess die Unterbrechung von Geschäftsprozessen verhindert werden, damit eine reibungslose Fortführung der Geschäftsprozesse erfolgen kann [vgl. ITSM2008, S.200].

Systemüberlastungen oder Performance-Engpässe können eine Ursache für unzureichende Verfügbarkeit oder gar Systemausfälle sein. Der Prozess „Kapazitätsplanung“ von ISO 27002 bietet die Möglichkeit die Verwendung von Ressourcen zu überwachen und abzustimmen, wobei anschließend eine Kapazitätsplanung aufgebaut werden soll, die auf Basis des gegenwärtigen belastbaren Zahlenmaterials die zukünftige Kapazität abschätzt [vgl. ITSM2008, S.158f.].

Die Verfügbarkeit stellt sowohl für den Teilprozess “Stelle den kontinuierlichen Betrieb sicher“ als auch für das ganze Sicherheitsmanagementsystem einen wichtigen Aspekt dar. Die Hauptaufgabe des Prozesses “SD4.4 Availability Management“ von ITIL ist die Überwachung der Verfügbarkeit von IT Services nach in Service Level Management definierte KPIs (Key Performance Indikators) sowie die Sicherstellung der Auswahl von Maßnahmen zur Erreichung verfügbarer Ziele. Darüber hinaus werden die Abweichungen vom Verfügbarkeitsplan beim Sicherheitsmanagement-system gemeldet, da die Urasche hierfür eine Sicherheitsstörung sein kann.

Um die Unterbrechung von Geschäftsprozessen zu verhindern und deren erneute Fortführung schnellstmöglich sicherzustellen, werden die Geschäftsprozesse durch folgende Maßnahmen geschützt: Zunächst werden die Sicherheitsanforderungen an Geschäftsprozesse durch den Prozess „14.1.1 Einbeziehen von Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs“ genau identifiziert und dokumentiert. Anschließend sollen die Risiken, die die Unterbrechung der Geschäftsprozesse verursacht haben könnten bzw. die Wahrscheinlichkeiten und Auswirkungen solcher Unterbrechungen durch den Prozess „14.1.2 Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung“ identifiziert werden. Auf dieser Basis werden die Pläne entwickelt und umgesetzt, um den Betrieb aufrechtzuerhalten oder

wiederherzustellen. Diese Aufgabe wird von dem Prozess „14.1.3 Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten“ übernommen. Des Weiteren ist es auch wichtig, sicherzustellen, dass die Pläne in komplexen Situationen widerspruchsfrei sind. Dies wird durch den Prozess „14.1.4 Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs“ erreicht. Ansonst sollen die Pläne durch den Prozess „14.1.5 Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung des Geschäftsbetriebs“ regelmäßig getestet und aktualisiert werden, um sie einerseits auf dem neusten Stand und andererseits effektiv beizubehalten [vgl. ITSM2008, S.201ff.].

Manage IT Risiko		
COBIT	**ISO/IEC 27002**	**ITIL**
PO9.1 Abstimmung des Risikomanagements der IT und des Unternehmens	**4.1 Beurteilung von Sicherheitsrisiken**	
PO9.2 Festlegung des Risikokontexts		
PO9.3 Ereignisidentifikation		
PO9.4 Bewertung von Risiken		
PO9.5 Maßnahmen zur Risikobehandlung	**4.2 Behandlung von Sicherheitsrisiken**	
PO9.6 Erhalt und Monitoring eines Plans zur Risikobehandlung		

Tabelle 3.16: Manage IT Risiko

Als Risiko wird laut /ISO 73/ eine Kombination aus der Wahrscheinlichkeit eines (unerwünschten, unerwarteten, schädlichen) Ereignisses und dessen Konsequenzen definiert [vgl. ITSM2008, S.22].

Diese Konsequenzen solcher Ereignisse können unmittelbare Schäden sein. Deshalb ist das Management für Sicherheitsrisiko ein wichtiges Element für das Informationssicherheitsmanagement. Außerdem müssen alle Informationssicherheits-

maßnahmen, die zur Erreichung der Informationssicherheitsziele getroffen wurden, gemäß einer risikobasierten Vorgehensweise ausgewählt werden [vgl. ITSM2008, S.21].

Durch den Prozess „4.1 Beurteilung von Sicherheitsrisiken“ werden die Sicherheitsrisiken mit Hilfe von Risikoanalyse und Risikobewertung eingeschätzt. Dabei können Sicherheitsrisiken konkret erkannt, und festgestellt werden, welchen Bedrohungen diese ausgesetzt sind, und für welche Schwachstellen sie anfällig sind. Darüber hinaus kann die Wahrscheinlichkeit und das Ausmaß der Schäden unter Berücksichtigung der vorhandenen Sicherheitsvorkehrungen ungefähr abgeschätzt werden. Die dadurch abgeschätzten Risiken sind zudem einer Bewertungsklasse zuzuordnen [vgl. ISM2006, S. 115].

Weiterhin zeigt der Prozess „4.2 Behandlung von Sicherheitsrisiken“, wie man mit Risiko überhaupt umgehen kann. Hier fordert es die Aufstellung eines Risikobehandlungsplans, in dem eine Auswahl für die Behandlung übrig gebliebener Risiken (*Restrisiko*) bestimmt, und schließlich auf alle verbleibenden Risiken angewendet wird [vgl. ITSM2008, S.30].

Manage Zugang		
COBIT	**ISO/IEC 27002**	**ITIL**
DS5.3 Identitätsmanagement	**11.1.1 Regelwerk zur Zugangskontrolle**	**SO 4.5 Access management**
DS5.4 Management von Benutzerkonten	**11.2.1 Benutzerregistrierung**	
	11.2.2 Verwaltung von Sonderrechten	
	11.2.3 Verwaltung von Benutzerpasswörtern	
	11.2.4 Überprüfung von Benutzerberechtigungen	
	11.3.1 Passwortverwendung	
	11.3.2 Unbeaufsichtigte Benutzerausstattung	
	11.3.3 Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms	
DS5.10 Netzwerk-Sicherheit	**11.4.1 Regelwerk zur Nutzung von Netzen**	
	11.4.2 Bnutzerauthentisierung für externe Verbindungen	
	11.4.3 Geräteidentifikation in Netzen	
	11.4.4 Schutz der Diagnose- und Konfigurationsports	
	11.4.5 Trennung in Netzwerken	
	11.4.6 Kontrolle von Netzverbindungen	
	11.4.7 Routingkontrolle für Netze	
DS5.7 Schutz von Sicherheitseinrichtungen	**11.5.1 Verfahren für sichere Anmeldung**	
	11.5.4 Verwendung von Systemwerkzeugen	
	11.5.5 Session time-out	
	11.5.6 Begrenzung der Verbindungszeit	
	11.5.2 Benutzeridentifikation und Authentisierung	
	11.5.3 System zur Verwaltung von Passwörtern	

Tabelle 3.17: Manage Zugang

Der Teilprozess „Manage Zugang“ beschäftigt sich mit den Benutzerberechtigungen. Hier wird zuerst mit Hilfe des Prozesses „11.1.1 Regelwerk zur Zugangs-

kontrolle“ von ISO 27002 eine Rechtstruktur aufgebaut, wobei jede Art von Benutzerberechtigung aufgelistet wird. Die allgemeinen Vergaberegeln von Benutzerberechtigungen werden als Regelwerk bezeichnet. Das Regelwerk muss konzipiert, dokumentiert, regelmäßig überprüft und ggf. überarbeitet werden [vgl. ISM2006, S.176]. Entscheidend dabei ist, dass Benutzerberechtigungen für die Systeme und Daten mit den festgelegten und dokumentierten Geschäftsbedürfnissen und Arbeitsplatzanforderungen identisch sind [vgl. ITGI2005, S.132].

Nachdem alle Berechtigungen definiert wurden, wird ein Management benötigt, das aufzeigt, wie die Berechtigungen an Benutzer vergeben oder entzogen werden können. Dabei werden folgende vier Maßnahmen von ISO 27002 angeboten: Zuerst soll durch den Prozess „11.2.1 Benutzerregistrierung“ sichergestellt werden, dass alle Informationssysteme und Dienste einen formalen Prozess besitzen, um dem Benutzer einen Account sowie eine Vergabe und schließlich den Entzug von Rechten einzurichten. Die Behandlungen der Rechte für so genannte sicherheitskritische Rollen bzw. kritische Situationen müssen separat definiert und regelmäßig kontrolliert werden. Diese Aufgabe wird von dem Prozess „11.2.2 Verwaltung von Sonderrechten“ übernommen. Außerdem wird ein formaler Verwaltungsprozess, der vom Prozess „11.2.3 Verwaltung von Benutzerpasswörtern“ angeboten wird, für Benutzerpasswörter gefordert. Letztendlich ist es überaus wichtig, mit Hilfe des Prozesses „11.2.4 Überprüfung von Benutzerberechtigungen“ alle Benutzer-berechtigungen regelmäßig zu überprüfen [vgl. ISM2006, S.177ff.].

Um ein effektives Management der Benutzerberechtigungen zu ermöglichen, wird die Erkennung der Verantwortungen von Benutzern gefordert. Zudem ist es unbedingt notwendig, dass Benutzer korrekte Sicherheitspraktiken bei der Auswahl und der Anwendung von Passwörtern folgen (11.3.1 Passwortverwendung) und beachten, dass eine unbeaufsichtigte Ausstattung genügend Schutz erhält (11.3.2 Unbeaufsichtigte Benutzerausstattung). Des Weiteren muss eine so genannte „Clear Desk Policy“ beibehalten werden, damit Unbefugte keinen Zugriff auf Daten, Medien und

anderweitige Dokumente erlangen können (11.3.3 Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms) [vgl. ISM2006, S.179f.].

Außerdem werden innerhalb dieses Teilprozesses die Sicherheitsmaßnahmen hinsichtlich der Zugangskontrolle für das Netzwerk bzw. Betriebssystem verdeutlicht. Wie genau diese Sicherheitsanforderungen erfüllt werden können, zeigt eine sehr detaillierte Maßnahme, die von ISO 27002 angeboten wird.

Manage Änderung		
COBIT	**ISO/IEC 27002**	**ITIL**
AI6.1 Standard und Verfahren für Änderungen	**12.5.1 Änderungskontrollverfahren**	**ST 4.2 Change management**
AI6.2 Bewertung von Auswirkungen, Priorisierung und Freigaben		
AI6.3 Notfallsänderungen		
AI6.4 Statusverfolgung und Berichterstattung		
AI6.5 Abschluss und Dokumentation von Änderungen		
	12.5.2 Technische Kontrolle von Anwendungen nach Änderungen am Betriebssystem	
	12.5.3 Einschränkung von Änderungen an Softwarepaketen	
	12.5.4 Ungewollte Preisgabe von Informationen	

Tabelle 3.18: Manage Änderung

Das Ziel des Teilprozesses „Manage Änderung“ ist es, sicherzustellen, dass alle Änderungen auf eine bestimmte Sicherheitsart und –weise durchgeführt werden, und im Falle von Änderungen zudem versuchen, dass keine Auswirkungen auf den alltäglichen Geschäftsprozess entstehen. Der Prozess „ST4.2 Change Management“ von ITIL ist ein zentraler Bestandteil im ITIL-Prozessmodell, der auch für das Sicherheitsmanagement die Möglichkeit bietet, dass alle Änderungen auf

kontrollierte Weise gemäß der Sicherheitsziele aus dem SLA umgesetzt werden.

Folgende Maßnahmen werden durch Änderung Management durchgeführt: Zunächst werden RfCs durch das Änderung Management bewertet, und erfahren, ob die Änderung dringt notwendig ist, da eine unbedingte Änderung ein verkürztes Verfahren verlangt. Daraufhin werden die Auswirkungen der Änderung in Bezug auf Informationssicherheit analysiert. Gemäß der Auswirkungen wird ein entsprechender Test durchgeführt, damit die Änderungen näher untersucht, und festgestellt werden kann, ob die Sicherheitsziele bereits erreicht wurden. Außerdem werden notwendige Änderungen auch durch so genannte „Smoke Tests“ getestet. Nicht erreichte Änderungen hingegen werden abgelehnt. Wenn die Sicherheitsziele positiv geprüft worden sind, können Änderungen freigegeben werden [vgl. ISM2006, S.83f.].

Am Ende des Prozesses müssen alle Änderungen dokumentiert und der Verantwortlichkeit zugewiesen werden, um alle Änderungen nachvollziehen zu können und eine vollständige Umsetzung der Änderungen sicherzustellen.

Damit ein Änderungsprozess sicher erfolgen kann, muss ein weiterer Aspekt berücksichtigt werden. Falls Betriebssysteme geändert werden, müssen geschäftskritische Anwendungen überprüft und getestet werden, um zu gewährleisten, dass kein Einfluss negativer Auswirkungen für den Betrieb und die Sicherheit der Organisation ausgelöst wird. Veränderungen an Softwarepaketen sollen zudem soweit wie möglich verhindert, auf die notwendigen Änderungen beschränkt und alle Veränderungen streng kontrolliert werden. Letztendlich sollen die Möglichkeiten für eine ungewollte Preisgabe von Informationen während Änderungsprozessen unbedingt vermieden werden [vgl. ISM2006, S.195f.].

Identifiziere, überwache und Berichte die Schwachstellen und Störungen		
COBIT	**ISO/IEC 27002**	**ITIL**
DS5.6 Definition von Security Störungen		**SO 4.2 Incident Management**
DS8.3 Eskalation von Störungen	**13.1.1 Melden von Informationssicherheitsereignissen**	
DS8.2 Registrierung von Kundenanfragen	**13.1.2 Melden von Sicherheitsschwachstellen**	
DS8.4 Schließen von Störungen		
	13.2.1 Verantwortlichkeiten und Verfahren	
DS8.5 Trendanalyse	**13.2.2 Lernen von Informationssicherheitsvorfällen**	
	13.2.3 Sammeln von Beweisen	
DS10.1 Identifikation und Klassifikation von Problem		**SO 4.4 Problem Management**
DS10.2 Problemverfolgung und –lösung		
DS10.3 Abschluss von Problem		

Tabelle 3.19: Identifiziere, überwache und berichte die Schwachstellen und Störungen

Das Ziel des Teilprozesses „Identifiziere, Überwache und Berichte die Schwachstellen und Störungen“ beinhaltet, dass alle Störungen zu verwalten und die Ursachen dafür zu finden sind. Die Aufgaben werden jeweils durch den Prozess „SO4.2 Incident Management“ und „SO4.4 Problem Management“ von ITIL übernommen.

Die Aufgabe des Störung Managements ist es, die Sicherheitsstörungen so schnell wie möglich zu identifizieren.

Eine Störung der Informationssicherheit (engl. Security Incident) ist ein Ereignis, das die Verfügbarkeit, die Integrität oder die Vertraulichkeit beim Betrieb eines IT-Services verletzt und das als tatsächliche oder mögliche Auswirkung eine Minderung der Sicherheitsziele verursacht. [vgl. ISM2006, S.75]

Durch den Prozess “SO4.2 Incident Management“ sollen zunächst alle Sicherheitsstörungen und Schwachstellen definiert und je nach Schadensauswirkung und Dringlichkeit klassifiziert werden, damit sie schließlich aufgenommen und gespeichert werden können. Nachdem Sicherheitsstörungen aufgenommen wurden, müssen sofortige Behandlungsmaßnahmen ergriffen werden. Die Sicherheits-störungen prüfen dann, ob es sich um eine bereits bekannte Störung handelt. Falls dieses zutrifft, wird die definierte Lösung ausgewählt. Wenn eine Störung nicht bekannt sein sollte und auch keine schnelle Lösung dafür gefunden werden kann, wird die Störung eskalieren. Außerdem werden die Sicherheitsstörungen verfolgt, und genau dokumentiert. Ein Abschluss einer Störung wird dann gelöst an dem Service Desk zurückgegeben, der dann den Anwender darüber informiert.

Das Problem-Management nimmt dort seinen Anfang, wo das Störungs-Management endet, denn: „Ein Problem ist ein Fehler, dessen Ursache noch nicht bekannt ist.“ [ISM2006, S.78].

Die Aufgabe des Problem-Managements ist es, die Ursachen für bereits bekannte Störungen reaktiv und für zukünftig eventuell auftretende Störungen proaktiv zu analysieren. Dabei wird so genannte Ursachenanalyse (*Root Cause Analysis*) durchgeführt, mit deren Hilfe die Ursachen von unbegreiflichen Sicherheitsproblemen aufgeklärt werden können.

Stelle Ordnungsmäßigkeit mit Forderungen sicher		
COBIT	**ISO/IEC 27002**	**ITIL**
ME3.1 Identifikation von Gesetzen und Regulativen mit einer potentiellen Auswirkung auf die IT	**15.1.1 Identifikation der anwendbaren Gesetze**	**SD4.2 Service Level Management**
	15.1.2 Rechte an geistigem Eigentum	
	15.1.3 Schutz von organisationseigenen Aufzeichnungen	
	15.1.4 Datenschutz und Vertraulichkeit von personenbezogenen Informationen	
	15.1.5 Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen	
	15.1.6 Regelungen zu kryptografischen Maßnahmen	
ME3.3 Evaluierung der Ordnungsmäßigkeit mit regulatorischen Anforderungen	**15.2.1 Einhaltung von Sicherheitsregelungen und -Standards**	
ME3.4 Positive Bestätigung der Ordnungsmäßigkeit	**15.2.2 Prüfung der Einhaltung technischer Vorgaben**	

Tabelle 3.20: Stelle Ordnungsmäßigkeit mit Forderungen sicher

Der Teilprozess „Stelle Ordnungsmäßigkeit mit Forderungen sicher“ gewährleistet, dass die Informationssicherheitsvorgaben mit gesetzlichen, regulativen, vertraglichen und wirtschaftlichen Anforderungen übereinstimmen und eingehalten werden.

Zuerst müssen durch den Prozess „15.1.1 Identifikation der anwendbaren Gesetze“ von ISO 27002 alle relevanten gesetzlichen, amtlichen und vertraglichen Anforderungen definiert werden, einschließlich dem Ansatz der Organisation, um diese Anforderungen schließlich zu erfüllen. Danach werden mit Hilfe der jeweiligen Prozesse die Gesetze und Vorschriften für geistiges Eigentum, organisationseigene Aufzeichnungen, Datenschutz und Vertraulichkeit von personenbezogenen Informationen beachtet. Außerdem soll durch die Prozesse „15.1.5 Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen“ und „15.1.6 Regelungen zu kryptografischen Maßnahmen“ die Benutzung von informationsverarbeitenden

Einrichtungen und kryptografischen Maßnahmen gemäß aller relevanten Vereinbarungen, Gesetze und Vorschriften geregelt werden [vgl. ITSM2008, S.204ff.].

Informationssicherheitsvorgaben sollen nicht nur gemacht, sondern auch deren Einhaltung kontrolliert werden. Dazu sollen einerseits durch den Prozess „15.2.1 Einhaltung von Sicherheitsregelungen und -Standards“ die Sicherheitsmanager dazu bewegt werden, ihrer Verantwortung für die Einhaltung der Sicherheitsregelungen und -Standards bewusst zu werden und diese auch vertrauenswürdig auszuführen. Andererseits sollen durch den Prozess „15.2.2 Prüfung der Einhaltung technischer Vorgaben“ die technischen Vorgaben regelmäßig überprüft werden, damit ermöglicht werden kann, dass Informationssysteme die Sicherheitsimplementierung ständig unterstützen können [vgl. ITSM2008, S.208f.].

3.4.4 Ressourcemanagement

Manage IT Human Resources		
COBIT	**ISO/IEC 27002**	**ITIL**
PO4.6 Rollen und Verantwortlichkeiten	**8.1.1 Aufgaben und Verantwortlichkeiten**	
PO7.2 Kompetenzen des Personals	**8.1.2 Überprüfung**	
PO 7.6 Verfahren zur Überprüfung von Personal		
PO7.1 Personalrekrutierung und –bindung	**8.1.3 Arbeitsvertragsklauseln**	
PO7.3 Besetzung von Rollen	**8.2.1 Verantwortung des Managements**	
PO7.4 Ausbildung des Personals	**8.2.2 Sensibilisierung, Ausbildung und Schulung für Informationssicherheit**	
PO7.7 Beurteilung der Leistung von Mitarbeitern		
	8.2.3 Disziplinarverfahren	
PO7.8 Stellenwechsel und Kündigung	**8.3.1 Verantwortlichen bei der Beendigung**	
	8.3.2 Rückgabe von organisationseigenen Werten	
	8.3.3 Aufheben von Zugangsrechten	

Tabelle 3.21: Manage IT Human Resources

Der Teilprozess „Manage IT Human Ressource“ beschäftigt sich mit der Qualifikation und Zuverlässigkeit des Personals. Dazu wird der Teilprozess in drei Sicherheitskategorien aufgeteilt, nämlich „Vor der Anstellung“, „Während der Anstellung “ sowie „Beendigung oder Änderung der Anstellung“.

