Thema:

Erarbeitung eines Referenzmodells zur Einführung eines Informationssicherheits-Managementsystems nach ISO 27001 auf Basis IT-Grundschutz

Diplomarbeit

Arbeitsgruppe Wirtschaftsinformatik

Themensteller: Prof. Dr. rer. pol. habil. Hans-Knud Arndt

Betreuer: Prof. Dr. rer. pol. habil. Hans-Knud Arndt

Vorgelegt von: Martin Holger Hübner

Abgabetermin: 25.08.08

Inhaltsverzeichnis

Abkürzungsverzeichnis

ARIS	Architektur integrierter Informationssysteme
BSI	Bundesamt für Sicherheit in der Informationstechnik
COBIT	Control Objectives for Information and related Technology
DV	Datenverarbeitung
eEPK	erweiterte ereignisgesteuerte Prozesskette
EPK	ereignisgesteuerte Prozesskette
FB	Funktionsbaum
GoM	Grundsätze ordnungsgemäßer Modellierung
GSTOOL	Grundschutz-Tool
ISACA	Information System Audit und Control Association
IS	Informationssicherheit
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
ITGI	IT Governance Institute
ITIL	IT Infrastructure Libary
OGC	Office Of Government Commerce
PDCA	Plan-Do-Check-Act
WKD	Wertschöpfungskettendiagramm

Abbildungsverzeichnis

Tabellenverzeichnis

1 Motivation und Zielsetzung

In einer Welt die zunehmend auf den Schutz der Informationen und Daten angewiesen ist, wird es zu einer zentralen Aufgabe der Organisationsführung für die Aufrechterhaltung der Informationssicherheit Sorge zu tragen. Einzellösungen wie Firewall, Virenschutz oder Verschlüsselung sind Teilaspekte eines größeren Ganzen. Ein umfassender Schutz vor Angriffen von Innen und Außen ist mit ihnen nicht zu realisieren. Das Zusammenspiel von organisatorischen sowie technischen Schutzmechanismen ist ganzheitlich zu betrachten. Das Bundesamt für Sicherheit in der Informationstechnik geht in ihrem Bericht „Die Lage der IT-Sicherheit in Deutschland 2007“ auf die zukünftigen Trends der IT-Bedrohungen näher ein und verdeutlicht, dass eher mit einem Anstieg als mit einer Abschwächung der Bedrohungslage gerechnet wird.

Quelle: Lage der IT-Sicherheit, S.67

Abb. 1.1: Entwicklung von IT-Bedrohungen

Der Aufbau eines Managementsystems, welches die Informationssicherheit als ganzheitlichen Ansatz in allen Organisationsbereichen abdeckt, ist von zentraler Bedeutung. Das Ziel der Etablierung eines institutionsweiten Informationssicherheitsprozesses kann nur zu Stande kommen, wenn die Organisationsleitung die Informationssicherheit als zentrale Aufgabe versteht. Um den Aufbau und die Aufrechterhaltung eines solchen Managementsystems zu bewerkstelligen, gibt die International Organization for Standardization (ISO) eine Norm vor, die sich zentral mit diesem Thema befasst. Es handelt sich dabei um die ISO 27001:2005. Da die ISO 27001:2005 aufgrund ihrer allgemeinen

Formulierungen aber keine Hilfe bei der Umsetzung stellt, wird der IT-Grundschutz, welcher vom Bundesamt für Sicherheit in der Informationstechnik gefördert wird, zusätzlich betrachtet.

Die ISO 27001 und der IT-Grundschutz bilden die Voraussetzungen für die Einführung eines Informationssicherheits-Managementsystems. Mit ihnen ist es möglich einen theoretischen und praktischen Umgang mit dem Thema Informationssicherheit organisationsweit zu erreichen.

Zielsetzung

Ziel der Diplomarbeit ist es ein Referenzmodell für ein Informationssicherheits-Managementsystem (ISMS) auf Basis der ISO 27001 und unter Zuhilfenahme des IT-Grundschutz zu erarbeiten. Die IT-Grundschutz-Vorgehensweise zur Einführung und Aufrechterhaltung eines Managementsystems zur Informationssicherheit wird als wesentlicher Teil bei der Modellierung betrachtet. Das erstellte Referenzmodell soll einerseits die zentralen Punkte der ISO 27001 Norm mit den praktischen Hilfen des IT-Grundschutzes verbinden und andererseits einen leicht anwendbaren Rahmen bieten, an dem sich Organisationen orientieren können, um ihre eigenen Realisierungen auszurichten.

Aufbau der Arbeit

Die Arbeit gliedert sich in die folgende Kapitelstruktur. Das Kapitel zwei geht auf die Grundsätze der ordnungsgemäßen Modellierung und auf die Phasen der Referenzmodellierung näher ein. Im Anschluss befasst sich Kapitel drei mit der ersten Phase der Referenzmodellierung, der Problemdefinition. Ein Einblick in die Thematik Managementsystem wird gegeben, der PDCA-Zyklus und Standards mit Bezug Informationssicherheits-Managementsystem werden vorgestellt. Kapitel vier widmet sich der zweiten Phase der Referenzmodellierung. Das verwendete Modellierungskonzept sowie das Modellierungswerkzeug werden vorgestellt. Nachfolgend wird sich Kapitel fünf dem erstellten Referenzmodell zu wenden. Die dritte und vierte Phase der Referenzmodellierung, die Referenzstruktur und die Komplettierung, des erstellten Referenzmodells werden vorgestellt. Die Anwendungsmöglichkeiten sowie die Bewertung des Referenzmodells werden in Kapitel sechs näher untersucht. Dieses Kapitel stellt die fünfte Phase der Referenzmodellierung dar.

2 Modellierungsgrundsätze

Bevor man sich der eigentlichen Modellierung zuwendet, ist es wichtig ein Verständnis zu erhalten, welche Grundsätze bei der Modellierung zu beachten sind. Die unter den Grundsätzen der ordnungsgemäßen Modellierung (GoM) zu beachtenden Kernpunkte werden in diesem Kapitel näher vorgestellt.

Im Vorfeld sind die wichtigsten Begriffe der Arbeit zu definieren. Diese nehmen eine zentrale Stellung ein und werden auf den folgenden Seiten näher vorgestellt.

Was ist ein Prozess?

Als erstes wird der Prozessbegriff definiert. „Ein Prozess stellt die inhaltliche abgeschlossene, zeitlich und sachlogische Abfolge der Funktionen dar, die zur Bearbeitung eines betriebswirtschaftlich relevanten Objekts ausgeführt werden.“[1]

„Als Prozess bezeichnen wir einen Vorgang, zu dem es eine Ablaufbeschreibung (Schema) gibt. Dabei unterscheidet man technische Prozesse (Beschreibung von Bewegungen) und ergonomische Prozesse (Beschreibung von Handlungen). Es ist klar, daß viele Arbeitsprozesse - synonym auch Arbeitsabläufe - Kombinationen aus technischen und ergonomischen Prozessen sind.“[2]

Was ist ein Modell?

„Ein Modell ist ein abstraktes, immaterielles Abbild realer Strukturen bzw. des realen Verhaltens für Zwecke des Subjekts. Das Subjekt, auch Modelladressat oder Auftraggeber genannt, ist hier stets das Unternehmen, d.h. die Frage der Relevanz von Modellelementen ist anhand der Unternehmenszwecke, aus denen sich die Modellierungszwecke ableiten, zu beantworten. Ein Modell kann damit auch als adäquates, vereinfachendes und idealisierendes Abbild der Realität charakterisiert werden.“[3]

„Ein Modell ist dabei ein immaterielles abstraktes Abbild der Realwelt für die Zwecke eines Subjektes. Modelle werden als Hilfsmittel zur Erklärung und Gestaltung realer Systeme eingesetzt. Erkenntnisse über Zusammenhänge und Sachverhalte bei Realproblemen können mit Hilfe von Modellen aufgrund der Ähnlichkeit gewonnen werden, die zwischen dem realbetrieblichen System und dem Modell als Abbild dieses Systems bestehen. Sinn des Modells ist es damit, die Wirklichkeit so zu vereinfachen, daß sie für die Zwecke, die das Subjekt verfolgt, handhabbar ist. Im Modell finden also all die Ge-

1 Rosemann (1996), S.9
2 Jablonski/Böhm/Schulze (1997), S.24
3 Rautenstrauch/Schulze (2003), S.225

gebenheiten der Realwelt keine Berücksichtigung, die dem Zweck, den das Subjekt mit der Modellierung verfolgt, nicht dienlich sind.“[4]

Was ist ein System?

„Ein System wird informell als eine Menge von Elementen mit Eigenschaften inklusive der zwischen diesen Elementen bestehenden Beziehungen verstanden (strukturelles Systemkonzept).“[5]

Was ist ein Prozessmodell?

„Prozessmodelle stellen zweckbezogene, immaterielle Abbilder des zeitlich-sachlogischen Ablaufs der Funktionen dar, die an einem Objekt durchgeführt werden.“[6]

Was ist ein Metamodell?

Ein Metamodell beschreibt die Syntax des Modells bzw. den Prozess der Modellerstellung.[7]

Was ist Prozessmanagement?