Unter der Kategorie „Vor der Anstellung“ wird aufgefasst, welche Anforderungen bestehen, wenn eine neue sicherheitsrelevante Aufgabe beauftragt oder eine neue Verantwortung an eine Person vergeben wird. Das Ziel verlangt, dass die Beauftragten zum einen ihre neu zugewiesene Aufgabe und Verantwortung tatsächlich begriffen haben und zum anderen, dass sie in der Durchführung über die nötige Qualifikation verfügen. Darüber hinaus sollten auch die personellen Risiken (Diebstahl, Betrug oder

Missbrauch) so weit wie möglich reduziert werden. Dafür werden folgende Maßnahmen durchgeführt: Zuerst werden durch den Prozess „8.1.1 Aufgaben und Verantwortliche“ die Sicherheitsaufgaben und –Verantwortungen klar definiert und dokumentiert. Denn nur auf Basis einer klaren Definition der Sicherheitsaufgaben und –Verantwortungen kann die Qualifikation und Zuverlässigkeit der beauftragten Person überprüft werden. Die Überprüfung der Aufgabe, Qualifikation und Zuverlässigkeit einer Person, wird mit Hilfe des Prozesses „8.1.2 Überprüfung“ ausgeführt. Schließlich fordert der Prozess „8.1.3 Arbeitvertragsklauseln“, dass Mitarbeiter den Vertragsklauseln (z.B. Datenschutzverpflichtung) zustimmen [vgl. ITSM2008, S.142f.].

Nach der Beauftragung einer neuen Sicherheitsaufgabe und –Verantwortung muss sichergestellt werden, dass die beauftragte Person „während der Anstellung“ die Sicherheitsaufgabe und –Verantwortung in der Tätigkeit tatsächlich umsetzen kann. Dazu wird zuerst durch den Prozess „8.2.1 Verantwortung des Managements“ vom Management gefordert, dass die Mitarbeiter bei der Anwendung der Sicherheit in Übereinstimmung mit den festgelegten Leitlinien und Verfahren der Organisation liegen. Weiterhin ist die regelmäßige Sensibilisierung, Ausbildung und Schulung in Bezug auf Informationssicherheit für die Mitarbeiter wichtig. Denn Sensibilisierung bietet die Möglichkeit, dass Mitarbeiter die Sicherheitsprobleme und ihre Auswirkungen auf die Organisation nachvollziehen. Durch die Ausbildung und Schulung werden dem Mitarbeiter notwendige Kenntnisse, wie beispielsweise durch die Lösung zu einem Problem, vermittelt. Ansonsten soll durch den Prozess „PO7.7 Beurteilung der Leistung von Mitarbeitern“ von COBIT ein Verfahren bereitstellen, um die Leistungen der Mitarbeiter regelmäßig zu beurteilen, wobei hingegen durch den Prozess „8.2.3 Disziplinarverfahren“ bestimmte Vorgaben adressiert werden, um mögliche Disziplinarverfahren einzuleiten, sofern der Mitarbeiter absichtlich oder fahrlässig gravierende Sicherheitsvorfälle verursacht hat [vgl. ITSM2008, S.144ff.].

Wenn die Beauftragung abgeschlossen oder weitergeleitet werden soll, müssen folgende Maßnahmen beachtet werden: Zunächst wird durch den Prozess „8.3.1 Verantwortliche bei der Beendigung“ von ISO 27002 eine Zuständigkeit bzw. ein Verfahren für den Wechsel einer Beauftragung bzw. die Beendigung gefordert. Weiterhin muss die Rückgabe der für die bisherige Tätigkeit genutzten Informationswerte der Organisation durch den Prozess „8.3.2 Rückgabe von organisationseigenen Werten“ bestätigt werden. Dies könnten beispielsweise Schlüssel, Chipkarten, Unterlagen oder Rechner sein. Darüber hinaus müssen die Zugangsrechte zur Information oder informationsverarbeitenden Einrichtung entweder aufgehoben, wenn die Beauftragung beendet ist oder an die Änderungen angepasst werden[vgl. ITSM2008, S.146f.].

Beschaffe und Warte Anwendung		
COBIT	**ISO/IEC 27002**	**ITIL**
AI2.2 Detailliertes Design		**SD 4.2 Service Level Management**
AI2.3 Anwendungskontrollen und Nachvollziehbarkeit	**12.2.1 Überprüfung von Eingabedaten**	
	12.2.2 Kontrolle der internen Verarbeitung	
	12.2.3 Integrität von Nachrichten	
	12.2.4 Überprüfung von Ausgabedaten	
AI2.4 Sicherheit und Verfügbarkeit der Anwendung	**11.6.1 Einschränkung von Informationszugriff**	
	11.6.2 Isolation sensibler Systeme	
AI2.5 Konfiguration und Implementierung von beschaffter Anwendungssoftware		
AI2.8 Software-Qualitätssicherung	**10.3.2 System-Abnahme**	
DS5.8 Verwaltung kryptografischer Schlüssel	**12.3.1 Leitlinie zur Anwendung von Kryptografie**	
	12.3.2 Verwaltung kryptografischer Schlüssel	
DS 5.9 Schutz vor, Erkennung und Korrektur von bösartiger Software	**10.4.1Maßnahmen gegen Schadsoftware**	
	10.4.2 Schutz vor mobiler Software	

Tabelle 3.22: Beschaffe und warte Anwendung

Der Teilprozess „Beschaffe und Warte Anwendung“ stellt sicher, dass einerseits die Anwendungen nach Sicherheitsanforderungen beschafft werden, und diese andererseits gegen Sicherheitsbedrohung gepflegt werden.

Um die Anwendungen nach Sicherheitsanforderungen schaffen zu können, wird zuerst durch den Prozess „AI2.2 Detailliertes Design“ ein Beschaffungsplan benötigt, der die Sicherheitsanforderungen enthält. Anschließend werden die Anwendungen durch den Prozess „AI2.3 Anwendungskontrollen und Nachvollziehbarkeit“ hinsichtlich der Richtigkeit und Vollständigkeit von Inputs und Outputs kontrolliert, damit Fehler, Verluste, unbefugte Veränderungen oder ein Missbrauch

von Informationen in Anwendungen verhindert werden kann. Außerdem sollen alle Beschaffungsinformationen genau dokumentiert werden, um den zukünftigen Audit zu ermöglichen. Darüber hinaus müssen durch den Prozess „AI2.4 Sicherheit und Verfügbarkeit der Anwendung“ die Anforderungen an Sicherheit und Verfügbarkeit der Anwendungen in Bezug auf identifizierte Risiken behandelt werden, vor allem bei Autorisierungsmechanismen, Integrität von Informationen, Zugriffsschutz und Backup. Weiterhin wird durch den Prozess „AI2.5 Konfiguration und Implementierung beschaffter Anwendungssoftware“ eine Testumgebung für die Konfiguration und Implementierung beschaffter Anwendungen aufgebaut, um sicherzustellen, dass die neuen Anwendungen mit bestehenden Anwendungen und Systemen übereinstimmen. Durch das von dem Prozess „AI2.8 Software-Qualitätssicherung“ definierte Abnahmekriterium, werden die beschafften Anwendungen, die definierte oder vereinbarte Qualität beinhalten, abgenommen [vgl. Goltsche2006, S. 86ff.].

Um die Sicherheit während des Benutzens der Anwendungen zu gewährleisten, wird heutzutage die Kryptografie von vielen IT-Anwendungen eingesetzt. Durch den Prozess „12.3.1 Leitlinie zur Anwendung von Kryptografie“ wird eine Leitlinie zur Anwendung kryptografischer Maßnahmen entwickelt, die dafür sorgt, die Maßnahmen umzusetzen. Außerdem sollen durch den Prozess “12.3.2 Verwaltung kryptografischer Schlüssel“ ein Verfahren sichergestellt werden, um die kryptografischen Schlüssel in der Organisation verwalten zu können [vgl. ITSM2008, S.192]. Schließlich müssen die Anwendungen vor nicht-integere Software geschützt werden, vor allem aber vor Schadsoftware und nicht genehmigten mobilen Programmcodes.

Beschaffe und Warte Technologie Infrastruktur		
COBIT	**ISO/IEC 27002**	**ITIL**
AI3.1 Beschaffensplan für technologische Infrastruktur		
AI3.2 Schutz und Verfügbarkeit von Infrastrukturressourcen	**12.1.1 Analyse und Spezifikation von Sicherheitsanforderungen**	**SD 4.6 Information Security Management**
AI3.3 Wartung von Infrastruktur	**9.2.4 Instandhaltung von Gerätschaften**	
	12.6.1 Kontrolle technischer Schwachstellen	
AI3.4 Testumgebung	**10.1.4 Aufteilung von Entwicklungs-, Test- und Produktiveinrichtungen**	**ST 4.4 Release and Deployment**
		ST 4.5 Service Validation and Testing

Tabelle 3.23: Beschaffe und warte Technologie Infrastruktur

Die Technologie-Infrastruktur stellt die Basis für sämtliche durch Informationstechnologie unterstützten Geschäftsprozesse, denn die automatischen Lösungen und Anwendungen müssen darauf aufgesetzt werden. Fehler in der Technologie-Infrastruktur können verheerende Auswirkungen verursachen.

Der Teilprozess „Beschaffe und warte Technologie Infrastruktur“ stellt einerseits sicher, dass die Technologie-Infrastruktur nach Sicherheitsanforderungen beschafft wird, und bietet andererseits Maßnahmen, wie die Technologie-Infrastruktur selbst geschützt werden kann.

Um die Technologie-Infrastruktur nach Sicherheitsanforderungen zu beschaffen, wird zunächst durch den Prozess „AI3.1 Beschaffungsplan für technologische Infrastruktur“ ein Einkaufsplan festgelegt, der den Geschäftsanforderungen in funktionaler und technischer Hinsicht gerecht wird und im Einklang mit der strategischen technologischen Ausrichtung steht. Weiterhin sorgt der Prozess „AI3.2 Schutz und Verfügbarkeit von Infrastrukturressourcen“ von COBIT dafür, dass die Maßnahmen implementiert, die beschaffte Infrastrukturkomponenten geschützt bzw. ihre Verfügbarkeit und Integrität gewährleistet werden können. Danach sollen die

Infrastrukturkomponenten durch den Prozess „AI3.4 Testumgebung“ die erreichte Testumgebung überprüfen, damit frühzeitig sichergestellt werden kann, ob die Infrastruktur wirksam sowie wirtschaftlich Machbar und mit bestehenden Anwendungen und der Infrastruktur integriert werden kann. Des Weiteren werden durch den Prozess „AI3.3 Wartung von Infrastruktur“ eine Strategie und ein Plan für die Wartung der Infrastruktur entwickelt bzw. sichergestellt, dass alle Änderungen entsprechend des unternehmensweiten Änderungsmanagement Prozesses gesteuert ablaufen [vgl. ITGI2005, S.90].

Manage Konfiguration		
COBIT	**ISO/IEC 27002**	**ITIL**
DS9.1 Konfigurationsinformation und Referenzversionen	**7.1.1 Inventar der organisationseigenen Werte**	**ST 4.3 Service Asset and Configuration Management**
DS9.2 Identifikation und Wartung von Konfiguration Items	**7.1.2 Eigentum von organisationseigenen Werten**	
	7.2.2 Kennzeichnung von und Umgang mit Informationen	
	7.1.3 Zulässiger Gebrauch von organisationseigenen Werten	
DS9.3 Review der Integrität der Konfiguration		

Tabelle 3.24: Manage Konfiguration

Configuration Items (CI) umfassen vor allem Hardware, Software, Gebäude, Personen und formale Dokumentationen, die verwaltet werden müssen, um einen IT-Service bereitstellen zu können. Diese werden in der Configuration Management Database (CMDB) gespeichert.

Der Prozess „ST 4.3 Service Asset and Configuration Management“ von ITIL bietet die Möglichkeit, einen Überblick sämtlicher CIs einer IT-Infrastruktur zu erzeugen und die Abhängigkeiten der CIs untereinander zu verdeutlichen. Dafür wird ein logisches Modell aufgebaut, in dem alle CIs in dem jeweils benötigten Detaillierungsgrad wieder zu finden sind[vgl. ITSM2008, S. 84f.].

Aus dem Sicherheitsaspekt her betrachtet, werden durch das Konfigurationsmanagement sämtliche CIs in CMDB nach den Informations-sicherheitsanforderungen, die sich aus den Anforderungen der Geschäftsprozesse ableiten, klassifiziert. Eine Klassifikation wird hinsichtlich der drei Hauptsicherheitsziele, nämlich Vertraulichkeit, Verfügbarkeit und Integrität, vorgenommen. Gemäß der betroffenen Klassifikation, müssen CIs von entsprechenden Sicherheitsmaßnahmen ergriffen werden. Durch das Konfigurationsmanagement lässt sich zudem leichter eine Analyse hinsichtlich Sicherheitsstörung durchführen.

Ermögliche Betrieb und Verwendung		
COBIT	**ISO/IEC 27002**	**ITIL**
AI4.1 Planung für operative Lösung		**ST 4.4 Release and Deployment**
AI4.2 Transfer von Knowledge an den Fachbereich		**ST 4.7 Knowledge management**
AI4.3 Transfer von Knowledge and Endbenutzer		
AI4.4 Transfer von Knowledge an Betriebs- und Supportmitarbeiter		**ST 4.7 Knowledge management**
	10.1.1 Dokumentierte Betriebsprozesse	
	13.2.2 Lernen von Informationssicherheitsvorfällen	**SO 4.4 Problem Management**
		SO 4.6 Operational activities of processes covered in other lifecycle phase
AI7.1 Schulung	**8.2.2 Sensibilisierung, Ausbildung und Schulung für Informationssicherheit**	**ST 4.4 Release and Deployment**

Tabelle 3.25: Ermögliche Betrieb und Verwendung

Der Teilprozess “Ermögliche Betrieb und Verwendung“ stellt durch die Entwicklung und Pflege von Anwender- und Betriebshandbüchern sowie Schulungen sicher, dass die Anwendungen und Infrastruktur korrekt und sicher verwendet werden. Außerdem muss darauf geachtet werden, dass die Anwender-Handbücher, Betriebshandbücher und Schulungsunterlagen auch in einem strukturierten Prozess entwickelt werden sollten. Dazu werden folgende Prozesse von COBIT benötigt:

Durch den Prozess „AI4.1 Planung für operative Lösung “ wird ein Plan entwickelt, der Betriebsanforderungen und Service-Level identifiziert und dokumentiert. Auf Basis des Plans werden entsprechende Kenntnisse und Fertigkeiten durch jeweilige Prozesse von COBIT (siehe Tabelle 3.25) in die notwendige Form zum Business Management, den Endanwendern und in den Betrieb der IT transferiert. Damit kann sowohl die Verantwortung als auch bestimmte Fähigkeiten erkannt werden, um die Anwendungen und Infrastruktur korrekt und sicher betreiben zu können.

Weiterhin soll durch den Prozess „AI7.1 Schulung“ sichergestellt werden, dass nach jedem Entwicklungs-, Implementierungs- oder Änderungsprojekt die Mitarbeiter der entsprechenden Abteilung und das Betriebspersonal der IT im Einklang mit bestimmten Schulungs- und Implementierungsplänen und den korrekten Unterlagen ausgebildet werden [vgl. ITGI2005, S.106].

Manage Daten		
COBIT	**ISO/IEC 27002**	**ITIL**
DS11.2 Speicherungs- und Aufbewahrungsvorkehrungen		
DS1.3 Medien-Bibliotheksmanagementsystem	**10.7.1 Verwaltung von Wechselmedien**	
DS11.4 Entsorgung	**10.7.2 Entsorgung von Medien**	
DS11.6 Sicherheitsanforderungen für Management der Daten	**10.7.3 Umgang mit Informationen**	
	10.7.4 Sicherheit der Systemdokumentation	
	12.4.2 Schutz von Test-Daten	
	12.4.3 Zugangskontrolle zu Quellcode	
	12.4.1 Kontrolle von Software im Betrieb	
DS5.11 Austausch sensitiver Daten	**10.8.1 Regelwerk und Verfahren zum Austausch von Informationen**	
	10.8.2 Vereinbarungen zum Austausch von Informationen	
	10.8.3 Transport physischer Medien	
	10.8.4 Elektronische Mitteilungen/ Nachrichten (Messaging)	
	10.8.5 Geschäftsinformationssysteme	
DS11.5 Backup und Wiederherstellung	**10.5.1 Information Backup**	

Tabelle 3.26: Manage Daten

Der Teilprozess „Manage Daten“ gewährleistet, dass zum einen alle Daten in Vollständigkeit, Integrität und Gültigkeit gespeichert sowie entsorgt und zum anderen sensitive Daten völlig geschützt werden können.

Mit Hilfe des Prozesses „DS11.2 Speicherungs- und Aufbewahrungs-vorkehrungen“ soll eine Methode für die Datenspeicherung und -archivierung definiert werden, damit Daten im Zugriff und verwendbar bleiben. Die Verfahren sollten Anforderungen bezüglich Wiederauffindung, Kostengünstigkeit, kontinuierliche Integrität und Sicherheit beachten. Nicht nur Daten, sondern auch Datenträger sollen sich auf Sicherheitsziele beziehen. Durch den Prozess “10.7.1 Verwaltung von Wechselmedien“ werden alle Datenträger vom Einkauf bis hin zum Entsorgen dokumentiert und zentral verwaltet bzw. durch den Prozess „10.7.3 Umgang mit Informationen“ nach Angaben zum Inhalt klassifiziert werden. Dadurch können die Informationen darauf vor unerlaubter Veröffentlichung oder Missbrauch geschützt werden. Bei Entsorgung verschiedener Datenträger, werden systematische Verfahren mit entsprechenden Methoden gefordert. Diese Aufgabe wird von dem Prozess „10.7.2 Entsorgung von Medien“ übernommen. Weiterhin soll besonders darauf geachtet werden, dass der Zugriff auf sensitive Informationen und Software von Geräten oder Datenträgern bei deren Entsorgung verhindert werden soll [vgl. ITSM2008, S.163f.].

Die Systemdateien und Dokumentationen sollen als hoch sicherheitsgestufte Daten gekennzeichnet und daher besonderes geschützt werden. Dazu bietet der Teilprozess „Manage Daten“ folgende Maßnahmen an: Zunächst wird der Sicherheitsdokumentation durch den Prozess „10.7.4 Sicherheit der Systemdokumentation“ ein bestimmter Wert zugemessen und geschützt. Weiterhin ist es für Systemdateien sehr wichtig, dass diese weder absichtlich noch unabsichtlich manipuliert werden. Zuerst fordert der Prozess „12.4.1 Kontrolle von Software im Betrieb“ nach Installation der Software auf dem entsprechenden System eine regelmäßige Kotrolle gegen die Manipulation von Systemdateien. Auch die Test-Daten werden durch den Prozess „12.4.2 Schutz von Test-Daten“ sorgfältig ausgewählt, geschützt und kontrolliert. Darüber hinaus soll durch den Prozess „12.4.3 Zugangskontrolle zu Quellcode“ der Zugriff auf den Quellcode beschränkt werden [vgl. ITSM2008, S.193].

Die sensitiven Daten sollen besonderes während des Austausches gesichert werden. Dafür ist der Prozess „DS5.11 Austausch sensitiver Daten“ zuständig. Hier finden notwendige Maßnahmen statt, die sicherstellen, dass sensitive Daten nur auf vertrauliche Art und Weise zwischen autorisierter Aufgabe und Empfang transportiert werden [vgl. ITGI2005, S.132].

Schließlich ist ein Backup-Verfahren für Daten und Dokumentation sehr wichtig, um die Verfügbarkeit und Kontinuität von IT-Service zu sichern. Durch den Prozess „10.5.1 Information Backup“ soll zunächst eine so genannte „Backup-Methode“ definiert werden. Dies bezieht sich auf das von der Organisation in Kraft gesetzte dokumentierte Verfahren der Datensicherung, das eine Vielzahl von Aspekten abdecken muss: Die Grundsätze, die technische Durchführung, ihr Nachweis, die „Aufbewahrung“ der Backup-Medien, das Verfahren der Wiedereinspielung [vgl. ITSM2008, S.161].

Manage die physische Umgebung		
COBIT	**ISO/IEC 27002**	**ITIL**
DS12.1 Standortwahl und Layout von Einrichtungen		
DS12.2 Physische Sicherheitsmaßnahmen	**9.1.1 Sicherheitszonen**	
	9.1.2 Zutrittskontrolle	
	9.1.3 Sicherung von Büros, Räumen und Einrichtungen	
	9.1.5 Arbeit in Sicherheitszonen	
	9.1.6 Öffentlicher Zugang, Anlieferungs- und Landezonen	
DS12.3 Physischer Zugang		
DS12.4 Schutz gegen Umwelteinflüsse	**9.1.4 Schutz vor Bedrohungen von Außen und aus der Umgebung**	
DS12.5 Management von physischen Einrichtungen	**9.2.1 Platzierung und Schutz von Betriebsmitteln**	
	9.2.2 Unterstützende Versorgungseinrichtungen	
	9.2.3 Sicherheit der Verkabelung	
	9.2.4 Instandhaltung von Gerätschaften	
	9.2.5 Sicherheit von außerhalb des Standorts befindlicher Ausrüstung	
	9.2.6 Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln	
	9.2.7 Entfernung von Eigentum	

Tabelle 3.27: Manage die physische Umgebung

Ziel des Teilprozesses „Manage die physische Umgebung“ ist es, eine passende physikalische Umgebung durch das Managen der Einrichtungen zu erzeugen, welche die IT-Gerätschaften und das Personal gegen Menschen-verursachte oder natürliche Schadensereignisse schützt und die dadurch verursachten Unterbrechungen des Geschäftsbetriebes minimiert [vgl. Goltsche2006, S.138].

Dazu werden zunächst durch den Prozess „DS12.1 Standortwahl und Layout von Einrichtungen“ die physischen Standorte für IT-Anwendungen ausgewählt. Die Standorte sollen einerseits die Strategie der Geschäftsbereiche unterstützen, und

andererseits die Risiken der Naturgewalten sowie Menschen-verursachten Probleme zu beachten. Nach der Auswahl der Standorte für IT-Anwendungen ist die Bestimmung der physischen Sicherheitsmaßnahmen an der Reihe. Durch den Prozess „DS12.2 Physische Sicherheitsmaßnahmen“ werden zunächst die Sicherheitszonen sowie die Versand- und Anlieferungszonen festgestellt, wobei insbesondere die Kontrolle für den Zutritt zu verschiedenen Sicherheitszonen geprüft werden muss. Weiterhin sollen in den Sicherheitszonen Sicherheitsgründe und -regelungen eingerichtet werden. Auch eine Festlegung der Verantwortlichkeiten für die Überwachung der Sicherheitszonen bzw. die Verhaltensregeln in Sicherheitszonen wird gefordert [vgl. ITGI2005, S.162].

Weiterhin sollen gemäß dem Prozess „DS12.3 Physischer Zugang“ alle Personen, inklusive Personal, temporäres Personal, Kunden, Lieferanten, Besucher oder andere Drittparteien, die das Gelände, Gebäude oder den Arbeitsbereich betreten, begründet, genehmigt, protokolliert und überwacht werden [vgl. ITGI2005, S.162].

Obwohl Naturgewalten einen relativ kleinen Teil von Problemen ausmachen, ist die Entwicklung und Implementierung der Maßnahmen zum Schutz gegen Umweltfaktoren notwendig. Durch den Prozess „DS12.4 Schutz gegen Umwelteinflüsse“ werden insbesondere die Ausrüstung und Geräte zur Überwachung und Steuerung der Umwelt installiert[vgl. ITGI2005, S.162].

Schließlich wird der Prozess „DS12.5 Management von physischen Einrichtungen“ gefordert, um alle physischen Einrichtungen zu verwalten. Allerdings werden auch von ISO 27002 sieben Maßnahmen dazu angeboten. Hier werden alle physischen Einrichtungen von Besorgung, Einrichtung bis hin zur Entsorgung betreut und verwaltet.

3.4.5 Messen der Performance

Monitore und evaluiere IT-Performance		
COBIT	**ISO/IEC 27002**	**ITIL**
	10.10.1 Auditprotokolle	**CSI 4.1 The 7-Step Improvement Process**
ME1.2 Definition und Sammlung von Monitoring-Daten	**10.10.2 Überwachung der Systemnutzung**	
	10.10.3 Schutz von Protokollinformationen	
	10.10.4 Administrator- und Betreiberprotokolle	
	10.10.5 Fehlerprotokolle	
	10.10.6 Zeitsynchronisation	
ME1.4 Beurteilung der Performance		
ME1.5 Berichte an geschäftsführende Gremien		
ME1.6 Verbesserungsmaßnahmen		

Tabelle 3.28: Monitore und evaluiere IT-Performance

Ziel des Teilprozesses „Monitore und evaluiere IT-Performance“ ist es, die Performance der Informationssicherheitsmaßnahmen regelmäßig zu überwachen und zu bewerten, damit das Sicherheitsmanagement konstant verbessert werden kann.

Um die Performance der Informationssicherheit effektiv zu überwachen, sollen folgende Objekte aufgedeckt und aufgezeichnet werden:

Mit Hilfe des Prozesses „10.10.1 Auditprotokolle“ werden in besonderem Maße Fehlerzustände und Alarmsignale, Sicherheitsvorfälle und Benutzeraktivitäten überwacht und aufgezeichnet. Hierbei können sich Erkenntnisse über die Wirksamkeit von Maßnahmen, die Einhaltung organisatorischer Regeln oder kritische Fehlerzustände der Systeme ergeben. Weiterhin können durch den Prozess „10.10.5 Fehlerprotokolle“ Fehler der Systeme protokolliert und analysiert werden, mit dem Ziel der Fehlerbehebung, indem entsprechende Maßnahmen dafür ergriffen werden

[vgl. ITSM2008, S.172ff.].

Der Prozess „10.10.2 Überwachung der Systemnutzung“ fordert, mit Hilfe der Überwachung der Nutzung von Systemen, die Kennzahlen für die Auslastung der Systeme zu ermitteln. Diese Kennzahlen dienen der Kapazitätsplanung und der Vermeidung von Engpässen [vgl. ITSM2008, S.173.].

Außerdem müssen die Aktivitäten von Systemadministratoren und Betreibern durch den Prozess „10.10.4 Administrator- und Betreiberprotokolle“ protokolliert werden, um sicherzustellen, dass die Systemadministratoren und Betreiber die hohen Privilegien nicht missbrachen [vgl. ITSM2008, S.174.].

Des Weiteren ist es wichtig, durch den Prozess „10.10.6 Zeitsynchronisation“ zu gewährleisten, dass alle Systeme einer Organisation auf eine vereinbarte, genaue Referenzzeit synchronisiert werden, damit eine vergleichbare Basis für die Analyse und Auswertung der Überwachungsdaten aufgebaut werden kann [vgl. ITSM2008, S.175.].

Schließlich weist der Prozess „10.10.3 Schutz von Protokollinformationen“ darauf hin, dass die Protokolle aus Sicherheitsgründen in besonderem Maße geschützt werden sollen. Das heißt, der Zugriff zu Aufzeichnungsverfahren und die aufgezeichneten Daten müssen beschränkt, und Änderungen sowie Manipulationen verhindert werden.

Die durch die Überwachung gesammelte Performance der Informationssicherheits-systeme werden durch den Prozess “ME1.4 Beurteilung der Performance“ beurteilt, um frühzeitig alle Ursachen der Performance zu erhalten. Weiterhin werden durch den Prozess „ME1.5 Berichte an geschäftsführende Gremien“ Managementberichte erstellt. Diese Managementberichte beinhalten Aktivitäten, um Performanceprobleme zu lösen. Anschließend werden die Abweichungen von erwarteter Performance identifiziert und geeignete Management-Aktivitäten eingeleitet und schließlich darüber berichtet [vgl. ITGI2005, S.172].

Letztlich sollen weiterhin auf Basis der vorgelegten Überwachung, Beurteilung und Berichterstattung, einerseits die Performance sowie andererseits die Abhilfemaßnahmen definiert werden, damit das Informationssicherheitssystem kontinuierlich optimiert werden kann.

Monitore und evaluiere Internal Controls		
COBIT	**ISO/IEC 27002**	**ITIL**
ME2.1 Monitoring des Control Frameworks	**15.2.1 Einhaltung von Sicherheitsregelungen und -standards**	
ME2.2 Übergeordneter Review		
ME2.3 Ausnahmebehandlung für Controls		
ME2.4 Selbstbeurteilung der Steuerung		
ME2.5 Bestätigung der Internal Controls		
ME2.6 Internal Controls bei Dritten		
ME2.7 Verbesserungsmaßnahmen		
ME2.5 Bestätigung der Internal Controls	**15.2.2 Prüfung der Einhaltung technischer Vorgaben**	

Tabelle 3.29: Monitore und evaluiere Internal Controls

Der Teilprozess „Monitore und evaluiere Internal Controls“ stellt sicher, dass die Manager nicht nur Sicherheitsvorgaben erstellen, sondern auch deren Einhaltung kontrollieren, welche in den meisten Unternehmen vernachlässigt werden.

Der Prozess „15.2.1 Einhaltung von Sicherheitsregelungen und -standards“ fordert, dass die Manager alle Sicherheitsverfahren in ihrem Verantwortungsbereich korrekt anwenden und entsprechend regelmäßig Kontrollen durchführen, um die Einhaltung von Sicherheitsregelungen und –standards zu erreichen. Nicht nur die Wirksamkeit des Sicherheitsmanagements soll überprüft werden, sondern auch die technischen Vorgaben für die Sicherheit von IT-Systemen sollen eingehalten werden, damit die

technische Basis für die Durchführung des Sicherheitsmanagements gesichert werden kann. Durch den Prozess „15.2.2 Prüfung der Einhaltung technischer Vorgaben“ werden beispielsweise die Einhaltung von VDE-Vorschriften und die Umgebungsbedingungen für IT-Systeme (Temperatur, Feuchtigkeit) überprüft [vgl. ITSM2008, S.208].

Unabhängige Bestätigung		
COBIT	**ISO/IEC 27002**	**ITIL**
ME2.5 Bestätigung der Internal Controls	**6.1.8 Unabhängige Überprüfung der Informationssicherheit**	
ME4.7 Unabhängige Bestätigung		
	15.3.1 Maßnahmen für Revisionen von Informationssystemen	
	15.3.2 Schutz von Revisionswerkzeugen für Informationssysteme	

Tabelle 3.30: Unabhängige Bestätigung

Der Teilprozess „Unabhängige Bestätigung“ gewährleistet, dass notwendige Überprüfungen in der Organisation von den unabhängigen Personen, die nicht in der Alltagstätigkeit der Organisation oder dem operationellen Betrieb der Systeme angehören, regelmäßig stattfinden sollen.

Um den Ansatz einer Organisation zur Handhabung und Umsetzung der Informationssicherheit in regelmäßigen Zeitabständen oder nach wesentlichen Änderungen an der implementierten Sicherheit zu überprüfen, fordert der Prozess „6.1.8 Unabhängige Überprüfung der Informationssicherheit“ interne und externe Audits [vgl. ITSM2008, S.209f.].

Darüber hinaus sollen auch die Audits für Informationssysteme, in denen die Betriebe sich befinden, sorgfältig geplant und durchgeführt werden, damit das Risiko von Störungen der Geschäftsprozesse so weit wie möglich reduziert werden kann.

Gleichzeitig muss jedoch auch die Sicherheit der Audittools gewährleistet werden, damit zum einen eine nicht autorisierte und unbeabsichtigte Nutzung verhindert, und zum anderen Manipulationen an den Tools selbst ausgeschlossen werden können, die möglicherweise verhindern, dass Sicherheitslücken entdeckt werden [vgl. ITSM2008, S. 210ff.].

Kapitel 4

Referenzmodell

In diesem Kapitel wird das Referenzmodell von Information Security Governance (ISG) in ARIS dargestellt. Wie bereits in Kapitel 3 analysiert, besitzt das Referenzmodell von Information Security Governance eine Drei-Ebenen-Struktur. Diese drei Ebenen präsentieren jeweils die Hauptaufgaben, Teilaufgaben und Aktivitäten von Information Security Governance, deshalb wird das Referenzmodell dadurch hierarchisch aufgebaut.

Wie bereits in Kapitel 2.5.2 erwähnt, wird im Rahmen der Modellierung eine Sechs-Grundsätze-Struktur als wesentliches Qualitätskriterium gefordert, wobei dessen Umsetzung bei der Modellierung näher erklärt wird.

Um den Grundsatz der Richtigkeit zu erfüllen, muss hier insbesondere die Vollständigkeit der syntaktischen Richtigkeit bzw. der Konsistenz, die der semantischen Richtigkeit zugeordnet wurde, gewährleistet werden.[14] Damit gilt hier die Gewährleistung der Vollständigkeit der Haupt-, Teilaufgaben bzw. Aktivitäten von Information Security Governance als eine der entscheidendsten Anforderungen, damit das Referenzmodell für eine Umsetzung von Information Security Governance als Ganzes herangezogen werden kann. Außerdem wird die Konsistenz hier als Widerspruchsfreiheit definiert [vgl. Ros96, S.98]. Insbesondere die möglichen n:m-Beziehungen zwischen den jeweiligen Haupt- sowie Teilaufgaben und Aktivitäten müssen als Anforderung für eine Konsistenz berücksichtigt werden. Um das Problem zu lösen, werden in dieser Arbeit sämtliche Beziehungen nach Entscheidungen zu einer n:1-Beziehung geschaffen.

[14] Dabei ist ausdrücklich zwischen der Konsistenz des Modellsystems gegenüber dem Metamodell als Anforderung des Grundsatzes der syntaktischen Richtigkeit und der Konsistenz zu anderen Modellsystemen als Anforderung des Grundsatzes der semantischen Richtigkeit zu differenzieren. [Ros96. S. 96]

Damit der Grundsatz der Relevanz berücksichtigt wird, beinhaltet deshalb das Information Security Governance Referenzmodell hier lediglich diejenigen Objekte, welche in direkter Relevanz zur Informationssicherheit stehen. Des Weiteren werden auch nur die Aktivitäten der drei Standards und Best Practices für die entsprechenden Teilaufgaben der Information Security Governance Referenzmodell bearbeitet bzw. zugeordnet, die relevant für den Zweck des Referenzmodells sind.

Unter den Grundsatz der Wirtschaftlichkeit, wird hier die Beibehaltung der Anpassungsfähigkeit und Erweiterbarkeit des Information Security Governance Referenzmodells verstanden, daher wird in dieser Arbeit der Versuch unternommen, einen anpassenden Detailgrad aufzufinden, wobei auch die Erweitungsmöglichkeit nicht eingeschränkt werden soll.

Um den Grundsatz der Klarheit zu gewährleisten, wird in dieser Arbeit die Modellierung streng gemäß der Anordnungsregeln durchgeführt, wie z.B. die vertikale etablierte Modellierung bei ereignisgesteuerten Prozessketten. Weiterhin wird die Anschaulichkeit des Referenzmodells auch durch den Einhalt der in Abbildung 3.1 (siehe Kapitel 3.1) definierten Drei-Ebenen-Struktur erhöht. Es fordert beispielsweise, dass Elemente immer in einer entsprechenden Ebene modelliert und zudem in einem deutlich dargelegten, sachlogischen Zusammenhang mit anderen gesetzt werden sollen.

Um den Grundsatz der Vergleichbarkeit schaffen zu können, ist eine einheitliche Grundlage für die gesamte Modellierung wichtig, damit wird in dieser Arbeit die Abbildung 3.1 (siehe Kapitel 3.1) als Grundlage für das Referenzmodell verwendet.

Der Grundsatz des systematischen Aufbaus fordert ein sichtenübergreifendes Metamodell, das für die Sichtintegration relevant ist. Ein solches Metamodell, wie zum Beispiel von ARIS, bietet die Möglichkeit an, dass das auf unterschiedliche Sichten erzeugte Modellobjekt stets Verweise impliziert.

Im Folgenden wird jede Ebene dargestellt und näher erläutert.

Auf der Ebene 1 wird eine einfache Übersicht auf einer Einstiegsseite für das ISG-Referenzmodell gezeigt. Hier werden alle Hauptaufgaben von Information Security Governance und dessen grundlegende externe Einbindung bzw. ihre Beziehung miteinander abgebildet. Im Anhang D ist eine vergrößerte Darstellung zu finden.

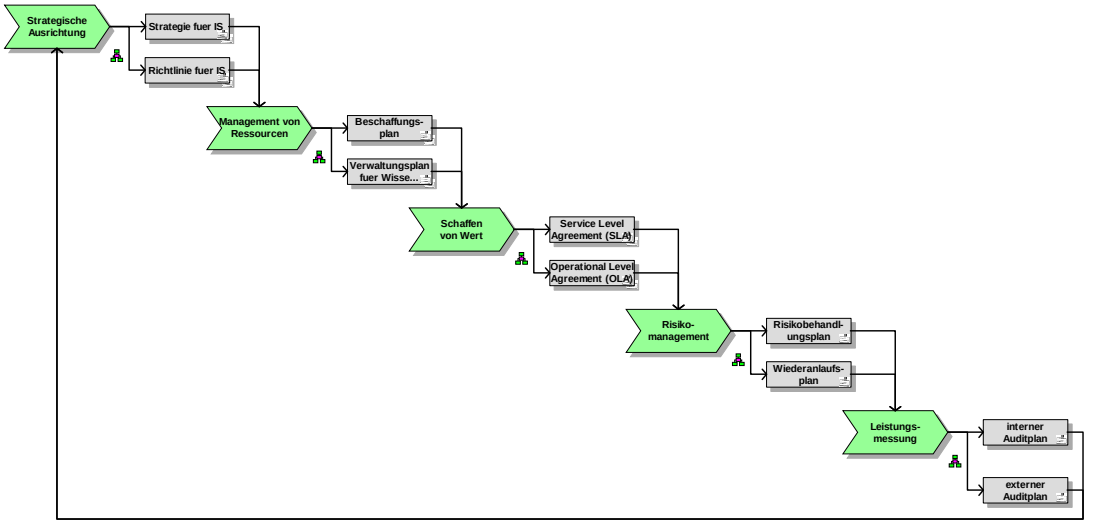

Abbildung 4.1: Ebene 1 der Gesamtübersicht zum ISG

Die Ebene 2 und 3 der ISG-Struktur wird in ARIS aus einer gemeinsamen Sicht dargestellt. Hier werden die Teilaufgaben von ISG bzw. deren anpassende detaillierte Prozesse von den drei Standards bzw. Best Practices, welche mit weiterer EPKs verlinkt sind, abgebildet. Im Anhang E befindet sich eine detaillierte Darstellung über die Prozess-Übersicht bzw. über das Prozess-Detailmodell.

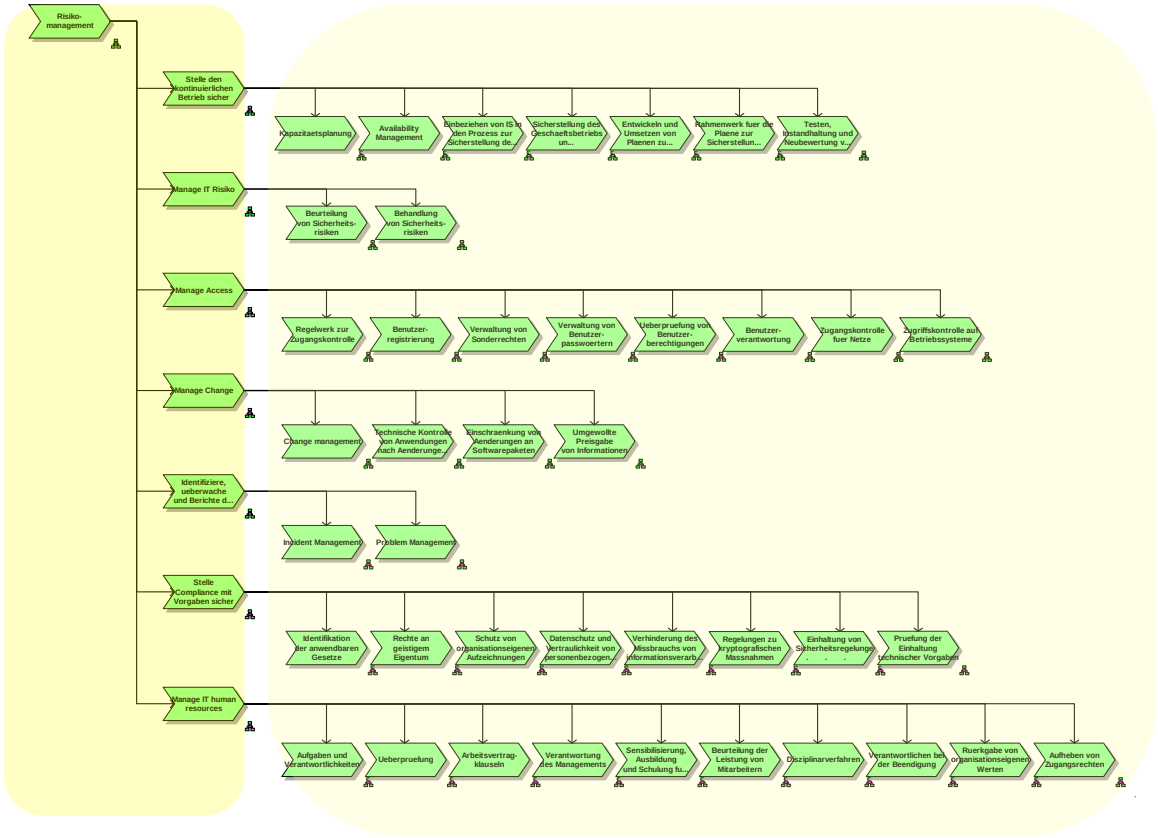

Abbildung 4.2: Ebene 2 und 3 - Prozess-Übersicht bzw. –Detailmodell

Für jeden detaillierten Prozess auf Ebene 3 wird ein EPK hintergelegt, die EPKs umfassen die notwendigen Arbeitsschritte für die Gewährleistung des Ziels vom jeweiligen Prozess. Abbildung 4.3 zeigt beispielsweise die Prozesskette für das Änderungs-Management.