Prozessmanagement übernimmt die Aufgabe der Planung, Steuerung, Durchführung und Kontrolle der Prozesse im Hinblick auf die angestrebten Ziele. [8]

Nutzengewinn mit der Ausrichtung an Prozessen

Mit der verstärkten Ausrichtung an Prozessen werden betriebswirtschaftliche Nutzeneffekte gefördert. Diese Nutzeneffekte resultieren aus der Integration von objektbezogen zusammengehörigen Aktivitäten. Die prozessorientierte Unternehmensgestaltung setzt die Betonung auf den Faktor Zeit. Eine Reduzierung der Durchlaufzeiten von Prozessen spielt eine zentrale Rolle. Zugleich ist die Verstärkung der Kundenorientierung durch die Prozessausrichtung gewährleistet. Der Kunde (intern oder extern) als Auslöser des Prozesses ist zu betrachten. Durch die verstärkte Ausrichtung an Prozessen erfolgt eine Reduktion des objektbezogenen Koordinationsaufwands. Dies bedeutet, dass organisatorische Schnittstellen durch eine prozessgetriebene Neugestaltung, beispielsweise durch die Institutionalisierung von Prozessverantwortung minimiert werden. Die Prozesskomplexität wird durch die Reduzierung der Anzahl an Prozessobjekten (z.B. durch

4 Vossen/Becker (1996), S.19
5 Rosemann (1996), S.14
6 Rosemann (1996), S.1
7 Vgl. Rosemann (1996), S.37
8 Vgl. Rosemann (1996), S.12

Bildung logischer Einheiten) verringert. Zugleich werden die Medienbrüche minimiert. Eine durchgängige informationstechnische Unterstützung der Prozesse wird angestrebt. Die Messbarkeit des Zielbeitrags der Organisation steigt mit der organisatorischen Ausrichtung an Prozessen.[9]

2.1 Grundsätze ordnungsgemäßer Modellierung

Die Grundsätze ordnungsgemäßer Modellierung sollen helfen die Eigenkomplexität von Prozessmodellen einzugrenzen. Die Eigenkomplexität ist gekennzeichnet durch das vorhanden sein von rudimentären Notationsregeln. Diese erlauben erhebliche Freiheitsgrade durch rein syntaktische Reglementierungen. Ein Prozessmodell wird einem Kunstwerk gleich, das Verständnis besitzt nur der Schöpfer. Die Partizipation heterogener Anwenderkreise mit unterschiedlichen Zielsetzungen soll gefördert werden und die Gefahr der Einzelprozessanalysen, d.h. ein einzelner Prozess wird ohne Berücksichtigung der Wechselwirkungen betrachtet, vermieden werden.[10]

Die Grundsätze ordnungsgemäßer Modellierung stellen einen Ordnungsrahmen dar, der die Modellqualität erhöht durch die Einhaltung von Gestaltungsempfehlungen. Die Modellqualität wird als Verwendungseignung des Modells anhand der verbunden Modellzielsetzung definiert. Die Begrenzung der Freiheitsgrade bei der Modellierung führt zu einer Reduzierung des subjektiven Elements im Modellentstehungsprozesses sowie der daraus hervorgehenden Komplexität. Zielsetzung der Grundsätze der ordnungsgemäßen Modellierung ist die Beherrschung der Komplexität und die Erhöhung der Qualität von Prozessmodellen.[11]

Die Grundsätze der ordnungsgemäßen Modellierung untergliedern sich in die folgenden Grundsätze[12]:

- Grundsatz der (syntaktischen bzw. semantischen) Richtigkeit
- Grundsatz der Relevanz
- Grundsatz des semantischen Aufbaus
- Grundsatz der Vergleichbarkeit

---

9 Vgl. Rosemann (1996), S.12
10 Vgl. Rosemann (1996), S.2f
11 Vgl. Rosemann (1996), Vorwort
12 Vgl. Rosemann (1996), S. 91

- Grundsatz der Klarheit
- Grundsatz der Wirtschaftlichkeit

Diese Grundsätze werden in den folgenden Abschnitten näher beschrieben.

Grundsatz der Richtigkeit

Der Grundsatz der Richtigkeit liegt in zwei Ausprägungen vor, der syntaktischen und der semantischen Richtigkeit.

Die syntaktische Richtigkeit untersucht den Tatbestand, ob das Modell richtig, also formal korrekt ist. Ein Modell ist syntaktisch richtig, wenn das Modell zu dem ihm zu Grunde liegende Metamodell konsistent ist. Die syntaktische Konsistenz liegt dann vor, wenn alle in dem Modell verwendeten Informationsobjekte und Notationsregeln durch das Metamodell erklärt werden. Die syntaktische Vollständigkeit wird erreicht wenn keine Konstrukte fehlen, welche die Modellsyntax zwingend erfordert. Der Fokus bei der syntaktischen Richtigkeit liegt auf der formellen Ausgestaltung von Prozessmodellen.

Die semantische Richtigkeit wendet sich der Struktur- und Verhaltenstreue zu. Die Struktur und das Verhalten des Modells gegenüber dem zu Grunde liegenden Objektsystem werden bemessen. Zusätzlich werden ein hohes Maß an Aktualität, der Ausweis des Erstelldatums und die zeitliche Gültigkeit des Modells angestrebt. Die semantische Konsistenz, also die konsequente Verwendung von Bezeichnungen im Daten- und Prozessmodell ist durchzusetzen. Einheitliche Namenskonventionen sind einzurichten. Nachteil der semantischen Richtigkeit ist, dass eine Überprüfung formal nahezu unmöglich ist. Eine Konsistenzprüfung ist aber durchführbar.[13]

Grundsatz der Relevanz

Eine Priorisierung der modellierungswerten Bestandteile der Realwelt (betriebswirtschaftliche Kenngrößen z.B. Prozesskosten) strebt der Grundsatz der Relevanz an. Ein Modell ist erst relevant wenn der Nutzeneffekt eines Modells sinkt, falls das Modellsystem weniger Informationen enthalten würde. Grundsätzlich lässt sich sagen, dass Modelle so viele Informationen wie nötig und so wenig wie möglich enthalten sollten. Diese Minimalitätsanforderung ist zu beachten. Der Grundsatz der Relevanz kann nur auf individuelle Modellierungsziele angewendet werden. Diese mit der Modellierung verbundenen Ziele sind festzulegen. Nur an diesen Zielen lässt sich die spätere Relevanz

[13] Vgl. Rosemann (1996), S.94

nachprüfen. Bei der Prüfung auf Relevanz sind sämtliche Modellkomponenten betroffen. Zum Einen muss das Objektsystem den Relevanzforderungen genügen, d.h. das Metamodell darf nicht zu umfangreich sein aber auch nicht zu klein. Die Wahl der Modellierungsmethode ist zu beachten. Zum Anderen sind die Freiheitsgrade im Modell nur nach Bedarf zu verwenden. Unter Freiheitsgrad ist der Abstraktionsgrad eines Modells gemeint. Je abstrakter das Modell desto wahrscheinlicher ist es, dass die Relevanz sinkt. Der Zusammenhang zwischen semantischer Richtigkeit zum Abstraktionsgrad ist abzuwägen.[14]

Grundsatz der Wirtschaftlichkeit

Die betriebswirtschaftlichen Aspekte werden beim Grundsatz der Wirtschaftlichkeit näher betrachtet. Aus Kostengründen können irrelevante Modellbestandteile (Siehe Grundsatz der Relevanz) entfernt oder auf die Erhöhung der Modellanschauung (Siehe Grundsatz der Klarheit) verzichtet werden. Der Grundsatz der Wirtschaftlichkeit setzt die obere Grenze bei der Modellierung. Der Erstellungsaufwand und Verwendungszweck spielen eine entscheidende Rolle. Wichtige Begriffe hierbei sind die Persistenz und die Flexibilität. Unter Persistenz versteht man die dauerhafte Beschaffenheit und das langfristige Fortbestehen des Modells. Flexibilität beschreibt die Anpassungsfähigkeit und Erweiterbarkeit eines Modells. Beide Sachverhalte spiegeln sich in den Kosten des Modells wider. Die Persistenz steigt mit dem Abstraktionsgrad, sinkt aber mit der Änderungsgeschwindigkeit des Objektsystems. Die Flexibilität kann an den erforderlichen Aufwand zur Anpassung an neue Sachverhalte bemessen werden. Mittel zur Kostenreduktion sind die Verwendung von Referenzmodellen, die Wiederverwendung von Modellbestandteilen sowie die Anwendung von Modellierungswerkzeugen. [15]

Grundsatz der Klarheit

Ein Modell muss gewährleisten, dass es für die Modelladressaten zugänglich und von diesen für ihre subjektiven Zielsetzungen anwendbar ist. Der Grundsatz der Klarheit wendet sich diesem Aspekt zu. Eine Abnahme der Modellklarheit geht einher mit der Reduzierung der Modelladressaten und dem Modellnutzen. Da die Beurteilung der Klarheit höchst subjektiver Art ist, ist er auch hochgradig vom Modelladressaten abhängig. Nicht-disjunkte, ästhetische Merkmale wie Strukturiertheit, intuitive Zugänglichkeit (Verständlichkeit), Übersichtlichkeit oder Lesbarkeit werden unter einem Oberbegriff zusammengeführt. Die Forderung nach einem einfachen Modell wird propagiert. Dieses zeichnet sich durch syntaktische Einfachheit aus. Sie verlangt den Einsatz von nur we-

---

14 Vgl. Rosemann (1996), S.95ff
15 Vgl. Rosemann (1996), S.97ff

nigen methodischen Konstrukten, die Abbildung der wesentlichen Sachverhalte sowie die Beachtung des Grundsatzes der Relevanz und der Wirtschaftlichkeit. Anordnungsbeziehungen wie symmetrische Modellstrukturen, Positionierung der Informationsobjekte in einem Raster, Kantenziehung nur in zwei orthogonale Dimensionen, maximale Gradlinigkeit der Kanten, minimale Kantenüberschneidungen sowie die graphische Hervorhebung von Korrespondenzen werden gefordert. Die notwendige Anschaulichkeit des Modells sollte mit einbezogen werden. Eine Beschreibung der Konstrukte fällt dem Grundsatz der Klarheit zu.[16]