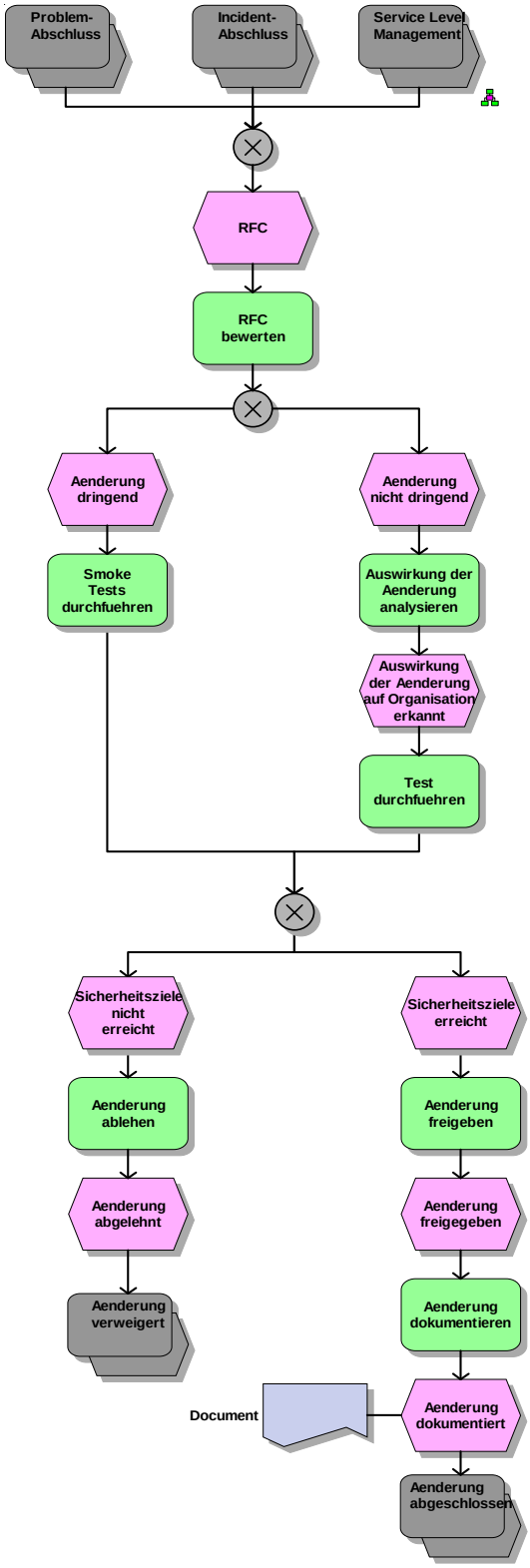

Abbildung 4.3: Prozesskette für das Änderungs-Management

In den folgenden Abbildungen wird die vollständige Prozess-Hierarchie des Referenzmodells von Information Security Governance dargestellt. Im Anhang F sind die vergrößerten Darstellungen zu finden.

- Strategische Ausrichtung

Die Hauptaufgabe Strategische Ausrichtung von Information Security Governance repräsentiert den ersten Schritt für die Informationssicherheit in Unternehmen. Durch die jeweiligen unterstützten Teilaufgaben wird die Strategie bzw. die Richtlinie für Informationssicherheit aufgestellt. Zudem sind auch die Sicherheitsverantwortlichkeiten und die Kommunikationsrichtung definiert, damit ein gemeinsames Verständnis über die anzustrebende Informationssicherheit erreicht werden kann (siehe auch Kapitel 2.4.3). Abbildung 4.4 zeigt alle Teilaufgaben von ISG, die die Hauptaufgabe „Strategische Ausrichtung“ unterstützen und die zu den Teilaufgaben zugeordnete Aktivität des jeweiligen Standards bzw. Best Practices.

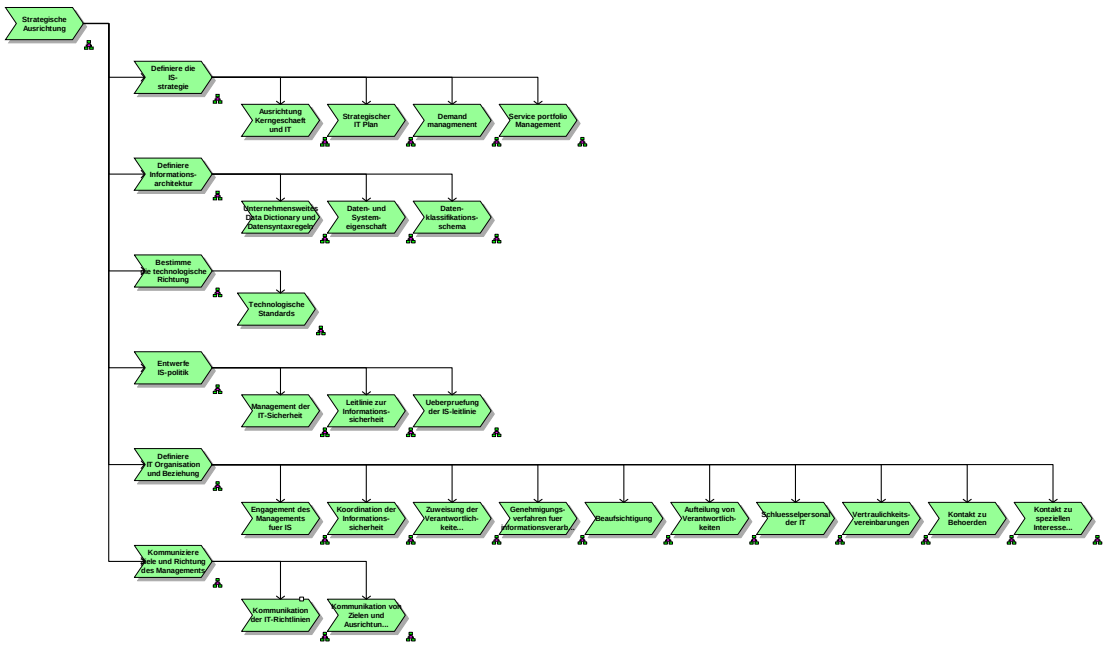

Abbildung 4.4: Prozessmodell Strategische Ausrichtung

- Management von Ressourcen

Die Hauptaufgabe Management von Ressourcen von Information Security Governance optimiert das Wissen sowie die IT Infrastruktur eines Unternehmens. Darüber hinaus stellt es durch die Bereitstellung von IT Ressourcen (Menschen, Anwendungen, Technologie, Einrichtungen, Daten) den Schlüsselfaktor für eine erfolgreiche Performance der Informationssicherheit dar (siehe auch Kapitel 2.4.3). Abbildung 4.5 zeigt alle Teilaufgaben von ISG, die die Hauptaufgabe „Management von Ressourcen“ unterstützen und die zu den Teilaufgaben zugeordnete Aktivität des jeweiligen Standards bzw. Best Practices.

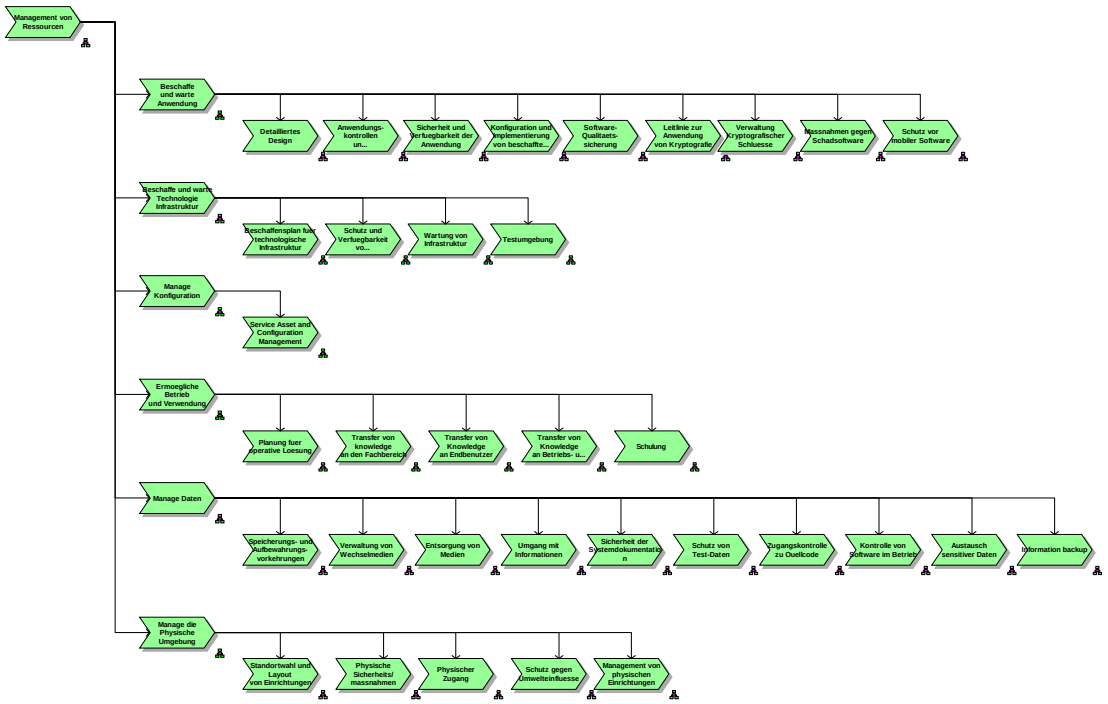

Abbildung 4.5: Prozessmodell Management von Ressourcen

- Schaffen von Wert

Die Hauptaufgabe Schaffen von Wert von Information Security Governance erzielt mit geringstem Aufwand die größten Erträge bei der Gewährleistung von Informationssicherheitszielen, nämlich die Vertraulichkeit, die Integrität sowie die Verfügbarkeit. Das heißt die Informationssicherheitsziele werden nach Kundenanforderungen spezifisch erfüllt (siehe auch Kapitel 2.4.3). Abbildung 4.6 zeigt alle Teilaufgaben von ISG, die die Hauptaufgabe „Schaffen von Wert“ unterstützen und die zu den Teilaufgaben zugeordnete Aktivität des jeweiligen Standards bzw. Best Practices.

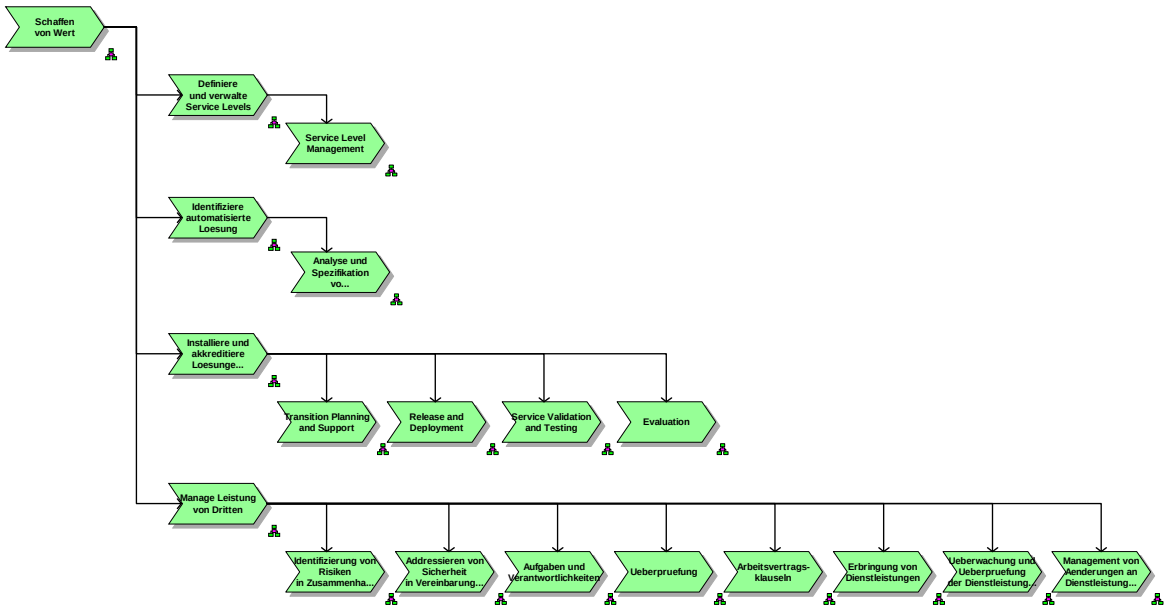

Abbildung 4.6: Prozessmodell Schaffen von Wert

- Risikomanagement

Die Hauptaufgabe Risikomanagement von Information Security Governance leistet einerseits einen guten Schutz für Informationsressourcen, andererseits ermöglicht es auch einen schnellen Wiederanlauf nach Katastrophen oder Krisenfallen (siehe auch Kapitel 2.4.3). Abbildung 4.7 zeigt alle Teilaufgaben von ISG, die die Hauptaufgabe „Risikomanagement“ unterstützen und die zu den Teilaufgaben zugeordnete Aktivität des jeweiligen Standards bzw. Best Practices.

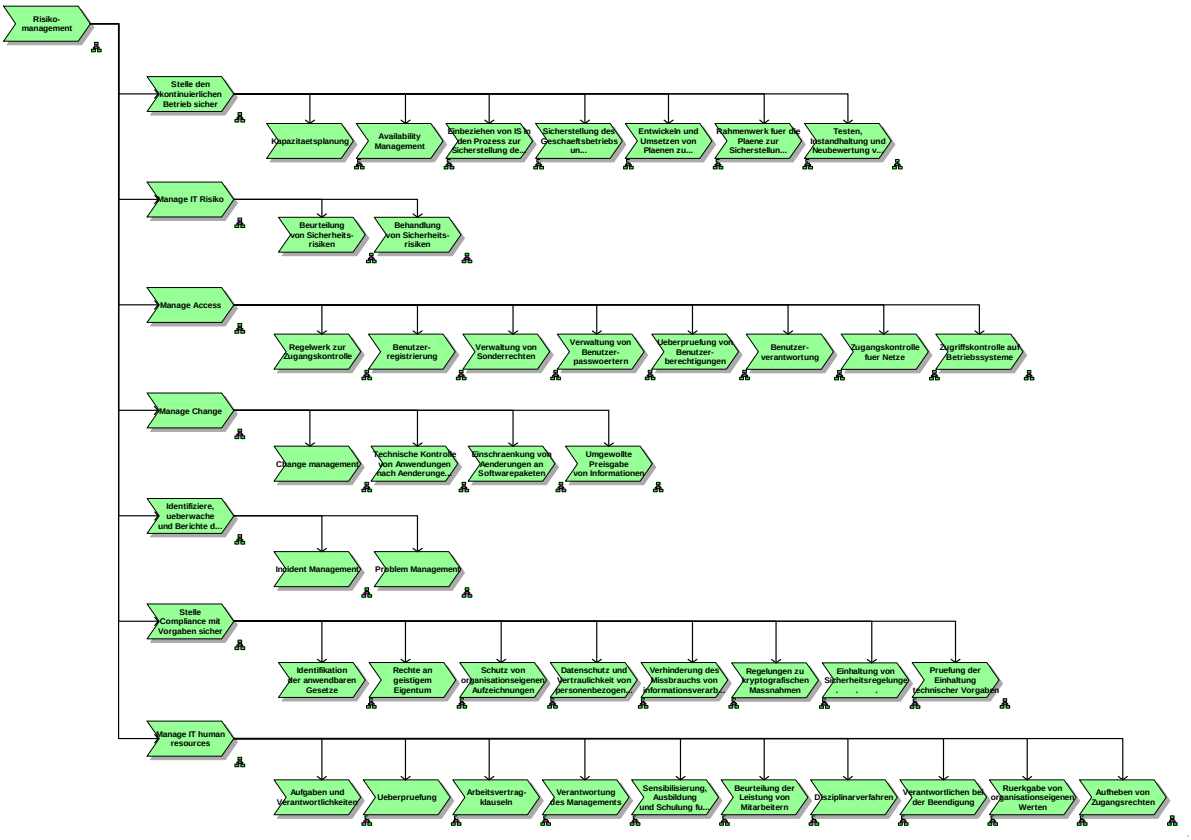

Abbildung 4.7: Prozessmodell Risikomanagement

- Leistungsmessung

Die Hauptaufgabe Leistungsmessung von Information Security Governance stellt durch die regelmäßige Überwachung und Berichterstattung der Informationssicherheitsprozesse bzw. die Messung der Performance sicher, dass die organisatorischen Ziele erreicht werden. Die Überwachung und Berichterstattung soll von den inneren Abteilungen einer Unternehmung sowie auch von unabhängigen Organisationen durchgeführt werden (siehe auch Kapitel 2.4.3). Abbildung 4.8 zeigt alle Teilaufgaben von ISG, die die Hauptaufgabe „Leistungsmessung“ unterstützen und die zu den Teilaufgaben zugeordnete Aktivität des jeweiligen Standards bzw. Best Practices.

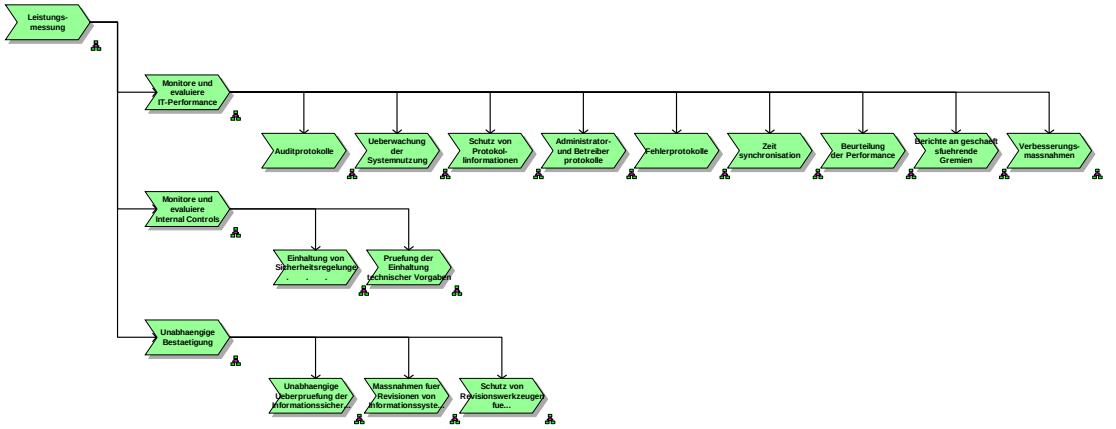

Abbildung 4.8: Prozessmodell Leistungsmessung

Kapitel 5

Zusammenfassung und Ausblick

5.1 Zusammenfassung

In der vorliegenden Arbeit wurde ein Gesamtbild des aktuellen Stands der Entwicklung von Information Security Governance (ISG) wiedergegeben bzw. ein Referenzmodell für Information Security Governance entwickelt, welche auf die in den Unternehmen sehr breit verwendeten Standards und Best Practices, nämlich ITIL, COBIT und ISO 27002 basiert. Als Grundlage wurden in Kapitel 2 alle relevanten Begriffe, Standards und Best Practices sowie das Vorgehen zur Referenzmodellierung näher erklärt. Weiterhin wurde in Kapitel 3 ein auf drei Ebenen strukturiertes Referenzmodell für die Information Security Governance festgelegt, sodass eine Zuordnung zu den drei Referenzmodellen wie ITIL, COBIT und ISO 27002 vorgenommen werden kann und somit Information Security Governance als konzeptioneller Ansatz auch für die Praxis nutzbar gemacht wird. Auf dieser Basis wurde in tabellarischer Form gezeigt, wie ITIL, COBIT und ISO 27002 bezüglich der Informationssicherheit miteinander in Beziehung stehen bzw. wie sie die Information Security Governance redundanzfrei unterstützen. In Kapitel 4 wurde das Referenzmodell für Information Security Governance mit Hilfe von ARIS erstellt.

Der Schwerpunkt dieser Arbeit ist zudem zum einen die Zuordnung von ITIL, COBIT und ISO 27002 zu Information Security Governance bzw. der weitere Vergleich dieser drei Standards bzw. Best Practices, um Überschneidungen unter ihnen herauszufinden und schließlich eine einheitliche Lösung für die Informationssicherheit zu entwickeln. Zum anderen soll die hergeleitete ISG-Konzeption in ein für die Praxis nutzbares Referenzmodell überführt werden.

Diese Arbeit hat des Weiteren ein umfassendes Referenzmodell für Information Security Governance erstellt, damit es nach der erforderlichen Anpassung in allen Unternehmen oder Organisationen, die Anforderungen hinsichtlich der Informationssicherheit besitzen, umsetzbar gemacht wird. Außerdem basiert das Referenzmodell auf ITIL, COBIT bzw. ISO 27002, die als bekannte Lösungen in modernen Unternehmen bereits umgesetzt werden. Daraus wird also ersichtlich, dass bei einer Einführung von Information Security Governance die bereits bestehenden Lösungen berücksichtigt werden.

5.2 Ausblick

In unserer heutigen Gesellschaft ist die Informationstechnik bis fast in jeden Bereich der modernen Unternehmen durchgedrungen. Dadurch wurden die Unternehmen immer mehr von IT und Information abhängig. Dies hat zu einer entscheidenden Entwicklung der Rolle der Informationssicherheit geführt. Auch wegen der großen Auswirkungen der Informationssicherheit auf das gesamte Unternehmen, wird Informationssicherheit immer mehr als eine Untergruppe von Corporate Governance betrachtet. Diese entstandenen Anforderungen bezüglich der Informationssicherheit in modernen Unternehmen, führt zur Entstehung einer neuen Disziplin, nämlich Information Security Governance [vgl. Rastogi/Solms2006, S224].

Information Security soll nicht mehr wie früher lediglich auf der technologischen Seite betrachtet werden, sondern auch die konzeptionelle, organisierende und kontrollierende sowie steuernde Seite. Dabei kann Information Security Governance, welche unter der Verantwortung des Unternehmensvorstands und der Führungskräfte liegen, den Unternehmen dazu verhelfen, ein umfassendes Framework zu bieten, um die Informationssicherheit strukturiert und effizient gewährleisten zu können.

Natürlich ist Information Security Governance, wie sie in dieser Arbeit vorgestellt wurde, keine feste Garantie für die Informationssicherheit in den Unternehmen und nicht unbedingt für jedes Unternehmen sinnvoll. Dennoch ist das hier vorgestellte

Information Security Governance Referenzmodell ein ganzheitlicher Ansatz, welcher der zunehmenden Bedeutung der Informationssicherheit Rechnung trägt.

Information Security Governance wird normalerweise auf einer sehr abstrakten Ebene wissenschaftlich bzw. konzeptionell verstanden und behandelt. Diese Arbeit zeigt, dass es durchaus möglich ist, Information Security Governance auch detaillierter zu betrachten, wie zum Beispiel auf der Ebene Haupt- und Teilaufgaben bzw. Aktivitäten. Es bleibt also zu hoffen, dass, zum Beispiel in Anlehnung an diese Arbeit, die Information Security Governance auch in der Praxis angewendet werden könnte. Allerdings wäre eine Umsetzung mittels Anwendungssoftware nur dann möglich, wenn es hier noch konkrete und detaillierte Informationssicherheitsaktivitäten geben würde.

Die in dieser Arbeit konzipierte Information Security Governance wurde auf Basis der Referenzmodelle COBIT, ITIL und ISO 27002 erstellt. Dies bietet den Unternehmen die Möglichkeit an, die schon in Unternehmen vorhandenen, spezialisierten IT-Lösungen bzw. Referenzmodelle nebeneinander einzusetzen und als eine Einheit zu betrachten und zu behandeln.

Insgesamt stellt das Information Security Governance Referenzmodell, so wie sie in dieser Arbeit konzipiert wurde, eine gute Basis dar, um den vielfältigen Anforderungen der Informationssicherheit in den Unternehmen gerecht zu werden. Für eine konkrete Umsetzung sind aber noch viele weitere konzeptionelle Arbeiten nötig. Notwendige Strukturierungen und Konkretisierungen sind aber bereits teilweise in dieser Arbeit enthalten, sodass also ein erster Schritt getan ist.

Anhang A

PO Plan and Organize	**Planung und Organisation**
PO1 Define a strategic IT plan	Definieren eines strategischen IT-Plan
PO2 Define the information architecture	Definieren der Informationsarchitektur
PO3 Determine technological direction	Festlegen der technischen Ausrichtung
PO4 Define the IT processes, organization and relationships	Definieren der IT- Organisation und ihrer Beziehungen
PO5 Manage the IT investment	IT-Investitionsmanagement
PO6 Communicate management aims and direction	Kommunizieren der Management-Ziele und Strategien
PO7 Manage human resources	Personalführungsmanagement
PO8 Manage quality	Qualitätsmanagement
PO9 Assess and manage IT risks	Risikomanagement
PO10 Manage projects	Projektmanagement
AI Acquire and Implement	**Beschaffung und Einführung**
AI1 Identify automated solutions	Identifizierung automatisierter Lösungen
AI2 Acquire and maintain application software	Erwerb und Pflege von Applikationssoftware
AI3 Acquire and maintain technology infrastructure	Erwerb und Pflege der technischen Infrastruktur
AI4 Enable operation and use	Befähigen des Betriebes
AI5 Procure IT resources	Zur Verfügung stellen von IT-Ressourcen
AI6 Manage changes	Änderung Management
AI7 Install and accredit solutions and changes	Installieren und Abnehmen von Systemen und Änderungen.
DS Delivery and Support	**Auslieferung und Unterstützung**
DS1 Define and manage service levels	Service Level Management
DS2 Manage third-party services	Lieferanten-Management

DS3 Manage performance and capacity	Performance und Kapazitätsmanagement
DS4 Ensure continuous service	Continuity Management
DS5 Ensure systems security	Security Management
DS6 Identify and allocate costs	Kostenmanagement
DS7 Educate and train users	Anwenderschulung und Training
DS8 Manage service desk and incident	Anwenderunterstützung
DS9 Manage the configuration	Konfigurationsmanagement
DS10 Manage problems	Problem Management
DS11 Manage data	Data Management
DS12 Manage the physical environment	Facility Management
DS13 Manage operations	Operationsmanagement
ME Monitor and Evaluate	**Monitoring und Evaluierung**
ME1 Monitor and evaluate IT performance	Überwachen und Evaluieren der IT-Performance
ME2 Monitor and evaluate internal control	Überwachung und Begutachtung der internen Kontrollen
ME3 Ensure compliance with external requirements	Sicherstellung der Einhaltung gesetzlicher Vorschriften
ME4 Provide IT Governance.	Sorgen für IT-Governance

Tabelle A.1: Übersicht über sämtliche COBIT-Prozesse und die dazugehörigen detaillierten Kontrollziele (Goltsche2006; ITGI2008)

Anhang B

Service Strategy (Servicestrategie)	**Service Operation (Servicebetrieb)**
Define the Market	Event Management
Develop the Offerings	Incident Management
Develop Strategic Assets	Problem Management
Prepare for Execution	Request Fulfillment
Financial Management	Access Management
Return on Invest	**Continual Service Improvement (Kontinuierliche Serviceverbesserung)**
Service Portfolio Management	The 7-Step Improvement Process
Demand Management	Service Reporting
Service Design (Serviceentwurf)	Service Measurement
Service Catalogue Management	Return on Invest for CSI
Service Level Management	Business Questions for CSI
Risikomanagement	Service Level Management
Capacity Management	
Availability Management	
IT Service Continuity Management	
Information Security Management	
Supplier Management	
Service Transition (Serviceüberführung)	
Transition Planning and Support	
Change Management	
Service Asset and Configuration Management	
Release and Deployment Management	
Service Validation and Testing	
Evaluation	
Knowledge Management	

Tabelle A.2: Fünf Prozessgebiete in ITIL bzw. ihre Teilprozesse (Olbrich2008)

Anhang C

4.0 Risk assessment and treatment	**4.0 Beurteilung und Behandlung von Risiken**
4.1 Assessing security risks	4.1 Beurteilung von Sicherheitsrisiken
4.2 Treating security risks	4.2 Behandlung von Sicherheitsrisiken
5.0 Security Policy	**5.0 Sicherheitsleitlinie**
5.1 Information security policy	5.1 Informationssicherheitslinie
5.1.1 Information security policy document	5.1.1 Leitlinie zur Informationssicherheit
5.1.2 Review of the information security policy	5.1.2 Überprüfung der Informationssicherheitsleitlinie
6.0 Organization of information policy	**6.0 Organisation der Informationssicherheit**
6.1 Internal organization	6.1 Interne Organisation
6.1.1 Management commitment to information security	6.1.1 Engagement des Managements für Informationssicherheit
6.1.2 Information security coordination	6.1.2 Koordination der Informationssicherheit
6.1.3 Allocation of information security responsibilities	6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit
6.1.4 Authorization process for information processing facilities	6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen
6.1.5 Confidentiality agreements	6.1.5 Vertraulichkeitsvereinbarungen
6.1.6 Contact with authorities	6.1.6 Kontakt zu Behörden
6.1.7 Contact with special interest groups	6.1.7 Kontakt zu speziellen Interessengruppen
6.1.8 Independent review of information security	6.1.8 Unabhängige Überprüfung der Informationssicherheit
6.2 External parties	6.2 Externe Parteien
6.2.1 Identification of risks related to external parties	6.2.1 Identifizierung von Risiken in Zusammenhang mit Externen
6.2.2 Addressing security when dealing with customers	6.2.2 Adressieren von Sicherheit im Umgang mit Kunden
6.2.3 Addressing security in third party agreements	6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten
7.0 Asset management	**7.0 Management von organisationseigenen Werten**
7.1 Responsibility for assets	7.1 Verantwortung für organisationseigene Werte
7.1.1 Inventory of assets	7.1.1 Inventar der organisationseigenen Werte
7.1.2 Ownership of assets	7.1.2 Eigentum von organisationseigenen Werten
7.1.3 Acceptable use of assets	7.1.3 Zulässiger Gebrauch von organisationseigenen Werten
7.2 Information classification	7.2 Klassifizierung von Informationen

7.2.1 Classification guidelines	7.2.1 Regelungen für die Klassifizierung
7.2.2 Information labeling and handling	7.2.2 Kennzeichnung von und Umgang mit Informationen
8.0 Human resource security	**8.0 Personalsicherheit**
8.1 Prior to employment	8.1 Vor der Anstellung
8.1.1 Roles and responsibilities	8.1.1 Aufgaben und Verantwortlichkeiten
8.1.2 Screening	8.1.2 Überprüfung
8.1.3 Terms and conditions of employment	8.1.3 Arbeitsvertragsklauseln
8.2 During employment	8.2 Während der Anstellung
8.2.1 Management responsibilities	8.2.1 Verantwortung des Managements
8.2.2 Information security awareness, education and training	8.2.2 Sensibilisierung, Ausbildung und Schulung für Informationssicherheit
8.2.3 Disciplinary process	8.2.3 Disziplinarverfahren
8.3 Termination or change of employment	8.3 Beendigung oder Änderung der Anstellung
8.3.1 Termination responsibilities	8.3.1 Verantwortlichkeiten bei der Beendigung
8.3.2 Return of assets	8.3.2 Rückgabe von organisationseigenen Werten
8.3.3 Removal of access rights	8.3.3 Aufheben von Zugangsrechten
9.0 Physical and environmental security	**9.0 Physische und umgebungsbezogene Sicherheit**
9.1 Secure areas	9.1 Sicherheitsbereiche
9.1.1 Physical security perimeter	9.1.1 Sicherheitszonen
9.1.2 Physical entry controls	9.1.2 Zutrittskontrolle
9.1.3 Securing offices, rooms and facilities	9.1.3 Sicherung von Büros, Räumen und Einrichtungen
9.1.4 Protecting against external and environmental threats	9.1.4 Schutz vor Bedrohungen von Außen und aus der Umgebung
9.1.5 Working in secure areas	9.1.5 Arbeit in Sicherheitszonen
9.1.6 Public access, delivery and loading areas	9.1.6 Öffentlicher Zugang, Anlieferungs- und Ladezonen
9.2 Equipment security	9.2 Sicherheit von Betriebsmitteln
9.2.1 Equipment sitting and protection	9.2.1 Platzierung und Schutz von Betriebsmitteln
9.2.2 Supporting utilities	9.2.2 Unterstützende Versorgungseinrichtungen
9.2.3 Cabling security	9.2.3 Sicherheit der Verkabelung
9.2.4 Equipment maintenance	9.2.4 Instandhaltung von Gerätschaften
9.2.5 Security of equipment off premises	9.2.5 Sicherheit von Außerhalb des Standorts befindlicher Ausrüstung
9.2.6 Secure disposal or re-use of equipment	9.2.6 Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln
9.2.7 Removal of property	9.2.7 Entfernung von Eigentum
10.0 Communications and operations management	**10.0 Betriebs- und Kommunikationsmanagement**

10.1 Operational procedures and responsibilities	10.1 Verfahren und Verantwortlichkeiten
10.1.1 Documented operating procedures	10.1.1 Dokumentierte Betriebsprozesse
10.1.2 Change management	10.1.2 Änderungsverwaltung
10.1.3 Segregation of duties	10.1.3 Aufteilung von Verantwortlichkeiten
10.1.4 Separation of development, test and operational facilities	10.1.4 Aufteilung von Entwicklungs-, Test- und Produktiveinrichtungen
10.2 Third-party service delivery management	10.2 Management der Dienstleistungs-Erbringung von Dritten
10.2.1 Service delivery	10.2.1 Erbringung von Dienstleistungen
10.2.2 Monitoring and review of third party services	10.2.2 Überwachung und Überprüfung der Dienstleistungen von Dritten
10.2.3 Managing changes to third party services	10.2.3 Management von Änderungen an Dienstleistungen von Dritten
10.3 Systems planning and acceptance	10.3 Systemplanung und Abnahme
10.3.1 Capacity management	10.3.1 Kapazitätsplanung
10.3.2 System acceptance	10.3.2 System-Abnahme
10.4 Protection against malicious and mobile code	10.4 Schutz vor Schadsoftware und mobilem Programmcode
10.4.1 Controls against malicious code	10.4.1 Maßnahmen gegen Schadsoftware
10.4.2 Controls against mobile code	10.4.2 Schutz vor mobiler Software
10.5 Backup	10.5 Backup
10.5.1 Information back-up	10.5.1 Backup von Informationen
10.6 Network security management	10.6 Management der Netzsicherheit
10.6.1 Network controls	10.6.1 Maßnahmen für Netze
10.6.2 Security of network services	10.6.2 Sicherheit von Netzdiensten
10.7 media handling	10.7 Handhabung von Speicher- und Aufzeichnungsmedien
10.7.1 Management of removable media	10.7.1 Verwaltung von Wechselmedien
10.7.2 Disposal of media	10.7.2 Entsorgung von Medien
10.7.3 Information handling procedures	10.7.3 Umgang mit Informationen
10.7.4 Security of system documentation	10.7.4 Sicherheit der Systemdokumentation
10.8 Exchange of information	10.8 Austausch von Informationen
10.8.1 Information exchange policies and procedures	10.8.1 Regelwerke und Verfahren zum Austausch von Informationen
10.8.2 Exchange agreements	10.8.2 Vereinbarungen zum Austausch von Informationen
10.8.3 Physical media in transit	10.8.3 Transport physischer Medien
10.8.4 Electronic messaging	10.8.4 Elektronische Mitteilungen/ Nachrichten (Messaging)
10.8.5 Business information systems	10.8.5 Geschäftsinformationssysteme
10.9 Electronic commerce service	10.9 E-Commerce-Anwendungen
10.9.1 Electronic commerce	10.9.1 E-Commerce
10.9.2 On-line transactions	10.9.2 Online-Transaktionen
10.9.3 Publicly available information	10.9.3 Öffentlich verfügbare Informationen
10.10 Monitoring	10.10 Überwachung
10.10.1 Audit logging	10.10.1 Auditprotokolle

10.10.2 Monitoring system use	10.10.2 Überwachung der Systemnutzung
10.10.3 Protection of log information	10.10.3 Schutz von Protokollinformationen
10.10.4 Administrator and operator logs	10.10.4 Administrator- und Betreiberprotokolle
10.10.5 Fault logging	10.10.5 Fehlerprotokolle
10.10.6 Clock synchronization	10.10.6 Zeitsynchronisation
11.0 Access control	**11.0 Zugangskontrolle**
11.1 Business requirements for access control	11.1 Geschäftanforderungen für Zugangskontrolle
11.1.1 Access control policy	11.1.1 Regelwerk zur Zugangskontrolle
11.2 User access management	11.2 Management des Benutzerzugriffs
11.2.1 User registration	11.2.1 Benutzerregistrierung
11.2.2 Privilege management	11.2.2 Verwaltung von Sonderrechten
11.2.3 User password management	11.2.3 Verwaltung von Benutzerpasswörtern
11.2.4 Review of user access rights	11.2.4 Überprüfung von Benutzerberechtigungen
11.3 User responsibilities	11.3 Benutzerverantwortung
11.3.1 Password use	11.3.1 Passwortverwendung
11.3.2 Unattended user equipment	11.3.2 Unbeaufsichtigte Benutzerausstattung
11.3.3 Clear desk and clear screen policy	11.3.3 Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms
11.4 Network access control	11.4 Zugangskontrolle für Netze
11.4.1 Policy on use of network services	11.4.1 Regelwerk zur Nutzung von Netzen
11.4.2 User authentication for external connections	11.4.2 Benutzerauthentisierung für externe Verbindungen
11.4.3 Equipment identification in networks	11.4.3 Geräteidentifikation in Netzen
11.4.4 Remote diagnostic and configuration port protection	11.4.4 Schutz der Diagnose- und Konfigurationsports
11.4.5 Segregation in networks	11.4.5 Trennung in Netzwerken
11.4.6 Network connection control	11.4.6 Kontrolle von Netzverbindungen
11.4.7 Network routing control	11.4.7 Routingkontrolle für Netze
11.5 Operating system access control	11.5 Zugriffskontrolle auf Betriebssysteme
11.5.1 Secure log-on procedures	11.5.1 Verfahren für sichere Anmeldung
11.5.2 User identification and authentication	11.5.2 Benutzeridentifikation und Authentisierung
11.5.3 Password management system	11.5.3 Systeme zur Verwaltung von Passwörtern
11.5.4 Use of system utilities	11.5.4 Verwendung von Systemwerkzeugen
11.5.5 Session time-out	11.5.5 Session Time-out
11.5.6 Limitation of connection time	11.5.6 Begrenzung der Verbindungszeit
11.6 Application and information access control	11.6 Zugangskontrolle zu Anwendungen und Informationen
11.6.1 Information access restriction	11.6.1 Einschränkung von Informationszugriff
11.6.2 Sensitive system isolation	11.6.2 Isolation sensibler Systeme

11.7 Mobile computing and teleworking	11.7 Mobile Computing und Telearbeit
11.7.1 Mobile computing and communications	11.7.1 Mobile Computing und Kommunikation
11.7.2 Teleworking	11.7.2 Telearbeit
12.0 Information systems acquisition, development and maintenance	**12.0 Beschaffung, Entwicklung und Wartung von Informationssystemen**
12.1 Security requirements of information systems	12.1 Sicherheitsanforderungen von Informationssystemen
12.1.1 Security requirements analysis and specification	12.1.1 Analyse und Spezifikation von Sicherheitsanforderungen
12.2 Correct processing in applications	12.2 Korrekte Verarbeitung in Anwendungen
12.2.1 Input data validation	12.2.1 Überprüfung von Eingabedaten
12.2.2 Control of internal processing	12.2.2 Kontrolle der internen Verarbeitung
12.2.3 Message integrity	12.2.3 Integrität von Nachrichten
12.2.4 Output data validation	12.2.4 Überprüfung von Ausgabedaten
12.3 Cryptographic controls	12.3 Kryptografische Maßnahmen
12.3.1 Policy on the use of cryptographic controls	12.3.1 Leitlinie zur Anwendung von Kryptografie
12.3.2 Key management	12.3.2 Verwaltung kryptografischer Schlüssel
12.4 Security of system files	12.4 Sicherheit von Systemdateien
12.4.1 Control of operational software	12.4.1 Kontrolle von Software im Betrieb
12.4.2 Protection of system test data	12.4.2 Schutz von Test-Daten
12.4.3 Access control to program source code	12.4.3 Zugangskontrolle zu Quellcode
12.5 Security development and support processes	12.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen
12.5.1 Change control procedures	12.5.1 Änderungskontrollverfahren
12.5.2 Technical review of applications after operating system changes	12.5.2 Technische Kontrolle von Anwendungen nach Änderungen am Betriebssystem
12.5.3 Restrictions on changes to software packages	12.5.3 Einschränkung von Änderungen an Softwarepaketen
12.5.4 Information leakage	12.5.4 Ungewollte Preisgabe von Informationen
12.5.5 Outsourced software development	12.5.5 Ausgelagerte Softwareentwicklung
12.6 Technical vulnerability management	12.6 Schwachstellenmanagement
12.6.1 Control of technical vulnerabilities	12.6.1 Kontrolle technischer Schwachstellen
13.0 Information security incident management	**13.0 Umgang mit Informationssicherheitsvorfällen**
13.1 Reporting IS events and weakness	13.1 Melden von Informationssicherheitsereignissen und Schwachstellen
13.1.1 Reporting information security events	13.1.1 Melden von Informationssicherheitsereignissen
13.1.2 Reporting security weaknesses	13.1.2 Melden von Sicherheitsschwachstellen