Grundsatz der Vergleichbarkeit

Hinzufügend zu den anderen Grundsätzen sorgt der Grundsatz der Vergleichbarkeit für die modellübergreifende konforme Ausgestaltung der Grundsätze ordnungsgemäßer Modellierung. Der Grundsatz ist relevant beim arbeitsteiligen Modellierungsprozess. Besonders der Bedarf zum Abgleichen von Ist- mit Istmodellen (Tochterunternehmen, Ist-mit Sollmodellen (Bspw. bei Reorganisationsprojekt) oder Ist- mit Referenzmodellen (Bspw. der Beurteilung der Abdeckungsrate eines Softwareproduktes) spielt diesem Grundsatz zu. Werden die Modelle anhand unterschiedlicher Methoden erstellt so ist zu fordern das die zugrundeliegenden Metamodelle ineinander überführbar sind. Ein Metamodellvergleich ist dann anzuraten. Werden Modelle, die auf einem Metamodell beruhen verglichen, so setzt dies konventionsgerechte Objektbenennungen und Modellieungskonstrukte sowie gleichartige Detailierungsgrade voraus. Der Grundsatz der Vergleichbarkeit lässt sich vom Grundsatz der Konsistenz abgrenzen. Die Einheitlichkeit von Modellen steht im Vordergrund dieses Grundsatzes. Die Vergleichbarkeit wird durch die Analyse von Modellen auf Diskrepanzen und die Integration von Modellen herbeigeführt.[17]

Grundsatz des systematischen Aufbaus

Der Grundsatz des systematischen Aufbaus geht näher auf den Sachverhalt der Modellierung in einzelne Sichten ein. Die Integration der einzelnen Sichten muss mittels eines sichtenübergreifenden Metamodells gewährleistet sein. Erst dann ist eine Integration der einzelnen Modell und Informationsobjekte in den Sichten durchführbar. Die Forderung nach Integrationsfähigkeit wird vom Grundsatz des systematischen Aufbaus gefordert.[18]

---

16 Vgl. Rosemann (1996), S.99-102
17 Vgl. Rosemann (1996), S.102f
18 Vgl. Rosemann (1996), S.103f

2.2 Vorgehensmodell zur Referenzmodellierung

Die zuvor vorgestellten Grundsätze ordnungsgemäßer Modellierung werden bei der Erstellung des Referenzmodells angewendet. Da die Grundsätze der ordnungsgemäßen Modellierung lediglich auf die Qualität von Modellen eingehen wird für die Referenzmodellierung eine allgemeine Vorgehensweise zur Erstellung von Referenzmodellen herangezogen. Diese Vorgehensweise findet in der Diplomarbeit Anwendung und wird in diesem Teil der Diplomarbeit näher beschrieben.

Was ist ein Referenzmodell?

„Referenzmodelle als vom Einzelfall abstrahierende Repräsentationen betriebswirtschaftlichen Wissens können unterschiedlichen Zwecken dienen (z.B. referenzmodellbasierte Kopplung von Softwarekomponenten, Einführung von Standardsoftware, Wissensmanagement, Geschäftsprozessmanagement, Einführung eines Workflowmanagementsystems).“[19] „Referenz-Informationsmodelle, die hier verkürzt als Referenzmodelle bezeichnet werden, streben die Repräsentation allgemeingültiger betrieblicher Sachverhalte an.“[20] Für Unternehmen sind Referenzmodelle eine Ausgangslösung zur Prozessgestaltung. Die Anpassung des Referenzmodells an unternehmensspezifische Anforderung transformiert das Referenzmodell zu einem unternehmensbezogenen Modell.[21] Referenzmodelle gehen nicht auf Detailfragen ein sondern widmen sich in abstrahierter allgemeingültiger Art betrieblichen Sachverhalten.

Das Vorgehensmodell

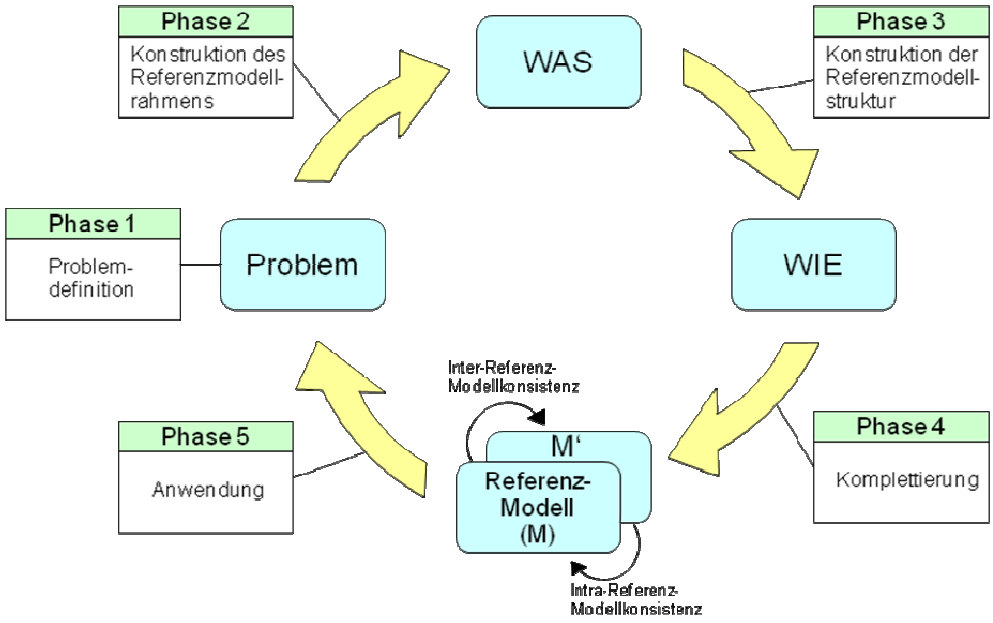
Die verwendete Vorgehensweise zur Referenzmodellierung gliedert sich in fünf Phasen. Diese Phasen sind[22]:

1. Phase: Problemdefinition
2. Phase: Konstruktion des Referenzmodellrahmens
3. Phase: Konstruktion der Referenzmodellstruktur
4. Phase: Komplettierung
5. Phase: Anwendung

---

19 Rosemann/Schütte (1999), S.22
20 Rosemann/Schütte (1999), S.23
21 Vgl. Scheer (2002), S.61
22 Vgl. Rosemann/Schütte (1999), S.26

Die Abb. 2.1 soll das Zusammenspielen der einzelnen Phasen näher verdeutlichen. Eine Beschreibung der einzelnen Phasen erfolgt auf den nachfolgenden Seiten.



Quelle: In Anlehnung an: Rosemann/Schütte (1999), S.27

Abb. 2.1: Modell zur Referenzmodellierung

Problemdefinition (Phase eins)

Die Problemdefinition bildet den Ausgangspunkt der Referenzmodellierung, in ihr wird die Modellplanung vorgenommen. Ein Fehler bei der Modellplanung kann später zu erheblichen Problemen führen. Dies geschieht meist dann, wenn ein Modell für ein Problem erarbeitet wird, das aber der Anwender in der Form nicht besitzt. Um diesem vorzubeugen ist das zu definierende Problem einem Einigungsprozess mit mehreren Personen zu unterziehen. Der Modellierer bezieht sich auf Hypothesen über Probleme, die dem Modellierer als relevant erscheinen. Eine Problemdefinition zieht Problemtypisierungen nach sich. Die Phase der Problemdefinition legt die grundsätzliche Abgrenzung des Gegenstandsbereiches aber auch grob die adressierten Perspektiven des zu erstellenden Referenzmodells fest. Es ist sicherzustellen, dass die Modellersteller die Perspektive der Modellnutzer einnehmen können. [23]

[23] Vgl. Rosemann/Schütte (1999), S.27f

Konstruktion des Referenzmodellrahmens (Phase zwei)

Nach der Definition des Problems ist die Methode zur Modellierung festzulegen. Es ist darauf zu achten, dass auf einem hohen Abstraktionsgrad eine für alle Anwender einheitliche Struktur der Modelle geschaffen wird. Um eine einheitliche Struktur zu erzeugen, kann man sich an Ordnungsrahmen halten. Ein Ordnungsrahmen gibt die relevante Struktur für eine Domäne wieder. Als Beispiele für Ordnungsrahmen seien hier das House-of-Facilities (Rahmen für das Facility-Management) sowie das Handels-H-Modell (Eine Architektur für Handelsinformationssysteme) genannt.[24]

Konstruktion der Referenzmodellstruktur (Phase drei)

Die zweite Phase spezifizierte das „WAS“ während die dritte Phase das „WIE“ spezifizieren soll. Die detailierte Struktur des Referenzmodellrahmens ist zu beschreiben. Als Anfangspunkt ist darzustellen, wie Alternativen im Prozess- und im Datenmodell isoliert voneinander abgebildet werden können. Im Prozessmodell werden dafür Buildtime-Operatoren verwendet (Konnektoren, die als OR, XOR bezeichnet werden). Im Datenmodell sind Buildtime-Beziehungen einzuführen. Eine Qualitätsbeurteilung der erstellten Modelle ist in dieser Phase durch den herangezogenen Interessenvertreter sicherzustellen.[25]

Komplettierung (Phase vier)

In der vierten Phase müssen die Referenzmodelle um Querverbindungen innerhalb des Referenzmodells und zwischen den Referenzmodellen erweitert werden. Erst dann ist eine konsistente Anwendung möglich. Die Verbindungen repräsentieren interne Verbindungen. In dieser Phase spielt auch die Integration von Modellen eine Rolle. Des Weiteren sind die Modelle in dieser Phase um quantitative Aussagen zu erweitern, wenn entsprechende Anforderungen gestellt wurden. Solche Anforderungen können Benchmarkingkennzahlen sein, wie Durchlaufzeiten, Auslastung, Kosten usw.[26]

Anwendung (Phase fünf)

Modelle können erst im konkreten Anwendungsfall ihren Nutzen entfalten. Eine Betrachtung des gesamten Zyklus von der Erstellung bis zur Anforderung ist für die kontinuierliche Weiterentwicklung eines Referenzmodells notwendig. Die Konstruktion und Anwendung von Modellen sollten eine Einheit bilden. Die Abweichung zwischen Refe-

---

24 Vgl. Rosemann/Schütte (1999), S.31f
25 Vgl. Rosemann/Schütte (1999), S.33-38
26 Vgl. Rosemann/Schütte (1999), S.38f

renzmodell und angepassten Modell dient als Maß. Treten Differenzen auf so führt dies zu einer eventuellen Erweiterung des Referenzmodells. Die Anwendung der Referenzmodelle ist an der Handlungsabsicht des Referenzmodellnutzers festzulegen.

Mit dem fünf Phasen umfassenden Vorgehensmodell sowie den Grundsätzen ordnungsgemäßer Modellierung lässt sich eine systematische, kriteriengeleitete Konstruktion und Anwendung von Referenzmodellen realisieren.[27]

Weitere Betrachtung

Die behandelten Phasen zur Referenzmodellierung werden in der Diplomarbeit umgesetzt. Kapitel drei wird die Phase eins, die Problemdefinition, näher untersuchen. Die Grundlagen der Managementsysteme bis hin zum ISMS und der IS0-27001 sowie dem IT-Grundschutz werden vorgestellt. Kapitel vier wendet sich der Phase zwei der Referenzmodellierung, der Konstruktion des Modellstrukturrahmens, zu. Die Grundlagen zur Architektur integrierter Informationssysteme sowie die Modellierungskonventionen werden vorgestellt. Das nachfolgende Kapitel fünf widmet sich der dritten und vierten Phase der Referenzmodellierung. Die inhaltlichen Schwerpunkte des verwendeten Standards sowie das Referenzmodell werden vorgestellt. Kapitel sechs geht näher auf die Anwendungsphase ein und gibt einen Überblick über die Anwendungsgebiete des erstellten Referenzmodells.

[27] Vgl. Rosemann/Schütte (1999), S.40-42

3 Problemdefinition

Dieser Teil der Diplomarbeit widmet sich der ersten Phase der Referenzmodellierung, der Problemdefinition. Zu Anfang wird auf das Thema Managementsysteme näher eingegangen. Im weiteren Verlauf des Kapitels werden der PDCA-Zyklus, die ISO 27001 und der IT-Grundschutz vorgestellt. Eine Einführung in die Thematik Informationssicherheits-Managementsysteme wird in diesem Kapitel angestrebt.

3.1 Managementsysteme

Als Einführung in die Thematik der Managementsysteme soll dieses Kapitel Einblick geben in die Ursprünge, der Begriffsentstehung, den Nutzen sowie den Gestaltungsregeln von Managementsystemen. Der Abschnitt wird die Grundgedanken eines Managementsystems widergeben, um im späteren Verlauf der Arbeit als Grundlage für das Managementsystem zur Informationssicherheit zu dienen.

Notwendigkeit von Managementsystemen

Managementsysteme haben ihren Ursprung in den Vereinigten Staaten von Amerika.[28] Die amerikanischen Unternehmen sahen sich einer aufkommenden Flut von Gerichtsprozessen gegenüber. Aufgrund des hohen Haftungsrisikos bei den Produkten und der Produktion, die mitunter den Kapitalwert des Unternehmens überschritten, war es Unternehmen nur möglich dieses Risiko zu begrenzen, indem die Unternehmen nachweisen, dass sie ihrer Sorgfaltspflicht bei allen Schritten der Entwicklung und Herstellung nachgekommen sind. Alle nach menschlichem Ermessen voraussehbaren Schadensfälle sind im Voraus zu berücksichtigen. Es sind zugleich Vorkehrungen zu treffen, die diese Vermeiden oder auf ein Minimum reduzieren. Das Unternehmen steht in der Nachweispflicht, dass die betriebliche Organisation im Hinblick auf die Entwicklung, die Herstellung, die Instruktion zum Umgang mit den Produkten sowie die Produktbeobachtung wirksam ist. Um diesen Sachverhalt umzusetzen, muss ein schriftlicher Beweis erbracht werden. Dieser Beweis ist erbracht mit der Durchführung von Kontrollen sowie der Dokumentation dieser Kontrollen. Qualitätsmanagementsysteme sind der Schlüssel zum Nachweis der Einhaltung dieser Sorgfaltspflichten. „.. sie beschreiben die Tätigkeiten in der Organisation, legen Umfang und Form der Aufzeichnung über getroffene Maßnahmen fest und beinhalten ein Verfahren zur dokumentierten Kontrolle der Durchführung.“[29] Neben der Einhaltung der Sorgfaltspflicht gibt es einen zweiten Grund der zum

---

[28] Vgl. Michael/Morawietz (1995), S.1
[29] Ahrens (2001), S.3

Durchbruch von Managementsystemen führte. In den Vereinigten Staaten gibt es kein Ausbildungssystem. Einen qualifizierten Berufsabschluss gibt es nicht, ein „learning by doing“ wird verfolgt. Ein Managementsystem-Handbuch mit Verfahrens- und Arbeitsanweisungen kann zum Anlernen der Mitarbeiter Verwendung finden und den Einarbeitungsprozess beschleunigen.

In Europa lagen diese Bedingungen nicht vor, dennoch kam es auch dort zum Einsatz von Managementsystemen. Dies liegt begründet in der Ausweitung der Kunden und Lieferantenbeziehungen. Der Trend zum Outsourcing aufgrund sinkender Transaktionskosten durch moderne Kommunikationsmethoden führte zu Problemen. Es fiel schwer die ausgegliederten Prozesse zu kontrollieren. Managementsysteme lösten diese Problematik. Ihre Einführung kann als eine vertrauensbildende und -erhaltende Maßnahme gesehen werden. Die Vertrauenswürdigkeit des Unternehmens steigt, wenn sich die Unternehmung einem Managementsystem unterordnet. Einem Lieferanten mit zertifiziertem Qualitätsmanagement traut man eher qualitätsgerechte Leistungen zu als Lieferanten ohne Zertifikat.

Ein weiterer Grund weshalb Managementsysteme sich auch außerhalb der Vereinigten Staaten durchgesetzt haben, ist die Schaffung neuer Anspruchsgruppen aufgrund der gesellschaftlichen Differenzierung. Nach Parson gliedert sich eine moderne Gesellschaft in vier Handlungssphären die untereinander agieren. Das Schema welches sich daraus ableitet wird als AGIL-Schema bezeichnet. Die erste Handlungssphäre ist die ökonomische Sphäre. In dieser Sphäre soll sich das Gesamtsystem flexibel und reaktionsschnell an die ständig verändernden Reaktionsbedingungen anpassen. Diese Adaption führt zum Namen der Sphäre die als A-System bezeichnet wird. Die politische Handlungssphäre grenzt das Gesamtsystem ein. Es werden bestimmte Ziele verfolgt, ein beliebiges Verhalten wird nicht gewünscht. Das System wird als G-System bezeichnet, welches sich aus dem englischen „Goul attainment“, (in deutsch „Zielerreichung“) ableitet. Die gemeinschaftliche Handlungssphäre soll die in den verschiedenen Handlungsfeldern tätigen Akteure in das Gesamtsystem integrieren und wird als I-System bezeichnet. Die letzte der vier Handlungssphären ist die kommunikative Handlungssphäre. Der Sinn des Gesamtsystems wird hier widergespiegelt. Nach ihrer englischen Bezeichnung „local pattern maintainance“ wird sie als L-System bezeichnet. Der Vorteil dieser Differenzierung der Gesellschaften liegt in der Spezialisierung auf bestimmte Aufgabenfelder und die Erbringung größerer spezifischer Leistungen. Dieses Schema zeigt, dass in modernen Gesellschaften Unternehmen trotz wirtschaftlicher Autonomie mit Forderungen konfrontiert werden, deren Ursprung in anderen Sphären zu suchen ist. Die Fremdsteuerung und Eigensteuerung werden dabei näher betrachtet. Eine Fremdsteuerung findet z.B. durch gesetzliche Regelungen statt. Die Forderung kommt von außen durch den

Gesetzgeber. Die Umsetzung bzw. Steuerung innerhalb des Unternehmens liegt aber in eigener Hand. Managementsysteme können nach außen anderen Sphären die Eigensteuerung näher bringen, indem sie dokumentiert aufzeigen wie sich zu Qualität, Umweltschutz und Informationssicherheit verhalten wird.

Die Notwendigkeit von Managementsystemen ergibt sich desweiteren durch die zunehmende Komplexität in Organisation und Technik. Dabei wird die Komplexität darin gesehen, dass aufgrund von Verknüpfungsengpässen nicht mehr jedes Element jederzeit mit jedem anderen Element verknüpft sein kann. Die Prozessvereinfachung bzw. das aufbrechen von alten Strukturen und die Schaffung kostengünstiger Produktionsverfahren fällt diesem Aspekt zu. Ziel ist es die Komplexität trotz ihrer Zunahme zu beherrschen. Managementsysteme erfüllen diesen Zweck. Sie erlauben es, in einer komplexen Organisation sowie im Hinblick auf komplexe technische Systeme Verantwortungen festzulegen.

Diese Komplexitätsbeherrschung ist der gemeinsame Kern von Managementsystemen. Alle Managementsysteme erreichen die Komplexitätsbeherrschung mittels Dokumentationen, explizierten Verantwortungszurechnungen, dokumentierten Kontrollen und nachzuweisenden Verbesserungen nach Bekanntgabe von Mängeln.[30]

Managementsysteme

Managementsysteme treten in zwei Formen auf. Die eine Form stellt die quasi natürlichen Managementsysteme dar, während die andere durch Gesetze, Vorgaben und Normen entsteht. Die quasi natürlichen Systeme liegen bereits vor der Einführung genormter Systeme vor und bilden eine Art Navigationssystem einer Organisation. Man spricht in diesem Zusammenhang auch oft von gewachsenen Strukturen. Die nicht natürlichen Systeme sollen die resultierenden Anforderungen aus Gesetzen, Vorgaben und Normen erfüllen. Zwischen beiden Managementsystemen kommt es zu Zielkonflikten. Diese liegen begründet in der Tatsache, dass beide Formen von Managementsystemen ein Eigenleben aufweisen.