13.2 Management of IS incidents and improvements	13.2 Umgang mit Informationssicherheitsvorfällen und Verbesserungen
13.2.1Responsibilities and procedures	13.2.1 Verantwortlichkeiten und Verfahren
13.2.2 Learning from information security incidents	13.2.2 Lernen von Informationssicherheitsvorfällen
13.2.3 Collection of evidence	13.2.3 Sammeln von Beweisen
14.0 Business continuity management	**14.0 Sicherstellung des Geschäftsbetriebs**
14.1 Including IS in the BCP process	14.1 Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs
14.1.1 Including information security in the business continuity management process	14.1.1 Einbeziehen von Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs
14.1.2 Business continuity and risk assessment	14.1.2 Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung
14.1.3 Developing and implementing continuity plans including information security	14.1.3 Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten
14.1.4 Business continuity planning framework	14.1.4 Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs
14.1.5 Testing, maintaining and reassessing business continuity plans	14.1.5 Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung des Geschäftsbetriebs
15.0 Compliance	**15.0 Einhaltung von Vorgaben**
15.1 Compliance with legal requirements	15.1 Einhaltung gesetzlicher Vorgaben
15.1.1 Identification of applicable legislation	15.1.1 Identifikation der anwendbaren Gesetze
15.1.2 Intellectual property rights (IPR)	15.1.2 Rechte an geistigem Eigentum
15.1.3 Protection of organizational records	15.1.3 Schutz von organisationseigenen Aufzeichnungen
15.1.4 Data protection and privacy of personal information	15.1.4 Datenschutz und Vertraulichkeit von personenbezogenen Informationen
15.1.5 Prevention of misuse of information processing facilities	15.1.5 Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen
15.1.6 Regulation of cryptographic controls	15.1.6 Regelungen zu kryptografischen Maßnahmen
15.2 Compliance with security policies and standards and technical compliance	15.2 Übereinstimmung mit Sicherheitspolitiken und Standards und technische Übereinstimmung
15.2.1 Compliance with security policies and standards	15.2.1 Einhaltung von Sicherheitsregelungen und –standards
15.2.2 Technical compliance checking	15.2.2 Prüfung der Einhaltung technischer Vorgaben
15.3 Information systems audit considerations	15.3 Überlegungen zu Revisionsprüfungen von Informationssystemen

15.3.1 Information systems audit controls	15.3.1 Maßnahmen für Revisionen von Informationssystemen
15.3.2 Protection of information systems audit tools	15.3.2 Schutz von Revisionswerkzeugen für Informationssysteme

Tabelle A.3: Überwachungsbereiche, Sicherheitskategorien bzw. Sicherheitsmaßnahmen von ISO 27002 (ITSM2008; ISO27001)

Anhang D

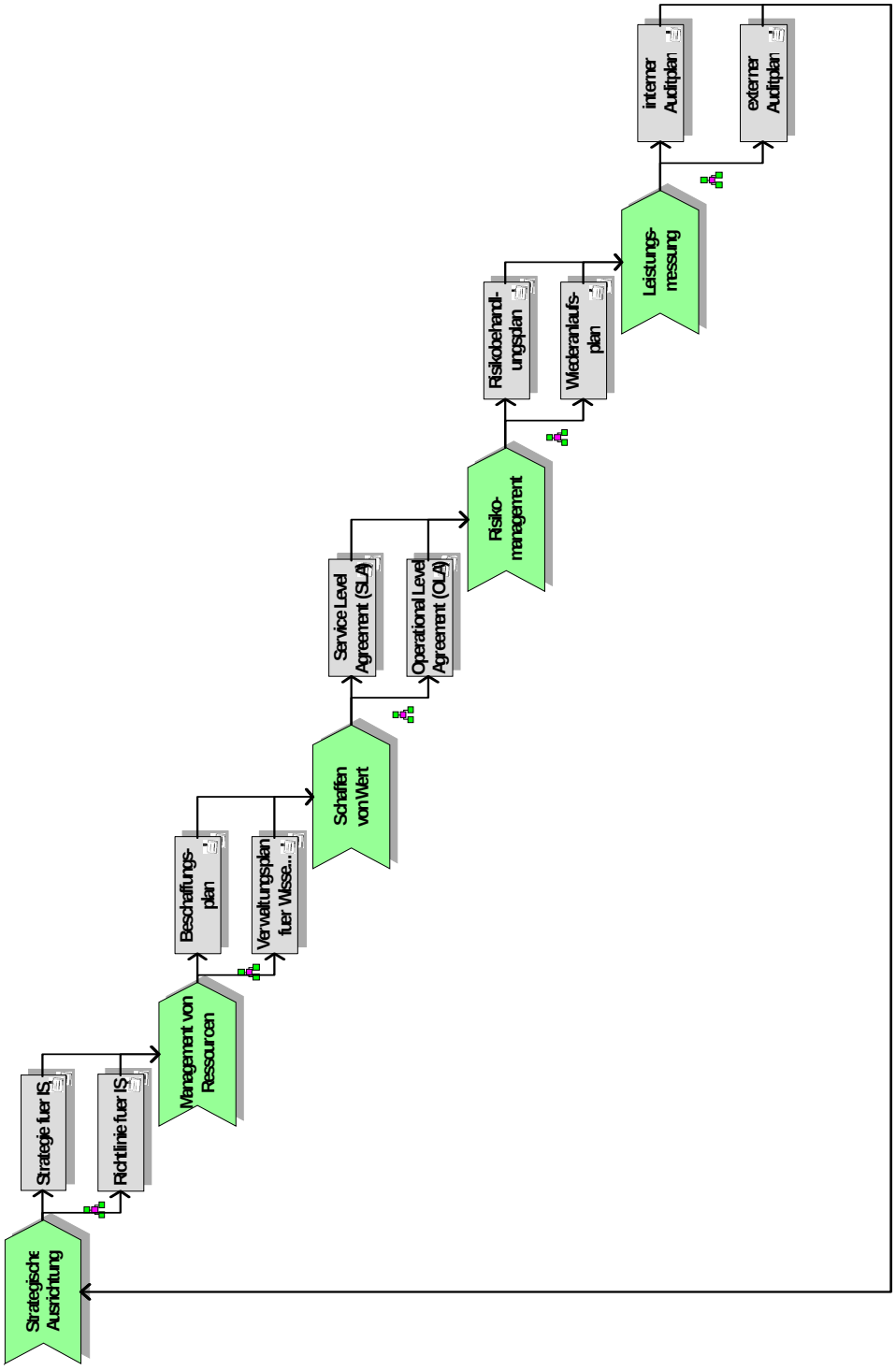

Abbildung A.1: Die Gesamtübersicht zum ISG

Anhang E

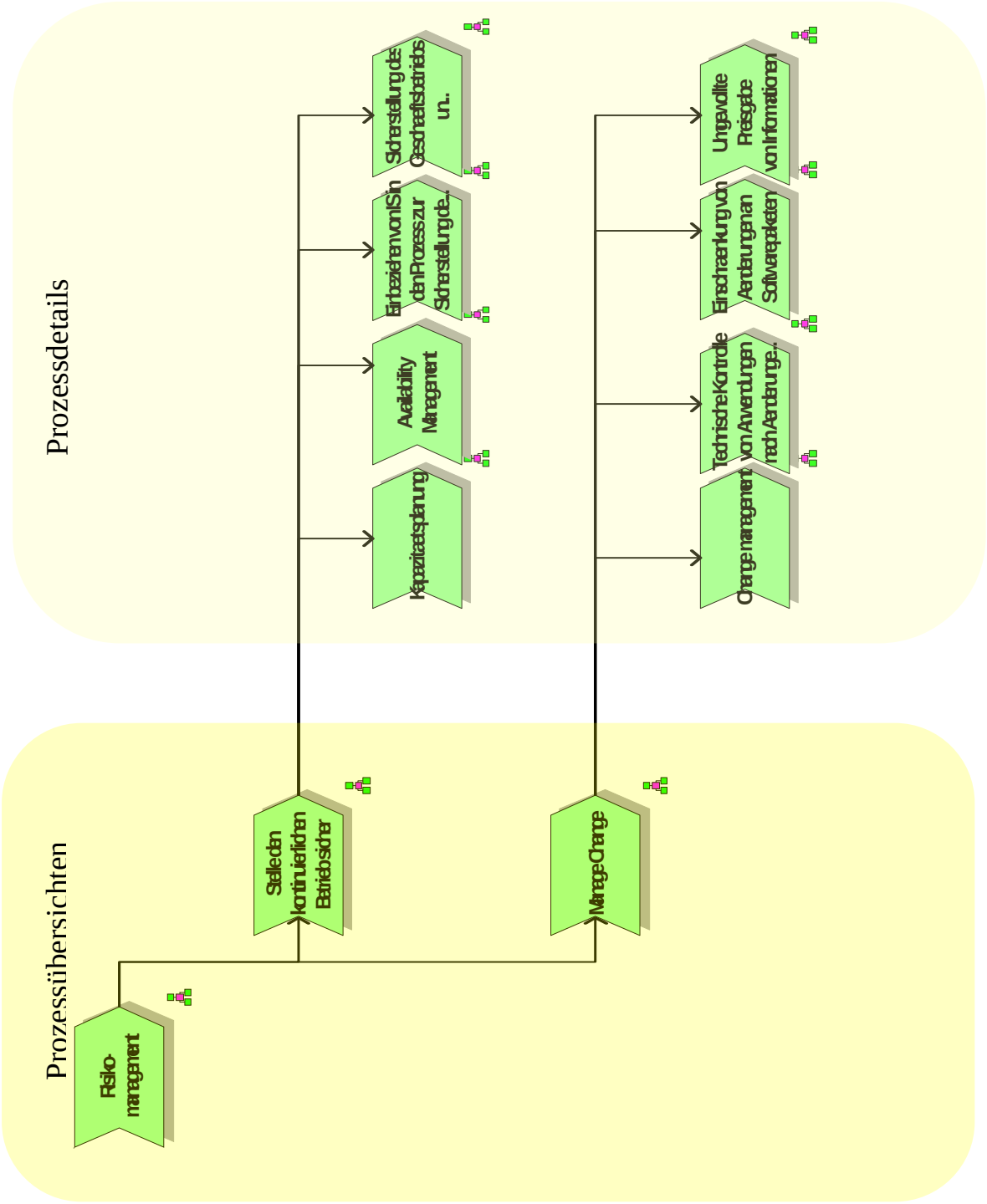

Abbildung A.2: Prozess-Übersicht bzw. -Detailmodell

Anhang F

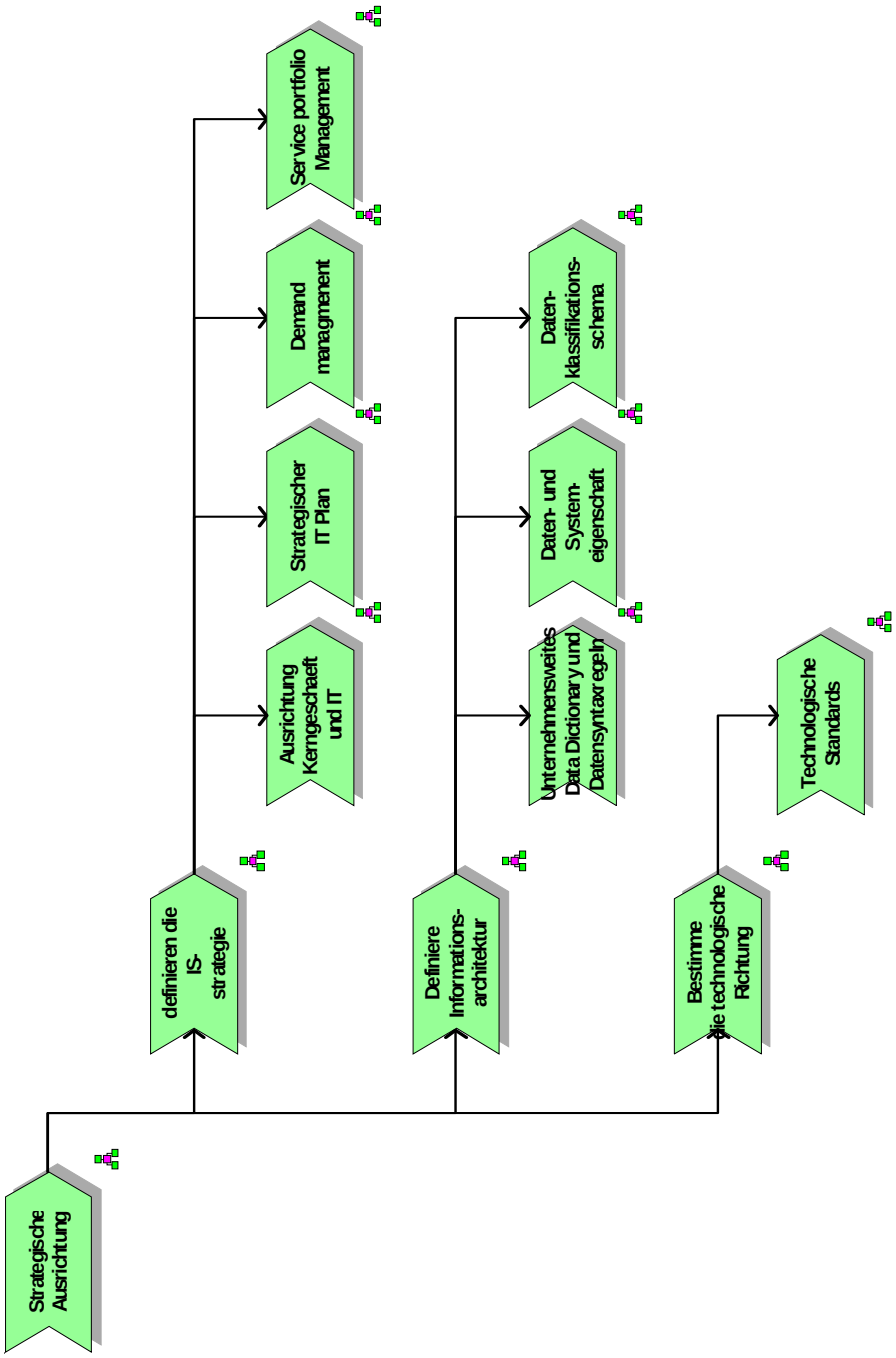

Abbildung A.3: Prozessindex Strategische Ausrichtung (1)

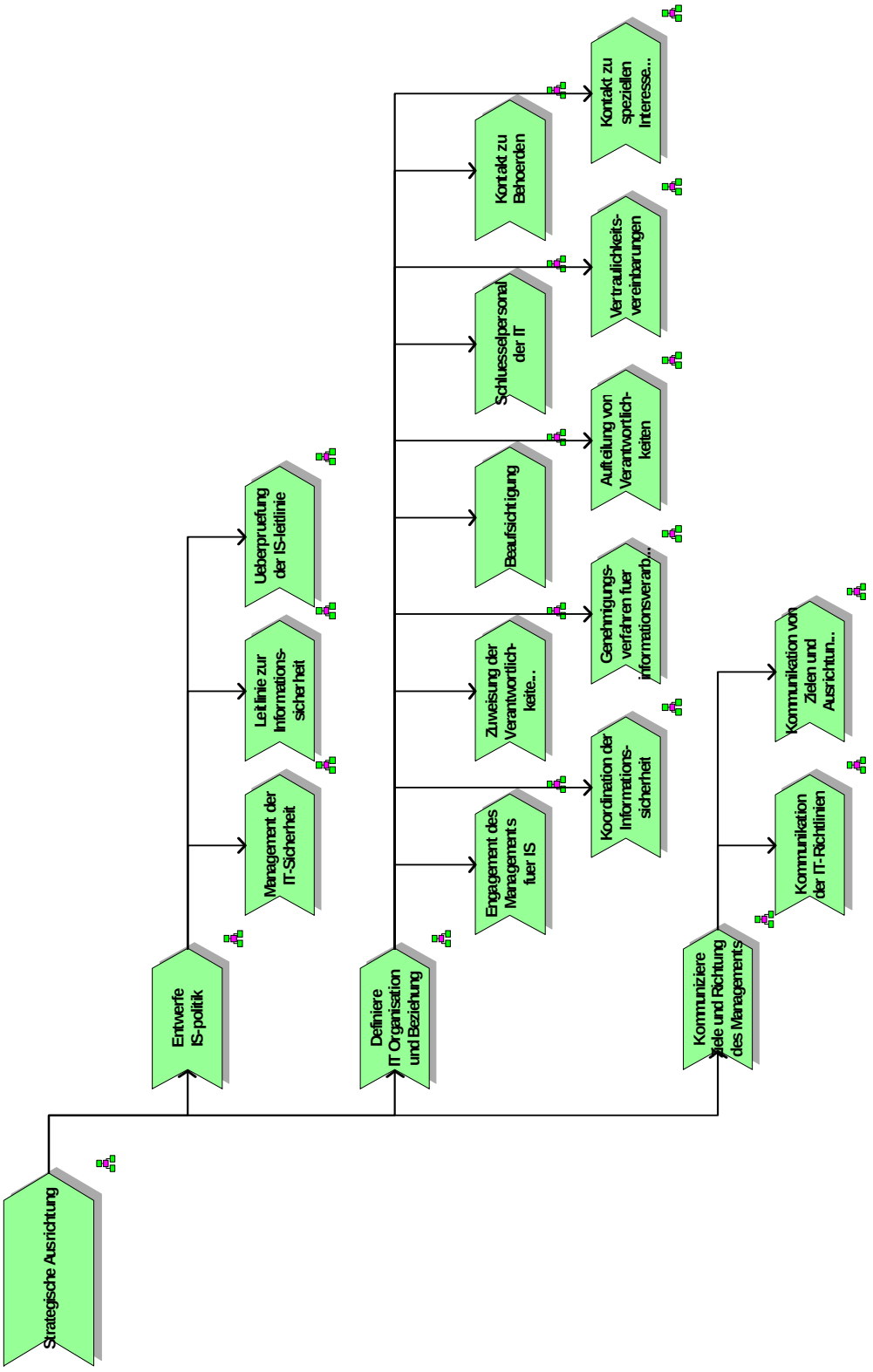

Abbildung A.4: Prozessindex Strategische Ausrichtung (2)

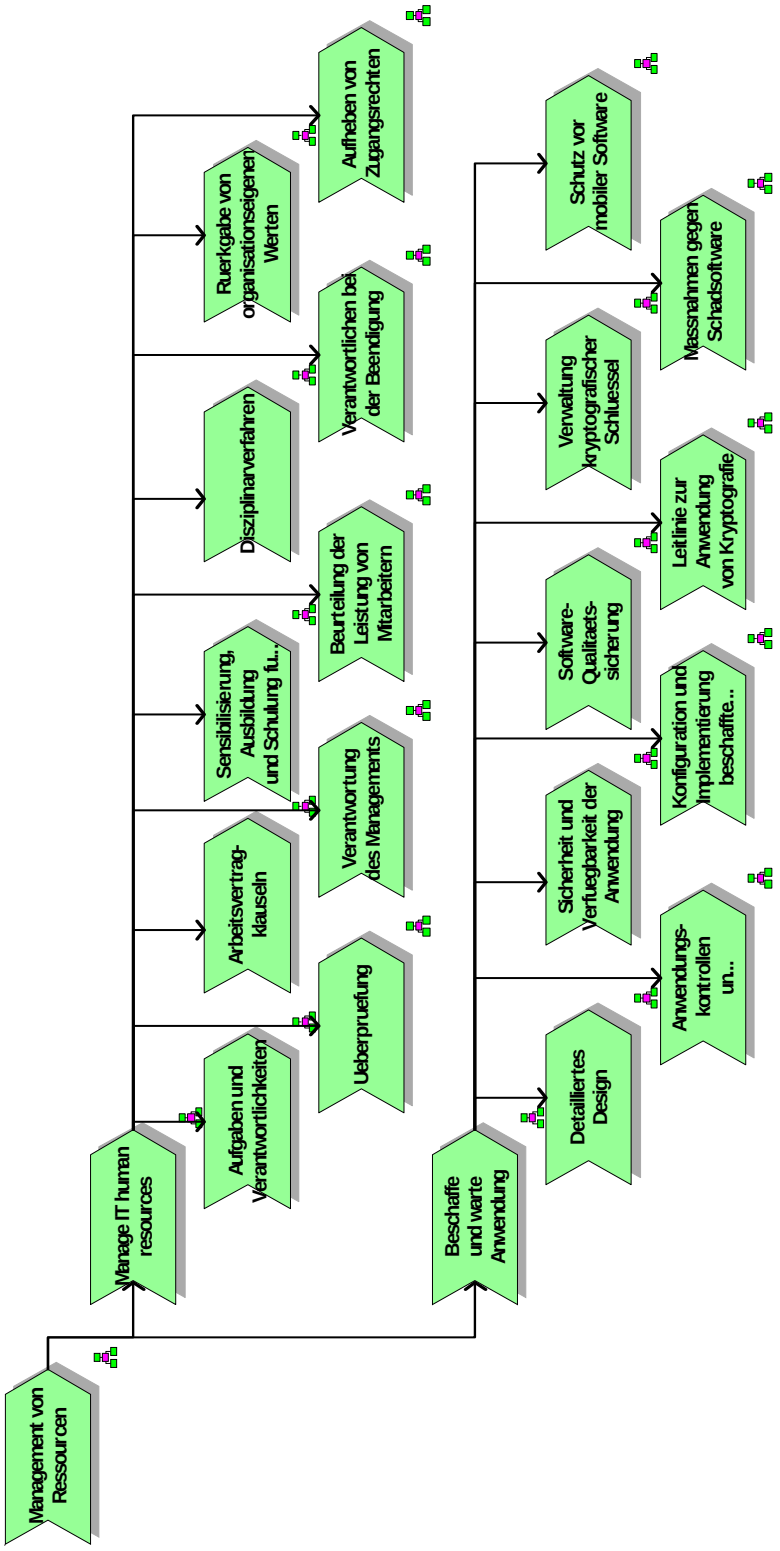

Abbildung A.5: Prozessindex Management von Ressourcen (1)

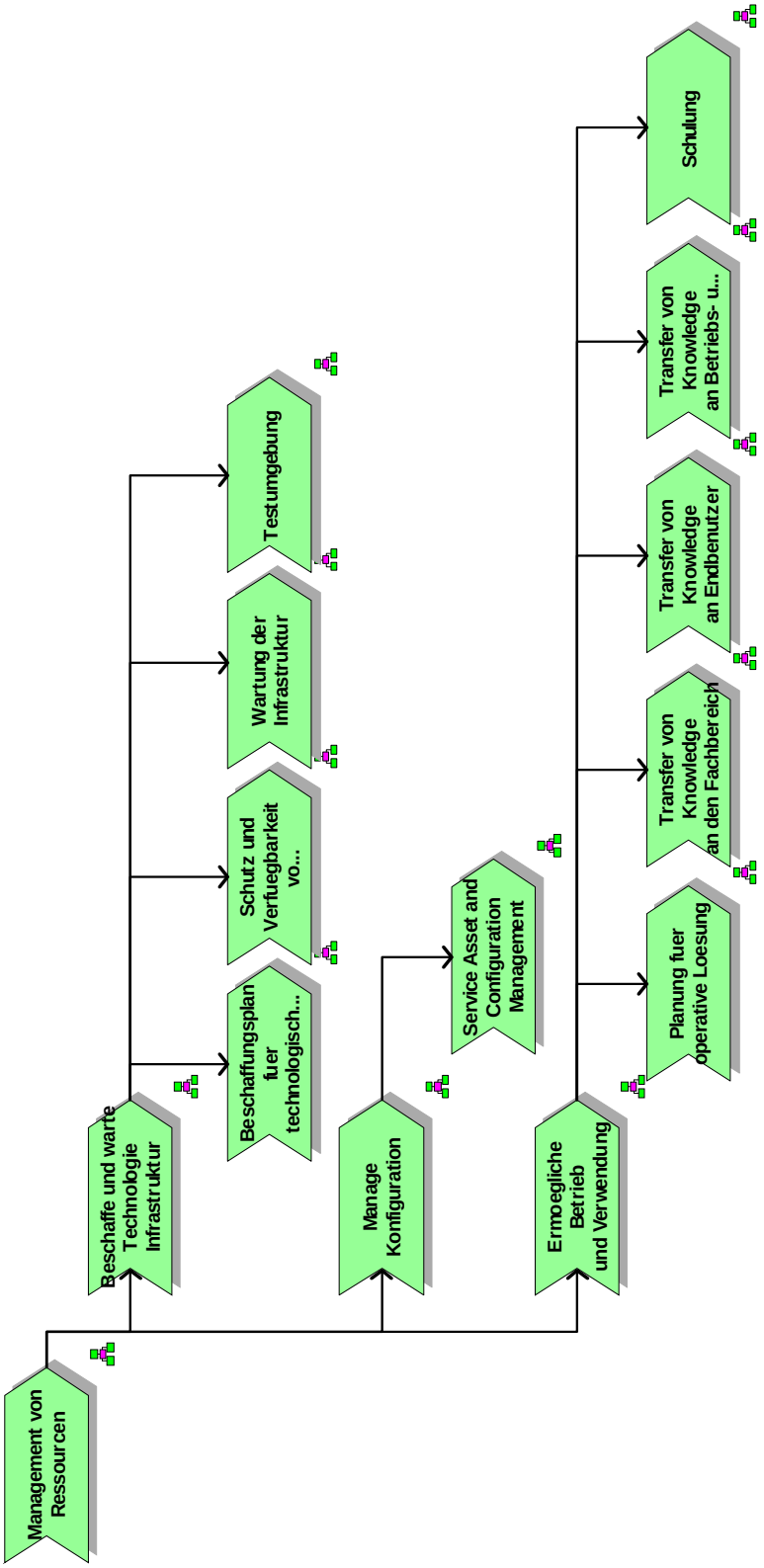

Abbildung A.6: Prozessindex Management von Ressourcen (2)

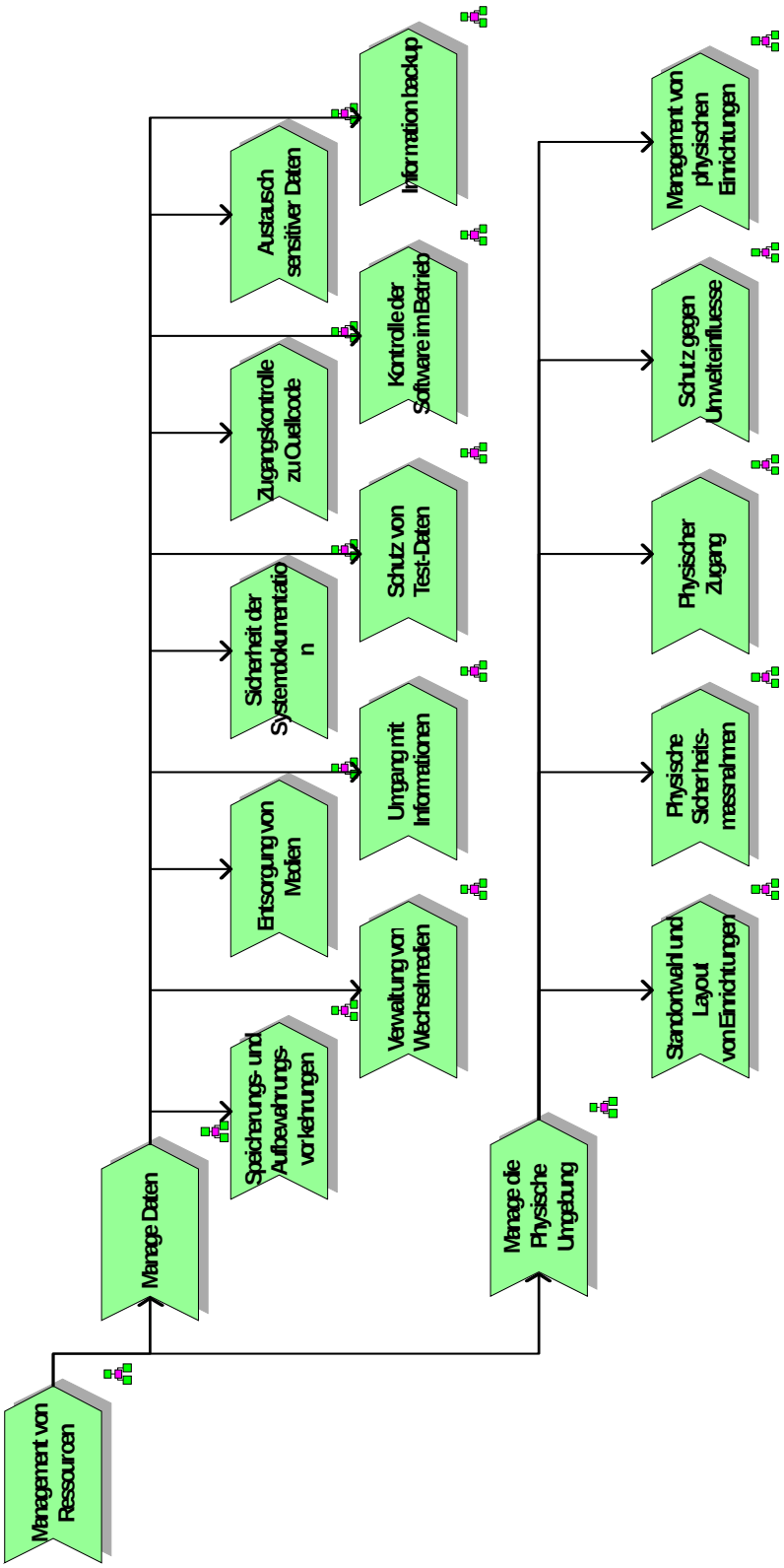

Abbildung A.7: Prozessindex Management von Ressourcen (3)

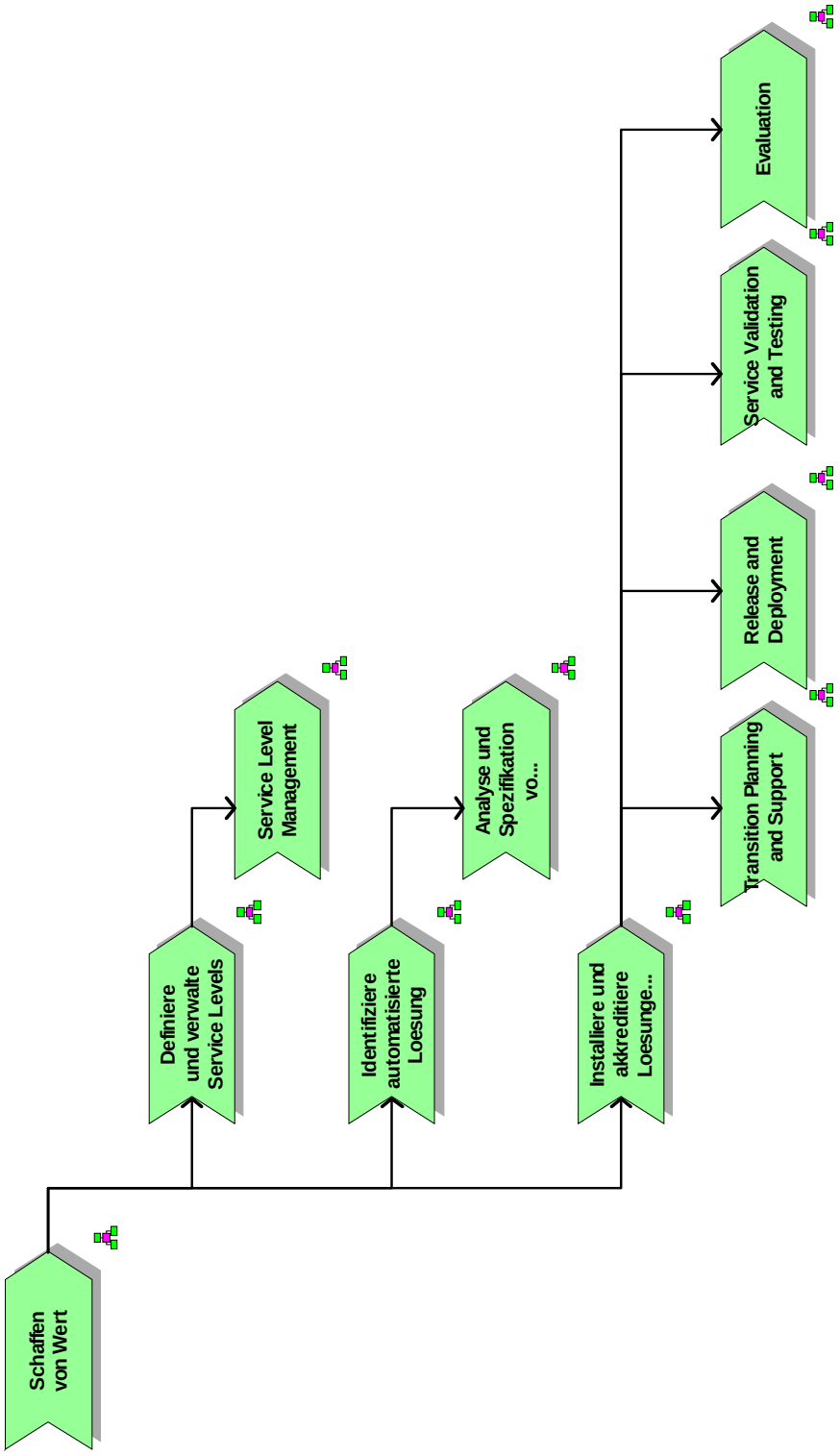

Abbildung A.8: Prozessindex Schaffen von Wert (1)

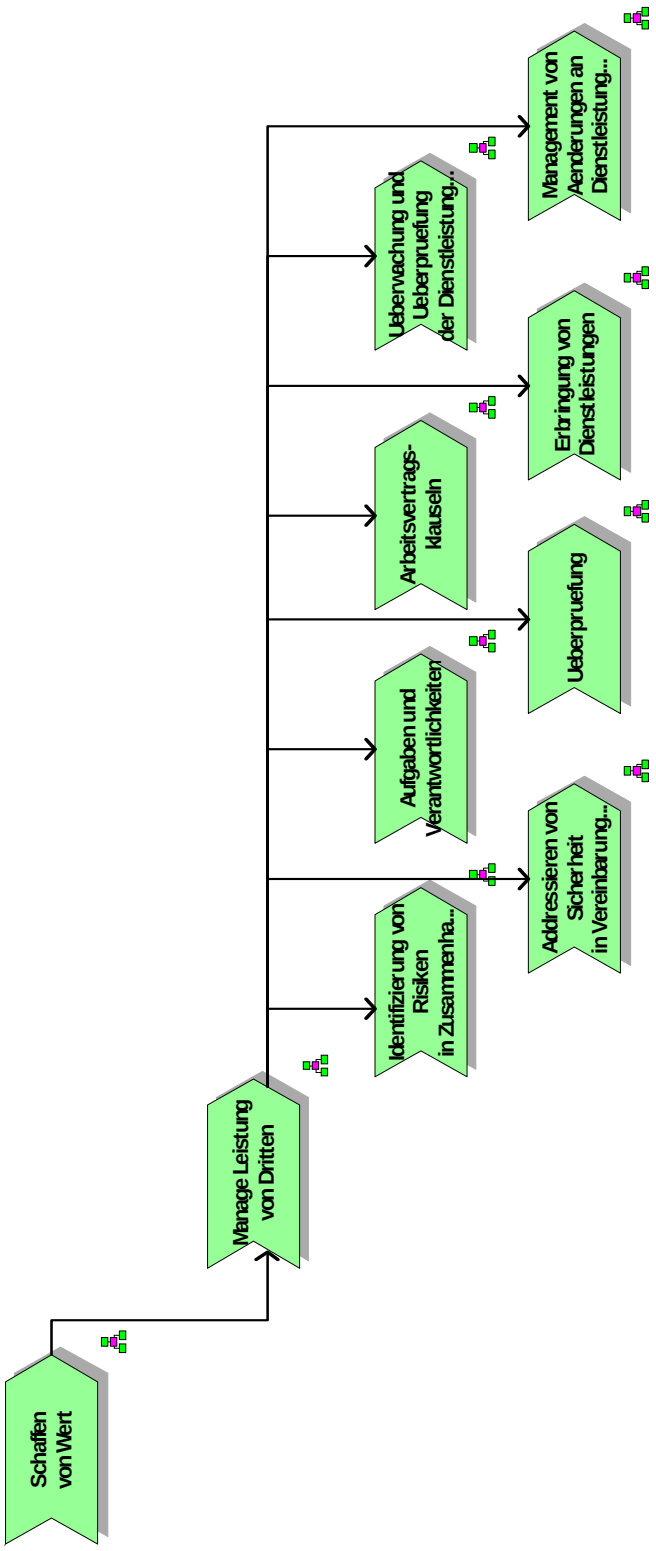

Abbildung A.9: Prozessindex Schaffen von Wert (2)

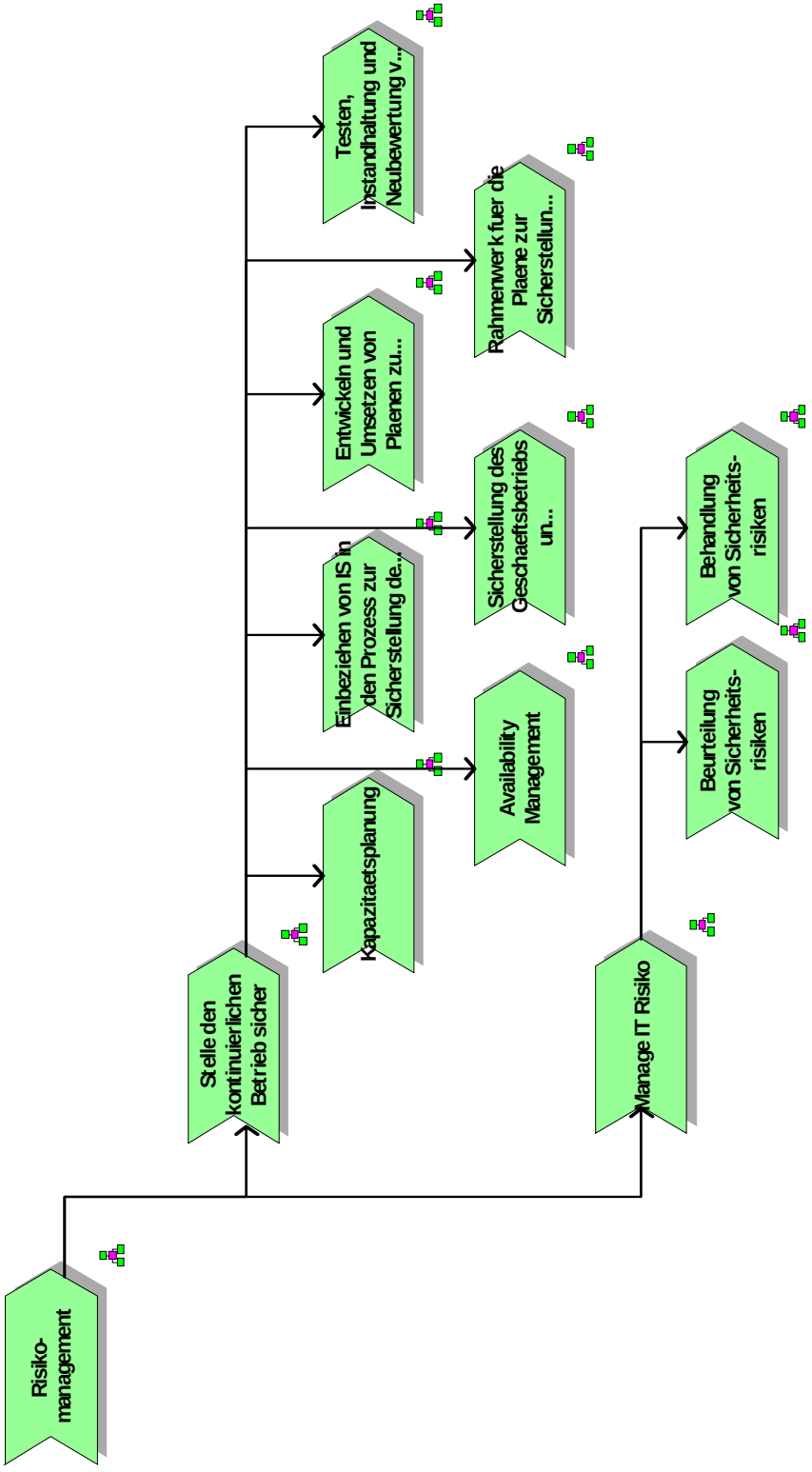

Abbildung A.10: Prozessindex Risikomanagement (1)