Das Wort „manage“ stammt aus dem englischen und bedeutet dirigieren, kontrollieren, steuern und regeln. Es ist nicht gleichzusetzen mit der Person des Managers und dessen Führungsverhalten. Kamensky beschreibt Managementsysteme wie folgt. „Managementsysteme sind spezielle Formen von Systemen, die weniger abstrakt zu verstehen sind und ganz pragmatisch die Summe aller Regeln bezeichnen, die in einem abge-

[30] Vgl. Ahrens (2001), S.3-15

grenzbaren Regelwerk zusammengefasst sind, um das Management eines bestimmten Aufgabengebietes zu unterstützen.“[31]

Nutzen von Managementsystemen

Nachdem die Notwendigkeit sowie eine allgemeine Beschreibung des Begriffs Managementsystem in den beiden vorherigen Abschnitten erfolgten, wird sich dieser Teil dem Nutzen von Managementsystemen widmen. Nach Kamensky liegt der Nutzen von Managementsystemen in der:[32]

- Bereitstellung von Regeln und Prinzipien, welche das Verhalten einer Organisation vorausschauend lenken sollen und der Vermittlung der Sinnhaftigkeit dieser Regeln
- Verbindung der Organisation zu Markt und Gesellschaft zur Aufrechterhaltung der Existenz- und Entwicklungsfähigkeit
- Möglichst genaue Wiedergabe von Markt- und Rahmenbedingungen und der daraus resultierenden Anforderungen sowie der Übertragung der Anforderungen in Aufgaben
- Effiziente und effektive Umsetzung dieser Aufgaben und deren Kontrollen
- Speicherung des durch tätigkeitsbegleitenden Lernen erworbenen Wissens
- Vorsorge und Wertsicherung zur Erhaltung dieser Funktionen

Regeln zur Gestaltung von Managementsystemen

Managementsysteme müssen für jeden Einzelnen die Zusammenhänge und die Logik des Managementsystems erkennen lassen. Gestaltungsregeln zum zusammenhängenden Aufbau eines Managementsystems sollen in diesem Abschnitt näher beschrieben werden. Kamensky gibt sieben Gestaltungsregeln vor, die als Konstruktionsprinzipien herangezogen werden können.[33]

1. Informationen über den Sinn und die Grundregeln

---

31 Hofmann-Kamensky (2001), S.21
32 Vgl. Hofmann-Kamensky (2001), S.26
33 Vgl. Hofmann-Kamensky (2001), S.26-37

Managementsysteme sollen das gemeinsame Ziel verdeutlichen in dem sie die Kommunikation mittels Zielvorgaben und der grundsätzlichen Ausrichtung, durch Programme und Stellungnahmen zu wesentlichen Sinnfragen unterstützen.

2. Informationen über den Bauplan der Organisation

   Die Konstruktion eines Managementsystems also der planenden, sinn- und wertschöpfenden sowie wertsichernden Tätigkeiten ist mittels geeigneter Modelle darzustellen. Prozessmodelle können dies unterstützen.

3. Schaffung von Verhaltensspielräumen und sichere Einhaltung von Vorgaben

   Unerwünschtes Verhalten ist mittels Sollvorgaben zu unterbinden. Eine Kontrolle und Korrektur erfolgt beim Verstoß der Sollvorgaben.

4. Dauernde, schrittweise Verbesserung durch Regelkreise

   Die kontinuierliche Verbesserung ist zu verankern. Suche und Umsetzung von Verbesserungen sind als Dauerprozess zu verstehen und in geeigneter Form in Regelkreisen zu organisieren

5. Zulassen der Selbstorganisation

   Etablierung einer Eigenregelung von Teilsystemen über Sollwerte, Regeln und Schlüsselfaktoren. Diese Sollwerte und Regeln sind dem Gesamtplan unterzuordnen und bei Abweichungen zu kommunizieren.

6. Schnittstelle für Aufnahme und Abgabe von Informationen schaffen

   Kommunikationsvernetzung mit dem Unternehmensumfeld und ständige Prüfung und Aktualisierung der Organisationsvision ist zu etablieren.

7. Organisation des Lernens und Weiterentwicklung der Organisation

   Wissen und Lernen sind zu steuern, zu kontrollieren und durchzuführen. Der Aufbau eines Wissensspeichers und der Transfer von Wissen sind wesentlicher Bestandteil eines Managementsystems.

3.2 PDCA-Zyklus

Der PDCA-Kreislauf wurde in den 1930er Jahren von Walter A. Shewhart aufgestellt und in den 1950er Jahren von William Edwards Deming weiterentwickelt. Der amerikanische Physiker und Statistiker beeinflusste mit dem Vorgehensmodell maßgeblich das heute Qualitätsmanagement. Der PDCA-Zyklus beschreibt die Phasen im kontinuierlichen Verbesserungsprozess und ist auch nach diesen Phasen benannt. Der kontinuierliche Verbesserungsprozess obliegt der Maxime der stetigen Verbesserung. Diese Haltung muss das ganze Unternehmen und alle Aktivitäten umfassen. Kennzeichnend für die kontinuierliche Verbesserung sind stetig kleine Verbesserungsschritte, in kontinuierlicher Teamarbeit.

Die Phasen des PDCA-Kreislaufs zeigen sich wie folgt auf:

Plan: Diese Phase umfasst das erkennen von Verbesserungspotentialen, die Analyse des aktuellen Zustands sowie das entwickeln eines neuen Konzeptes

Do: Die konzipierten Planungen werden getestet und praktisch optimiert. Es finden Einzeltests z.B. mit provisorischen Einrichtungen statt. Der eigentliche Prozess soll vorerst nicht beeinflusst werden.

Check: Die im Kleinen stattgefunden Tests werden untersucht und ausgewertet. Eine Überprüfung auf Verbesserung findet statt. Überwiegen die Vorteile so wird die Umsetzung auf breiter Front freigegeben. Er wird als „Standard“ für den organisatorischen Ablauf freigegeben.

Act: In dieser Phase erfolgt die organisationsweite Umsetzung des Freigegebenen „Standards“. Eine regelmäßige Überprüfung der Einhaltung ist festzulegen. Die Verbesserung dieses Standards erfolgt wiederum in der Planungsphase „Plan“.

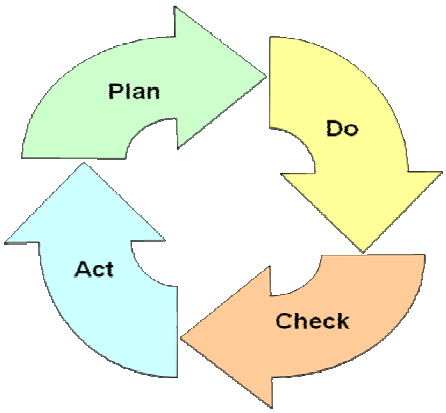


Abb. 3.1: PDCA-Kreislauf

Anhand der Abb. 3.1 zeigt sich, wie die einzelnen Phasen ineinander übergehen und einen Zyklus fortschreiben. Es zeigt sich, dass eine stetige Verbesserung stattfindet und die Maxime, nichts hinzunehmen, wie es ist, verfolgt wird.

3.3 Informationssicherheits-Managementsysteme

Das Thema dieser Arbeit widmet sich der Erarbeitung eines Referenzmodells für die Einführung eines Informationssicherheits-Managementsystems nach ISO 27001:2005 auf Basis IT-Grundschutz. In den folgenden Teilkapiteln wird näher auf die Bedeutung der Informationssicherheit in Organisationen eingegangen sowie der ISO 27001:2005 Standard und der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) vorgestellt. Zum besseren Verständnis werden im Folgenden die wichtigsten Begrifflichkeiten zum Thema Informationssicherheit näher beschrieben.

Informationen

Um Informationssicherheit näher beschreiben zu können, muss im Vorfeld der Begriff Information näher definiert werden. Der Informationsbegriff besitzt unterschiedliche spezifische Bedeutungen. In der Naturwissenschaft, der Technik und dem Bereich des menschlichen Handelns wird dies besonders deutlich sichtbar. Die Naturwissenschaften verstehen unter Information ein potenziell oder tatsächlich vorhandenes nutzbares Muster von Materie und Energieformen, das für den Betrachter innerhalb eines bestimmten Zusammenhangs relevant ist. Information ist das, was sich aus dem Zustand eines Systems für die Zustände anderer Systeme ableiten lässt. In der mathematischen Informationstheorie bezieht sich Information auf die Auftritts-Wahrscheinlichkeiten von bestimmten Folgen von Elementen (Folge von Buchstaben) aus einer festgelegten Menge (das Alphabet). Im Bereich des menschlichen Handelns wird unter Information ein Wissen (Ergebnis eines Erfahrungsprozesses) verstanden. Diese wird je nach Situation einer Bedeutung und Geltung beigemessen. Information wird zugleich mit der Beseitigung oder Verkleinerung von Ungewissheit verbunden. Dies geschieht mittels Auskunft, Aufklärung, Mitteilung, Benachrichtigung oder durch Kenntnis über Gegenstände. Das Wesentliche mit dem Begriff Information ist die Eigenschaft, Veränderungen im empfangenden System hervorzurufen.[34]

Information kann weiterhin definiert werden als: „Daten, die in eine Form gebracht wurden, die für Menschen bedeutungsvoll und nützlich ist.“[35] Daten sind als Fakten, die

---

[34] Vgl. Wikimedia Foundation Inc. (Hrsg.): Information, http://de.wikipedia.org/wiki/Information, [20.08.2008]

[35] Laudon et al. (2006), S.32

Ereignisse repräsentieren und noch nicht strukturiert oder in eine für den Menschen verarbeitungsfähige Form gebracht wurden, zu verstehen.[36]

Sicherheit

Unter Sicherheit versteht man einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird. Sicherheit, kann sich sowohl auf ein einzelnes Individuum als auch auf andere Lebewesen sowie auf unbelebte Objekte oder Systeme wie auch auf abstrakte Gegenstände beziehen.[37] Sicherheit kann nicht als ein unveränderbarer Zustand, der einmal erreicht wird und sich niemals ändert, angesehen werden. Organisationen sind dynamischen Veränderungen unterworfen, wie z.B. Änderungen an Geschäftsprozessen oder Veränderungen in der Organisationsstruktur. Die Sicherheit ist bei jeder Veränderung zu betrachten und aufrechtzuerhalten bzw. zu verbessern.[38]

Informationssicherheit

„Informationssicherheit hat als Ziel den Schutz von Informationen jeglicher Art und Herkunft. Dabei können Informationen sowohl auf Papier, in Rechnersystemen oder auch in Köpfen der Nutzer gespeichert sein.“[39] Informationssicherheit wird vielfältig mit IT-Sicherheit gleichgesetzt. Der Begriff IT-Sicherheit ist aber nicht umfassend genug. „IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung“[40]. IT-Sicherheit strebt den Schutz elektronischer Daten an ist aber im Zusammenhang mit der Sicherheit von Informationen nicht ausreichend. Die Sicherheit von Informationen wird nicht nur durch vorsätzliche Handlungen (z.B. Computer-Viren, Diebstahl von Rechnern) sondern unter anderen auch durch höhere Gewalt (z.B. Feuer), fehlerhafte Software-Update oder durch den eigenen Mitarbeiter gefährdet. Die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit sind die Grundlage für den Schutz von Informationen und damit der Informationssicherheit.[41]

Vertraulichkeit ist als Schutz der unbefugten Preisgabe von Informationen zu verstehen. Unter Integrität wird Sicherstellung der Korrektheit (Unversehrtheit) von Daten und Informationen sowie der konkreten Funktionsweise von Systemen verstanden. Verfüg-

---

36 Vgl. Laudon et al. (2006), S.32

37 Vgl. Wikimedia Foundation Inc. (Hrsg.): Information, http://de.wikipedia.org/wiki/Sicherheit, [20.08.2008]

38 Vgl. BSI-Standard 100-1, S.14

39 BSI-Standard 100-1, S.8

40 BSI-Standard 100-1, S.8

41 Vgl. BSI-Standard 100-1, S.8

barkeit als dritter Grundwert ist gegeben, wenn Dienstleistungen und Funktionen eines IT-Systems, von IT-Anwendungen oder IT-Netzen oder auch Informationen genutzt werden können, wenn der Anwender diese für seine Aufgabenerfüllung benötigt.[42]

Schwachstellen

Unter einer Schwachstelle versteht man einen sicherheitsrelevanten Fehler eines IT-Systems oder einer Institution. Ursprung von Schwachstellen liegen in der unzureichenden Konzeption, den angewendeten Algorithmen, der Implementierung, der Konfiguration, dem Betrieb sowie der Organisation. Eine Schwachstelle führt dazu, dass eine Bedrohung wirksam wird. Dies kann zu einer Schädigung der Institution oder des Systems führen. Durch eine Schwachstelle wird eine Institution oder ein System für Bedrohungen anfällig.[43]

Bedrohungen

Eine Bedrohung ist allgemein ein Ereignis oder Umstand, durch das oder den ein Schaden entstehen kann. Der Schadenswert bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. In der Informationstechnik ist eine Bedrohung ein Umstand, welcher die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann. Dem Eigentümer bzw. Anwender der Informationen kann ein Schaden entstehen. Bedrohungen treten in vielfacher Form auf. Beispiele sind höhere Gewalt wie Feuer, menschliche Fehlhandlungen wie unsachgemäße Handhabung von Softwarewerkzeugen, technisches Versagen wie der Ausfall von IT-Systemen oder vorsätzliche Handlungen wie Diebstahl oder Einbruch. Bei Auftritt einer Bedrohung auf eine Schwachstelle entsteht eine Gefährdung.[44]

Sicherheitsmaßnahmen

Unter einer Sicherheitsmaßnahme werden alle Aktionen bezeichnet, die Sicherheitsrisiken steuern und entgegenwirken. Dabei werden organisatorische, personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen mit eingeschlossen.[45] Beispiel für eine Sicherheitsmaßnahme ist die Sperrung des Arbeitsplatzrechners nach Aufgabenerfüllung sowie das Abschließen des Büroraums nach dem Verlassen.

---

42 Vgl. Glossar im IT-Grundschutz-Katalog
43 Vgl. Glossar im IT-Grundschutz-Katalog
44 Vgl. Glossar im IT-Grundschutz-Katalog
45 Vgl. Glossar im IT-Grundschutz-Katalog

Informationssicherheits-Management

Ein Informationssicherheits-Management übernimmt die Planungs- und Lenkungsaufgabe, die notwendig ist, um einen wirksamen Prozess zur Herstellung und Aufrechterhaltung von Informationssicherheit zu etablieren und kontinuierlich umzusetzen.[46]

Informationssicherheits-Managementsystem (ISMS)

„Ein ISMS legt fest, mit welchen Instrumenten und Methoden die Führungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt."[47] Zu diesen Aufgaben und Aktivitäten gehören Planung, Einsetzung, Durchführung, Überwachung und Verbesserung des ISMS.[48]

IT-Sicherheitsorganisation

Die IT-Sicherheitsorganisation dient neben dem Sicherheitskonzept zur Umsetzung der Sicherheitsstrategie. In ihr werden Regeln, Anweisungen, Prozesse, Abläufe und Strukturen definiert und dokumentiert.

IT-Sicherheitskonzept

„Ein IT-Sicherheitskonzept dient zur Umsetzung der IT-Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das IT-Sicherheitskonzept ist das zentrale Dokument im IT-Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete IT-Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen".[49]

IT-Sicherheitsstrategie

Mit einer IT-Sicherheitsstrategie wird das Vorgehen geplant, um einen kontinuierlichen IT-Sicherheitsprozess zu etablieren. Mit Hilfe eines IT-Sicherheitskonzepts und einer IT-Sicherheitsorganisation wird die IT-Sicherheitsstrategie umgesetzt.[50]

Sicherheitsleitlinie

Kernaussagen zu Sicherheitszielen und strategischen Vorgaben sind in der Sicherheitsleitlinie (engl. Information security policy oder IT security policy) zu dokumentieren.

---

46 Vgl. Glossar im IT-Grundschutz-Katalog
47 BSI-Standard 100-1, S.13
48 Vgl. BSI-Standard 100-1, S.12
49 Vgl. Glossar im IT-Grundschutz-Katalog
50 Vgl. BSI-Standard 100-1, S.17

Die Leitlinie soll die Sicherheitsziele, die Beziehung der Sicherheitsziele zu den Institutionszielen und das angestrebte Sicherheitsniveau wiedergeben. Desweiteren soll sie Aussagen treffen wie das angestrebte Sicherheitsniveau zu erreichen ist und wie es nachgewiesen werden kann.[51]

Risiko

Ein Risiko ist eine auf Berechnungen aufgebaute Vorhersage eines eventuell zu erwartenden Schadens oder möglichen Nutzens. Der Begriff kann zum einen positiv, als Chance, aber auch negativ als Gefahr aufgefasst werden. Die Wertvorstellung gibt vor, was als Chance bzw. Gefahr aufgefasst wird. Eine andere Definition von Risiko ist die Kombination aus Wahrscheinlichkeit des Schadensauftritts und der Schadenshöhe.[52]

Risikoanalyse

Mit Hilfe der Risikoanalyse wird untersucht welche Ereignisse zu Schäden führen können, wie hoch die Eintrittswahrscheinlichkeit ist und welche Folgen bei Eintritt der Ereignisse entstehen können.[53]

3.3.1 Standards mit Bezug auf Informationssicherheits-Managementsysteme

In den letzten Jahren kam es zu einer verstärkten Standardisierung im Bereich der Informationssicherheits-Managementsysteme. Dieses Kapitel soll einen kurzen Einblick über die derzeitigen Normierungen in diesem Bereich geben.

ISO 27000

Der ISO 27000 Standard gibt einen allgemein Überblick über Managementsysteme für Informationssicherheit. Dabei werden die Zusammenhänge der ISO-2700x-Familie mit berücksichtig. Grundlegende Prinzipien, Konzepte, Begriffe und Definitionen eines Informationssicherheits-Managementsystem werden vorgestellt.[54]

ISO 27001

Mit Hilfe des ISO-Standards 27001 „Information technologie – Security techniques – Information security management systems requirements specification“ ist es für Organisationen erstmals möglich sich im Bezug auf ihr Informationssicherheits-

---

51 Vgl. BSI-Standard 100-2, S.21
52 Vgl. Glossar im IT-Grundschutz-Katalog
53 Vgl. Glossar im IT-Grundschutz-Katalog
54 Vgl. BSI-Standard 100-1, S.9

Managementsystem zertifizieren zu lassen. Der Standard gibt allgemeine Empfehlungen. Diese beziehen sich auf die Einführung, den Betrieb und der Verbesserung eines dokumentierten Informationssicherheits-Managementsystems. Die Risikobetrachtung wird im Standard mit einbezogen. Der Standard besitzt einen Anhang, der auf die Maßnahmen aus der ISO 27002 verweist. Der Standard gibt dabei lediglich das Grundgerüst wider, praktische Hilfen sind nicht enthalten.[55]

ISO 27002

Die Inhalte des ISO-Standards 17799:2005 gingen Anfang 2008 in den Standard 27002 auf. Der Standard befasst sich mit den Schritten, die notwendig sind um ein funktionierendes Sicherheitsmanagement aufzubauen und es in der Organisation zu etablieren. Auf ungefähr 100 Seiten werden die Sicherheitsmaßnahmen kurz beschrieben. Schwerpunkt wird auf die Managementebene gelegt. Konkrete technische Hinweise werden nicht gegeben. Mit Hilfe der ISO 27002 ist es möglich die Anforderungen der ISO 27001 zu erfüllen.[56] Grundlage für die Standardisierung war hierbei die Sammlung von Erfahrungen, Verfahren und Methoden aus der Praxis. Diese wurden in einen „Best practice“ Ansatz zusammengeführt und als Standard etabliert. So erklärt sich auch der Aufbau des Standards. Er untergliedert sich in 11 Überwachungsbereiche. Diese werden in 39 Hauptkategorien, den Kontrollzielen („Controls objectives“) eingeteilt. Folgende Überwachungsbereiche liegen vor:[57]

- Information security policy – Informationssicherheitsleitlinie
- Organization of information security – Organisatorische Sicherheitsmaßnahmen und Managementprozesse
- Asset management – Verantwortung und Klassifizierung von Informationswerten
- Human resources security – Personelle Sicherheit
- Physical and Environmental Security – Physische Sicherheit und öffentliche Versorgungsdienste
- Communcations and operations Management – Netzwerk und Betriebssicherheit (Daten und Telefonie)

---

55 Vgl. BSI-Standard 100-1, S.9

56 Vgl. BSI-Standard 100-1, S.9

57 Herangezogen wurde die ISO 17799:2005 da die Inhalte der ISO 17799:2005 in der ISO 27002 aufgingen und es lediglich zu einer Änderung in der Kennzeichnung des Standards kam.