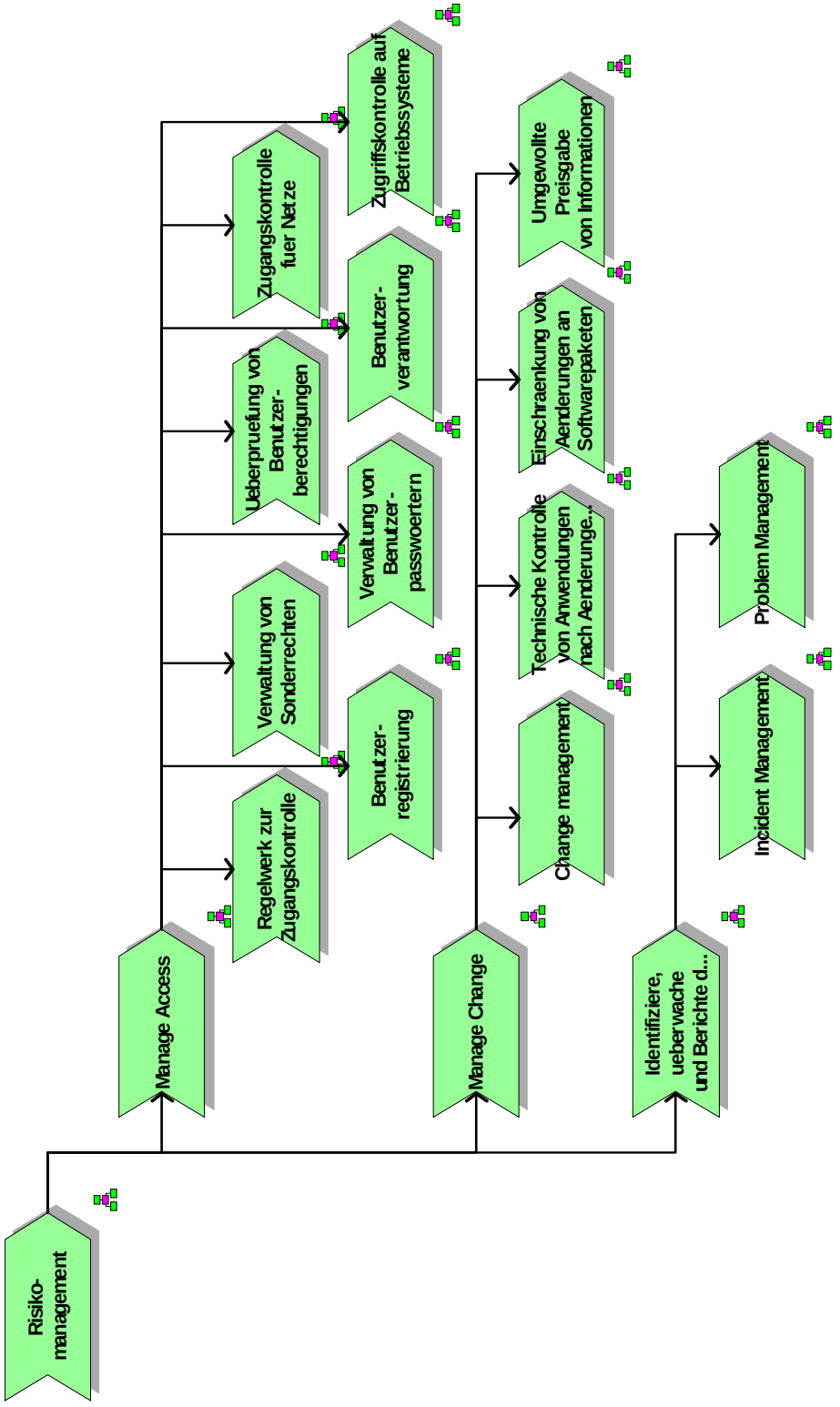

Abbildung A.11: Prozessindex Risikomanagement (2)

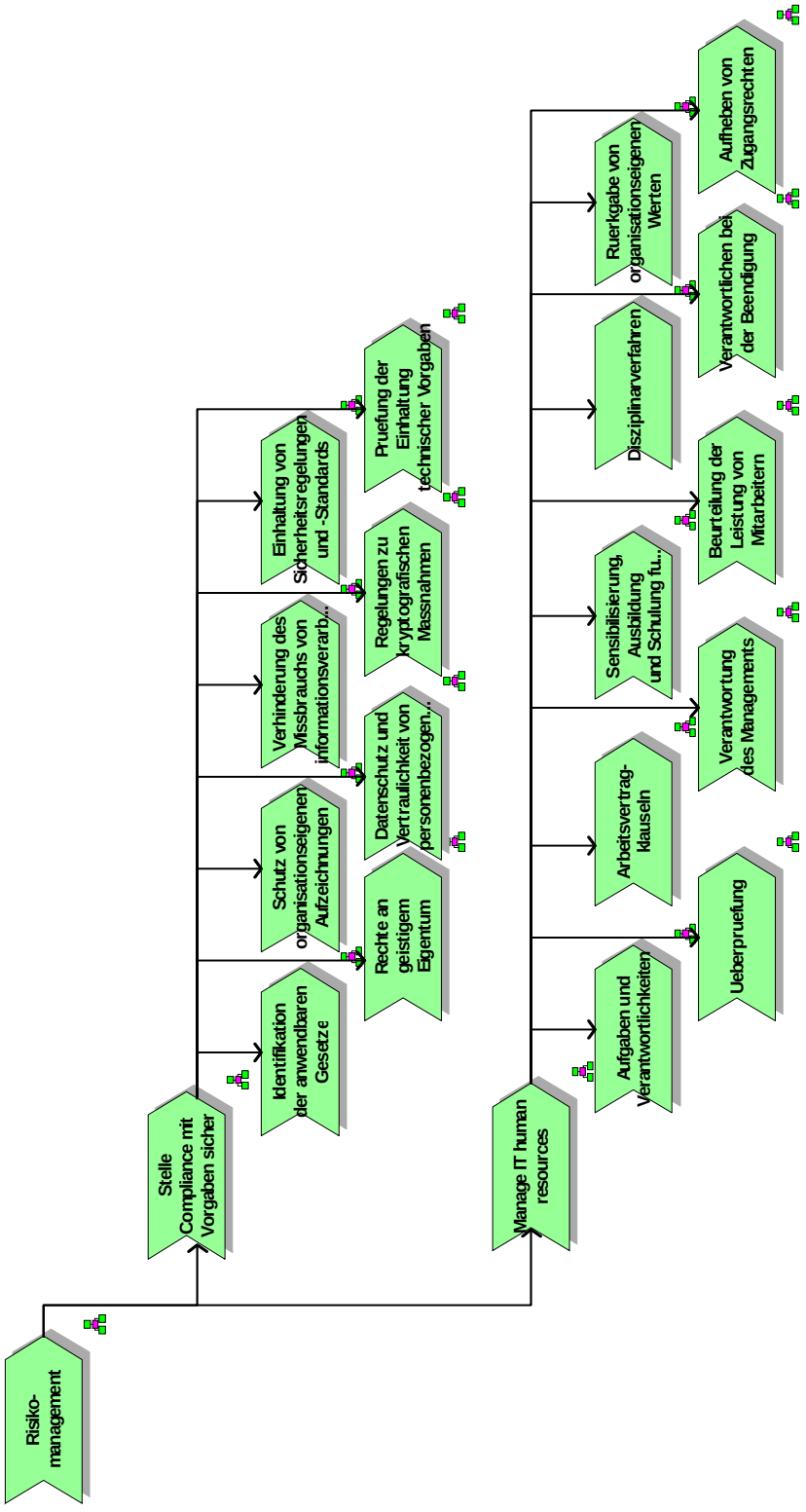

Abbildung A.12: Prozessindex Risikomanagement (3)

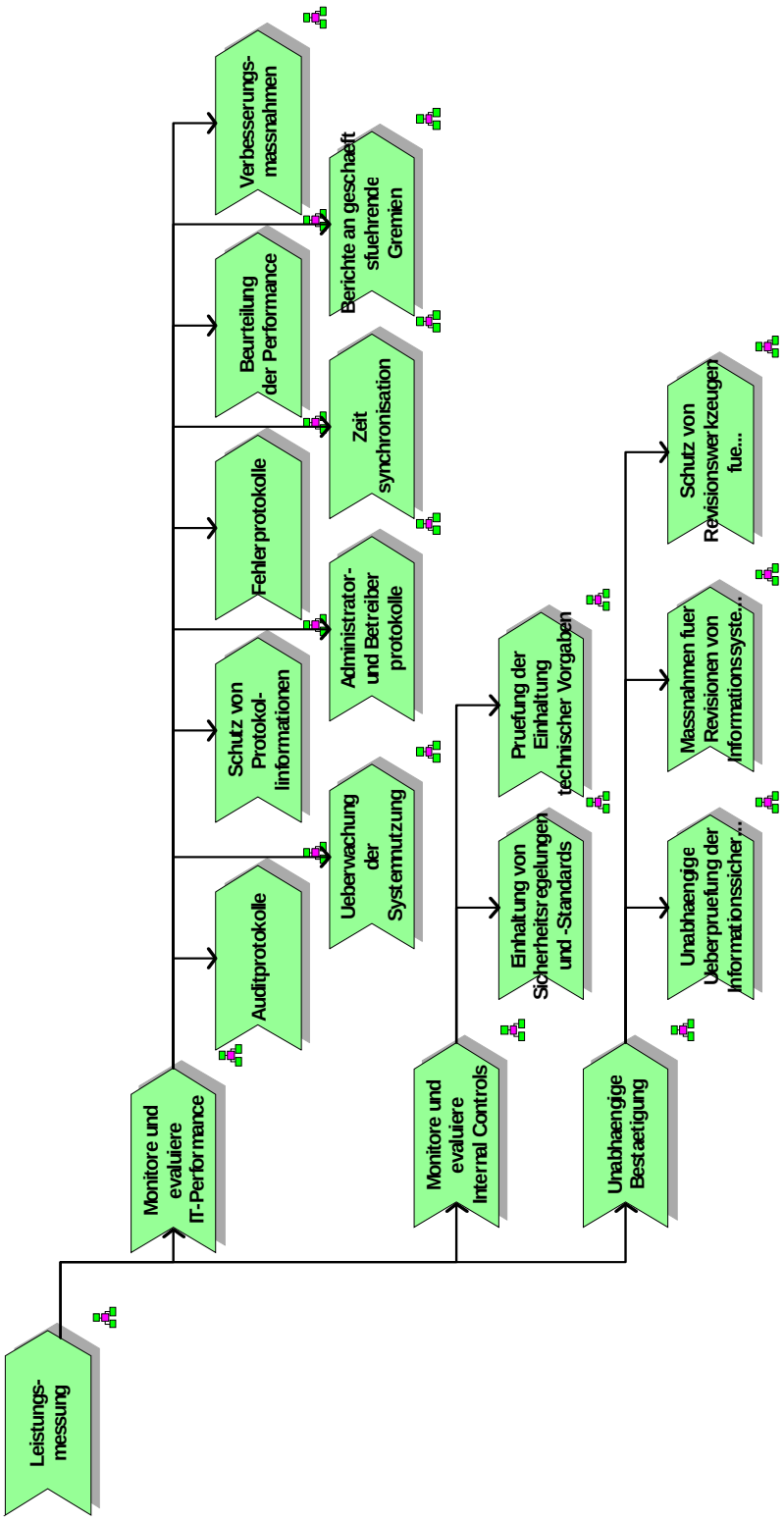

Abbildung A.13: Prozessindex Leistungsmessung

Literaturverzeichnis

[Abts/Mülder2004]: D. Abts/W. Mülder: Grundkurs Wirtschaftsinformatik, Eine kompakte und praxisorientierte Einführung. 5. Auflage. 2004.

[AISG2003]: Moulton, R. and Coles, R.S.: Applying Information Security Governance. Computers & Security, Vol. 22, No. 7, 2003.

[ANAO2003]: Public Sector Governance Volume 1 Better Practice Guide Framework, Process and Practices. Australian National Audit Office.

[Bec97]: Jörg Becker: Grundsätze ordnungsmäßiger Modellierung – Über Kontruktivisten, Handels- H´s und Referenzmodelle. http://www.wi.uni-muenster.de/improot/is/pub_imperia/doc/1794.pdf. *(16.11.09)*

[Bec98]: Jörg Becker: Die Grundsätze ordnungsmäßiger Modellierung und ihre Einbettung in ein Vorgehensmodell zur Erstellung betrieblicher Informationsmodelle.

[Binner1997]: Hartmut F. Binner: Integriertes Organisations- und Prozess-management, 1. Aufl. – München; Wien: Hanser, 1997.

[BSI-Standard]: BSI-Standard 100-2 IT - Grundschutz-Vorgehensweise. http://www.bsi.bund.de/literat/bsi_standard/standard_1002.pdf. *(16.11.09)*

[Buchsein2008]: R. Buchsein/F. Victor/H. Günter/V. Machmeier: IT-Management mit ITIL V3, Strategien, Kennzahlen, Umsetzung, 2. aktualisierte und erweiterte Auflage 2008.

[CIO2007]: CIO:http://www.presseportal.de/pm/39396/995107/idg_cio_it_

wirtschaftsmagazin. Ausgabe 06/2007. *(16.11.09)*

[Druker1993]: Drucker, Peter; Management Challenges for the 21st Century, Harpers Business, 1993.

[Kodex 2005]: Deutscher Corporate Governance Kodex, in der Fassung vom 2. Juni 2005, Regierungskommission Deutscher Corporate Governance Kodex.http://www.corporate-governance-code.de/ger/download/D_CorGov_Endfassung2005.pdf. *(16.11.09)*

[GCCG2001]: German Code of Corporate Governance (GCCG), Berliner Initiativkreis German Code of Corporate Governance, 2000 http://www.ecgi.org/codes/documents/gccg_d.pdf.

[GIS2007]: Sangkyum Kim: Governance of Information Security: New Paradigm of Security Management. In Computational Intelligence in Information Assurance and Security. 2007.

[Gossy2008]: Gregor Gossy: A Stakeholder Rationale for Risk Management, Implications for Corporate Finance Decisions, 2008.

[Goltsche2006]:Wolfgang Goltsche: COBIT kompakt und verständlich: Der Standard zur IT Governance – So gewinnen Sie Kontrolle über Ihre IT – So steuern Sie Ihre IT und erreichen Ihr Ziele. 2006.

[Han/Neu]: H.R. Hansen/ G. Neumann: Arbeitsbuch Wirtschaftsinformatik, 7. Auflage.

[Heinrich2004]: L.J.Heinrich/A.Heinzl/F. Roithmayr: Wirtschaftsinformatik-Lexikon, 7. Auflage, 2004.

[ISG2009]: S.H.von Solms/ R.von Solms: Information Security Governance, 2009.

[ISM2006]: Jochen Brunnstein; ITIL Security Management realisieren, IT-Service

Security Management nach ITIL- So gehen Sie vor. 2006.

[ISO27001]: ISO/IEC FDIS 27001:2005 Information technology - Security techniques – Information security management systems – Requirements. 2005.

[ITS 2009]: An Introduction to the Business Model for Information Security. ISACA

[ITGI2003a]: IT Governance Institute: Board Briefing on IT Governance. ITGI 2003, 2nd Edition.

[ITGI2003b]: IT Governance Institute: IT Governance für Geschäftsführer und Vorstände, 2. Ausgabe. http://www.itgi.org/Template.cfm?Section=Home&CONTENTID=14529&TEMPLATE=/ContentManagement/ContentDisplay.cfm. *(16.11.09)*

[ITGI2005]: IT Governance Institute: CobiT 4.0, Deutsche Ausgabe, 2005. http://www.isaca.at/Ressourcen/CobiT%204.0%20Deutsch.pdf. *(16.11.09)*

[ITGI2006 a]: IT Governance Institute: Information Security Governance - Guidance for Boards of Directors and Executive Management. ITGI, 2006, 2nd Edition.

[ITGI2006 b]: About ITGI. http://www.itgi.org/template_ITGI.cfm?Section=About_ITGI&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19648. *(16.11.09)*

[ITGI2006 c]: IT Governance Institute: CobiT Mapping, Mapping of ISO/IEC 17799: 2005 with CobiT 4.0, 2006.

[ITGI2006 d]: IT Governance Institute: CobiT Mapping, Mapping of ITIL v3 with

COBIT 4.1. 2006

[ITGI2007a]: IT Governance Institute: CobiT Security Baseline, An Information Security Survival Kit 2nd Edition.

[ITGI2007b]: IT Governance Institute: CobiT 4.1, 2007.

[ITGI2008]: IT Governance Institute: Aligning CobiT 4.1, ITIL, V3 and ISO/IEC 27002 für Business Benefit, A Management Briefing Form ITGI and OGC, 2008. http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=45932. *(16.11.09)*

[ITSM2008]: H.Kersten/J.Reuter/ K.W. Schröder: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Der Weg zur Zertifizierung, Herausgegeben von Heinrich Kersten und Klaus-Dieter Wolfenstetter, 2008.

[ITS2007]: Marcus Heitmann: IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie. 2007.

[Mertens2007]: Peter Mertens: Operative Systeme in der Industrie, Band 1 von Gabler Lehrbuch. Gabler Wiesbaden, 16. Auflage, 2007.

[Müller2008]: Klaus-Rainer Müller: IT-Sicherheit mit System: Sicherheitspyramide –Sicheits-, Kontinuitäts- und Risikomanagement-Normen und Practices- SOA und Softwareentwicklung. 3., erweiterte und aktualisierte Auflage. 2008.

[OECD2004]: Organisation für wirtschaftliche Zusammenarbeit und Entwicklung: OECD-Grundsätze der Corporate Governance, Neufassung 2004, http://www.oecd.org/dataoecd/57/19/32159487.pdf. *(16.11.09)*

[Olbrich2008]: Alfred Olbrich: ITIL kompakt und Verständlich: Effizientes IT Service Management- Den Standard für IT-Prozesse kennenlernen, verstehen und erfolgreich in der Praxis umsetzen. 4., erweiterte und verbesserte Auflage. 2008.

[Lektion2009]: Online-Verwaltungslexikon, Management und Reform der öffentlichen Verwaltung. www.olev.de

[Rastogi/Solms2006]: R. Rastogi/ R. von Solms: Information Security Governance – A re-definition. IFIP International Federation for Information Processing, Springer Boston, 193/2006

[Ros96]: Meichael Rosemann: Komplexitätsmanagement in Prozeßmodellen, methodenspezifische Gestaltungsempfehlungen für die Informations-modellierung/ Miechael Rosenmann.- Wiesbanden: Gabler. 1996

[Rau/Sch2003]: Claus Rautenstrauch/Thomas Schulze: Informatik für Wirtschaftswissenschaftler und Wirtschaftsinformatiker. 2003.

[Stych/Zeppenfeld2008]: Christof Stych/ Klaus Zeppenfeld: ITIL. 2008.

[Schütte98]: Schütte, R.: Grundsätze ordnungsmäßiger Referenzmodellierung, Konstruktion konfigurations- und anpassungsorientierter Modelle. Wiesbaden 1998.

[Sei2006]: Heinrich Seidlmeier: Prozessmodellierung mit ARIS: Eine beispielorientierte Einführung für Studium und Praxis. Aktualisiert Auflage November 2006.

[Sewera2005]: Sonja Sewera: Referenzmodelle im Rahmen von IT-Governance CobiT ITIL MOF, arbeit im Rahmen des Seminars auf Informationswirtschaft im SS2005. http://wwwai.wu-wien.ac.at/~koch/lehre/inf-sem-ss-05/referenzmodelle.pdf.*(16.11.09)*

[Scheer2001]: August-Wilhelm Scheer: ARIS- Modellierungsmethoden Metamodelle. Anwendungen. Springer, Berlin, Vierte Auflage. 2001

[Scheer96]: A.W. Scheer: ARIS-Toolset: Von Forschungs-Prototypen zum Produkt, Praxisbericht, Informatik-Spektrum 19: 71-78 (1996)

[Siems2008]: Florian U. Siems/Manfred Brandstätter/Herbert Gölzner (Hrsg.): Anspruchsgruppenorientierte Kommunikation, Neue Ansätze zu Kunden-, Mitarbeiter- und Unternehmenskommunikation. 1. Auflage, 2008.

[Stahlknecht/Hasenkamp2005]: Stahlknecht/Hasenkamp: Einführung in die Wirtschaftsinformatik. 11. Auflage. 2005

[Widhalm2002]: Richard. Widhalm /Thomas Mück: Topic Maps, 2002.

Selbstständigkeitserklärung

Ich versichere, dass ich die Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Die Stellen der Arbeit, die anderen Werken dem Wortlaut oder dem Sinn nach entnommen sind, habe ich unter Angabe der Quellen der Entlehnung kenntlich gemacht. Dies gilt sinngemäß auch für gelieferte Zeichnungen, Skizzen und bildliche Darstellungen und dergleichen.

_____ _____

Ort, Datum Unterschrift