- Access control – Zugriffskontrolle
- Information systems acquisition, development and maintenance - Systementwicklung und Wartung
- Information security incident management – Umgang mit Sicherheitsvorfällen
- Business continuity Management – Notfallvorsorgeplanung
- Compliance – Einhaltung rechtlicher Vorgaben, der Sicherheitsrichtlinien und Überprüfung durch Audits

ISO 27005

Rahmenempfehlungen für das Risikomanagement für Informationssicherheit bietet der ISO-Standard 27005 „Information security risk management“. Er unterstützt die Umsetzung der Anforderung des ISO-Standards 27001. Der Standard löst den bisherigen ISO 13335-2 Standard ab. Dieser zweite Teil des ISO 13335 Standards widmete sich vorher den Techniken des Risikomanagements für Informationssicherheit.[58]

ISO 27006

Der ISO-Standard 27006 „Information technology – Security techniques – Requirements for the accreditation of bodies providing certification of information security management systems“ widmet sich der Zertifizierung. Der Standard spezifiziert Anforderungen an die Akkreditierung von Zertifizierungsstellen, welche sich der Zertifizierung eines Informationssicherheits-Managementsystem zuwenden. Er behandelt zudem die Besonderheiten der Zertifizierungsprozesse.[59]

IT-Grundschutz

Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationssicherheit (BSI) beschreibt das Management von Informationssicherheit und Sicherheitsmaßnahmen im Bereich Technik, Organisation, Personal und Infrastruktur. Das BSI stellt vier Standards sowie die IT-Grundschutz-Kataloge zur Verfügung. Die Standards setzen sich zusammen aus dem BSI-Standard 100-1 „Managementsysteme für Informationssicherheit“, BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“, BSI-Standard 100-3 „Risikoanalyse auf Basis von IT-Grundschutz und dem BSI-Standard 100-4 „Notfallmanagement“. Die IT-Grundschutz-Kataloge sind in Module unterteilt und enthalten Gefähr-

58 Vgl. BSI-Standard 100-1, S.9
59 Vgl. BSI-Standard 100-1, S.9

dungen und Sicherheitsmaßnahmen zu Prozessen, Anwendungen und IT-Komponenten. Nähere Informationen zum IT-Grundschutz werden im Kapitel 3.3.3 IT-Grundschutz gegeben.[60]

COBIT

COBIT (Control Objectives for Information and related Technology) definiert eine Methode zur Risikokontrolle. Augenmerk liegt hierbei auf den geschäftsrelevanten Abläufen, welche mittels IT unterstützt werden. Dokumentationen über COBIT werden vom IT Governance Institute (ITGI) welche der Information System Audit und Control Association (ISACA) angehört bereitgestellt. Die COBIT Entwickler orientierten sich an Standards im IT-Sicherheitsmanagement wie der ISO 27002.[61]

ITIL

Die IT Infrastructure Libary (ITIL) bietet umfangreiche Hilfe im Umgang mit dem IT-Service Management. Die Entwicklung lag beim United Kingdom's Office Of Government Commerce (OGC). Ziel von ITIL ist die Verbesserung der Qualität von IT-Services und der Kosteneffizienz sowohl aus Sicht einer internen IT-Abteilung als auch als externer Service-Provider.[62]

3.3.2 ISO 27001:2005

Nachdem ein kurzer Blick auf die Normierungen im Bereich Informationssicherheit gegeben wurde, wird sich dieses Kapitel der genaueren Analyse der ISO 27001:2005 sowie im kommenden Kapitel dem IT-Grundschutz widmen. Ziel ist es die beiden Konzepte näher vorzustellen, da sie für die spätere Modellierung von Bedeutung sind.

Die Entstehung der ISO 27001 lässt sich zurückführen auf das Jahr 1992. Am britischen Department of Trade und Industry wurde eine Kommission einberufen, die anerkannte Verfahren aus dem Bereich Informationssicherheit bewerten sollte. 1993 wurden diese Ergebnisse veröffentlich und 1995 vom Britischen Standard Institute als BS7799:1995 standardisiert. Ende 2005 erfolgte dann die ISO Zertifizierung. Der zweite Teil der BS7799 ging in der ISO 27001:2005 auf. Seitdem stellt die ISO 27001 den internationalen Standard für die Einführung und Bewertung eines Informationssicherheits-Managementsystems dar. Der prozessorientierte Aspekt, der Aufbau sowie die konti-

---

60 Vgl. BSI-Standard 100-1, S.10
61 Vgl. BSI-Standard 100-1, S.11
62 Vgl. BSI-Standard 100-1, S.12

nuierliche Verbesserung eines ISMS stehen im Vordergrund. Abb. 4.2 stellt den PDCA-Zyklus eines ISMS nach ISO 27001 vor. Die einzelnen Phasen sowie die Einwirkungen von sowie nach Außen werden dargestellt.

Quelle: In Anlehnung an: ISO 27001:2005

Abb. 3.2: PDCA-Zyklus ISO 27001

Inhaltliche Schwerpunkte der ISO 27001

Der Standard beginnt mit einer kurzen Erläuterung des Anwendungsbereiches sowie einer Definition der grundlegenden Begrifflichkeiten im Bereich Informationssicherheit. Kapitel vier des Standards widmet sich dem Informationssicherheits-Managementsystem selbst. In diesem Kapitel wird auf die generellen Anforderungen, der Festlegungen und Verwaltung sowie den Dokumentationsanforderungen an ein ISMS eingegangen. Das Teilkapitel „Festlegen und Verwalten eines ISMS“ geht hierbei auf die Aspekte Festlegung, Umsetzung und Durchführung, Überwachung und Überprüfung sowie Aufrechterhaltung und Verbesserung des ISMS näher ein. Kapitel fünf setzt sich mit den Verantwortungen des Managements auseinander. Im Fokus stehen in diesem Kapitel die Verpflichtungen der Institutionsleitung und die Verwaltung von Ressourcen. Die Verpflichtungen des Institutionsleitung umfassen die Punkte: Entwicklung der Sicherheitspolitik, Sicherstellung der Zielerreichung, Definition von Rollen und Verantwortlichen, Informationspolitik in der Institution zum Thema Informationssicherheit, Bereitstellung von Ressourcen zur Etablierung und Aufrechterhaltung, Risikoniveauabschätzung sowie die Bewertung des ISMS an sich. Kapitel sechs stellt Anforderungen hinsichtlich interner Überprüfungen (Audits) dar. Zielstellung ist es interne Überprüfungen zu planen und zu gestalten, so dass die Ergebnisse zur Bewertung des Managementsystems genutzt werden können. Kapitel sieben und acht stellen die Managementbewertungen sowie die Verbesserung des ISMS dar. In ihnen werden die Aspekte Informationseingang und Ergebnisse der Überprüfung des ISMS, kontinuierliche

Verbesserung sowie korrigierende und präventive Handlungen näher betrachtet. Der Anhang A des Standards repräsentiert die Abschnitte fünf bis fünfzehn des ISO 27002 Standards. Diese sollen als Unterstützung bei der Umsetzung eines ISMS dienen. Anhang B zeigt die OECD Richtlinie und deren Umsetzung in der ISO 27001 auf. Anhang C spiegelt den Zusammenhang zwischen ISO 9000, ISO 14001 und ISO 27001 wider. Die Anhänge B und C sollen Gemeinsamkeiten der zuvor genannten Standards hinsichtlich Überschrift und Kapitelnummerierung näher darstellen.[63]

3.3.3 IT-Grundschutz

Der IT-Grundschutz des Bundesamtes für Informationstechnik kann als Skizze zum Aufbau eines ISMS gesehen werden. Seinen Ursprung hat die Methodik im Jahr 1994 als das IT-Grundschutzhandbuch veröffentlicht wurde. Er beinhaltete zum damaligen Zeitpunkt nicht nur eine Methode zum Aufbau und zur Aufrechterhaltung eines ISMS sondern auch IT-Sicherheitsmaßnahmen zu Technik, Organisation, Personal und Infrastruktur. Im Jahre 2005 erfolgte eine Umstrukturierung des Werks. Eine Trennung des Grundschutzhandbuches in IT-Grundschutz-Vorgehensweise und IT-Grundschutz-Katalog erfolgte. Es entstanden die BSI-Standards 100-1, 100-2 sowie 100-3. Sie beschreiben die relevanten Sachverhalte zum Thema Informationssicherheit und die Vorgehensweise nach IT-Grundschutz.

BSI-Standards und IT-Grundschutz-Katalog

Die BSI-Standards unterteilen sich in unterschiedliche Themengebiete. Der BSI-Standard 100-1 definiert allgemeine Anforderungen an ein ISMS. Der Standard ist zugleich vollständig kompatibel mit der ISO-Norm 27001 und berücksichtigt desweiteren die Empfehlungen der ISO-Standard 27000 und 27002. Aufgrund seines Inhalts wird dieser Standard auch als „Managementsystem[e] für Informationssicherheit (ISMS)“ bezeichnet.

Die IT-Grundschutz-Vorgehensweise wird im BSI-Standard 100-2 näher vorgestellt. Dieser Standard wird als Schritt für Schritt Anleitung zum Aufbau und zum Betrieb eines ISMS angesehen. Schwerpunkt wird auf die Erstellung einer IT-Sicherheitskonzeption, die Auswahl von Sicherheitsmaßnahmen, der Umsetzung der erstellten Sicherheitskonzeption sowie die Aufrechterhaltung des ISMSs im laufenden Betrieb gelegt. Der Standard repräsentiert die Anforderungen der ISO-Standard 27000, 27001 und 27002. Der dritte Standard „Risikoanalyse auf Basis IT-Grundschutz“ gibt

---

63 Vgl. ISO 27001:2005, S.1-33

die Methodik zur Risikoanalyse nach IT-Grundschutz wider. Die Besonderheit der Risikoanalyse auf Basis IT-Grundschutz liegt darin begründet, dass der IT-Grundschutz auf eine detailierte Risikoanalyse mit Eintrittswahrscheinlichkeit und Schadenshöhe verzichtet. Vielmehr werden Schutzbedarfskategorien gebildet und dem Untersuchungsgegenstand zugeordnet. Diese legen im Anschluss fest welche Sicherheitsmaßnahmen aus dem IT-Grundschutz-Katalog angewendet werden müssen bzw. ob zusätzliche Maßnahmen zu ergreifen sind. Seit 2007 ist ein vierter Standard in Arbeit. Er wird sich dem Notfallmanagement widmen und steht mit Entwurfsversion 0.9 bereits zur freien Verfügung. Die Aufrechterhaltung und Etablierung des Notfallmanagements stehen bei diesem BSI-Standard im Vordergrund. Neben den vier Standards gibt es weiterhin den IT-Grundschutz-Katalog. Der Aufbau des Katalogs ist generisch gehalten. Im 1. Kapitel führt ein Vorspann in die Thematik ein. Kapitel zwei widmet sich dem Aufbau des Kataloges. Nach den beiden Kapiteln schließen sich die Baustein-Kataloge an. Diese Kataloge sind in übergreifende Aspekte, Infrastruktur, IT-Systeme, Netze und Anwendungen unterteilt und spiegeln typische Bereiche und Aspekte zum Thema Informationssicherheit wieder. Übergreifende Themen (z.B. Datensicherungskonzept) und spezielle Komponenten der IT-Umgebung (z.B. Windows XP) werden als Bausteine im Katalog aufgeführt. Im Anschluss an die Baustein-Kataloge folgen die Gefährdungs-Kataloge und die Maßnahmen-Kataloge. In ihnen werden die Gefährdungen und Maßnahmen ohne die Zuordnung zu den Baustein-Katalogen näher beschrieben.[64]

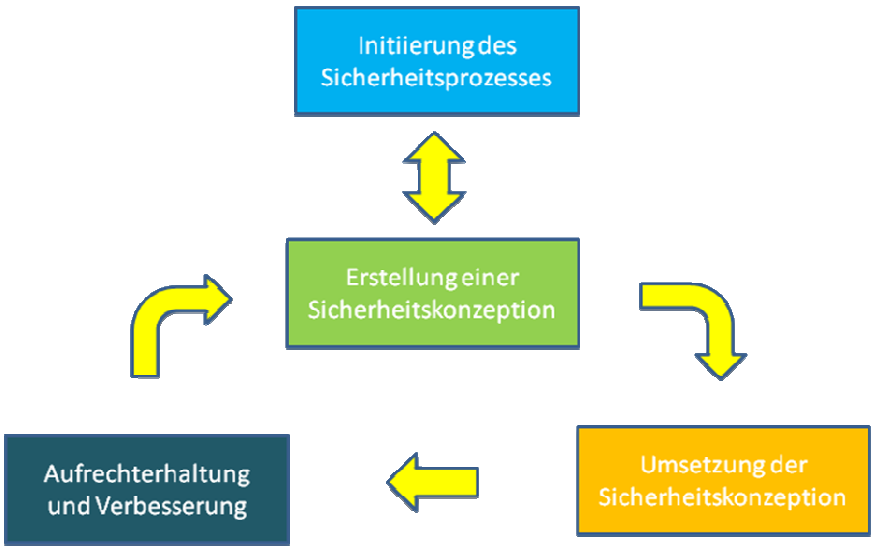
IT-Grundschutz-Vorgehensweise

Nachdem im vorherigen Abschnitt kurz auf die zentralen Dokumente des IT-Grundschutzes eingegangen wurde, werden in diesem Abschnitt die zentralen Punkte der IT-Grundschutz-Vorgehensweise näher beschrieben.

Der erste Schritt bei der Einführung eines ISMS ist die Initiierung des IT-Sicherheitsprozesses. In diesem Schritt werden Sachverhalte wie IT-Sicherheitsorganisation, Leitlinie zur Informationssicherheit, Ressourceneinsatz sowie die Konzeption und Planung des IT-Sicherheitsprozesses näher beschrieben. Die Erstellung einer Sicherheitskonzeption nach IT-Grundschutz ist der zweite Schritt der Vorgehensweise. Hauptaugenmerk dieses Schrittes liegt in der Identifizierung von erforderlichen Sicherheitsmaßnahmen. Im dritten Schritt wird die IT-Sicherheitskonzeption realisiert und die ermittelten nicht- bzw. teilweise realisierten Maßnahmen umgesetzt. Schritt vier befasst sich mit der Thematik der Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit. In diesem Schritt wird das Managementsys-

64 Vgl. BSI-Standard 100-1, S.10f

tem bewertet und ggf. Änderungen beschlossen. Sind Änderungen erforderlich wird mit Schritt zwei fortgesetzt. Ein Kreislauf bildet sich der die Schritte: Erstellung der Sicherheitskonzeption, Umsetzung der Sicherheitskonzeption sowie die Aufrechterhaltung und Verbesserung beinhaltet. Sind die Änderungen mit der Sicherheitskonzeption nicht abzufangen muss eine Neu-Initiierung des Sicherheitsprozesses erfolgen. Die Abb. 3.3 stellt die einzelnen Schritte grafisch dar.



Quelle: In Anlehnung an: BSI-Standard 100-2 S.13

Abb. 3.3: Vorgehensweise IT-Grundschutz

3.4 Weiteres Vorgehen

Das Kapitel drei stellt den grundlegenden Aufbau von Managementsystemen dar und beschreibt wie ein solcher Aufbau sich gestalten sollte. Der ganzheitlichen Sicht auf Informationssicherheit haben sich die Informationssicherheits-Managementsysteme untergeordnet. Sie gewährleisten, dass Sicherheitsziele erfüllt werden, eine feste Zuordnung von Verantwortlichkeiten und die Dokumentation des Informationssicherheitsprozesses erfolgt. Des Weiteren sind die ISO27001 als internationaler Standard sowie der IT-Grundschutz als nationaler Ansatz zur Etablierung eines ISMS vorgestellt worden.

Die Modellierung der IT-Grundschutz-Vorgehensweise zur Einführung und Aufrechterhaltung eines ISMS ist das Ziel dieser Arbeit. Die ISO 27001 als internationaler Standard stellt die Anforderungen an ein ISMS während der IT-Grundschutz den Weg beschreibt; Schritt für Schritt. Um die Anzahl der zu modellierenden Prozesse zu beherrschen ist ein Prozessmodellierungstool notwendig. Dieses Tool wird im folgenden Kapitel näher vorgestellt. Das Referenzmodell soll ermöglichen, bestehende Strukturen in den IT-Sicherheitsprozess einzubinden und zu analysieren welche Verbesserungspoten-

tiale sich ergeben. Aus diesen Schlussfolgerungen wird ersichtlich, welche Schritte auf eine Institution zukommen, wenn sie sich dem Thema Informationssicherheit und dem Aufbau und der Aufrechterhaltung eines ISMS zuwenden.

4 Referenzmodellrahmen

In diesem Kapitel wird der Referenzmodellrahmen, die Phase zwei der Referenzmodellierung, näher betrachtet. Im ersten Abschnitt wird auf das verwendete Rahmenwerk der Modellierung näher eingegangen. Der zweite Abschnitt geht auf die Modellierungskonventionen ein. Er stellt die wesentlichen Modelltypen näher dar und grenzt die Modellvielfalt ein. Die ausgewählten Modelltypen werden im weiteren Verlauf für die Modellierung des Referenzmodells verwendet.

4.1 Architektur integrierter Informationssysteme (ARIS)

Das für die Modellierung eingesetzte Werkzeug ist das ARIS-Toolset. Um das ARIS-Toolset im Ganzen zu verstehen, wird in diesem Abschnitt näher auf den ARIS Hintergrund eingegangen.

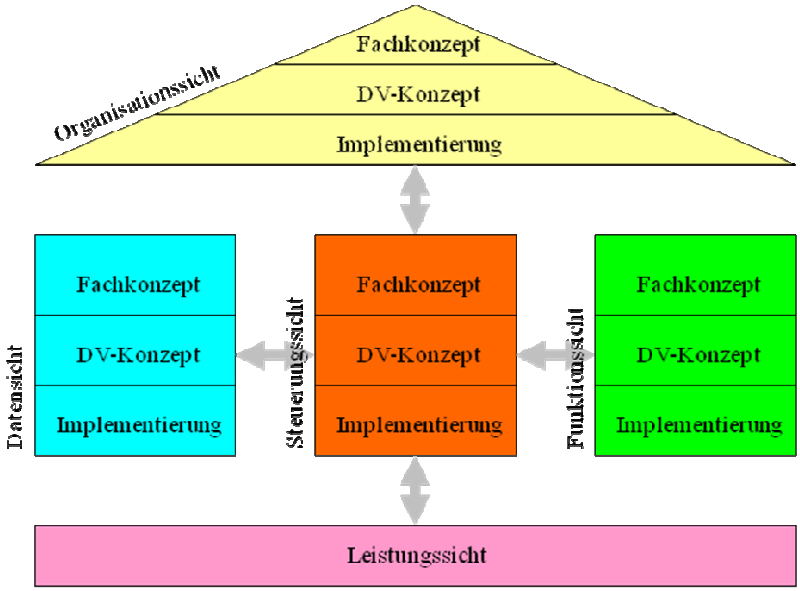
Die Grundideen für das ARIS-Toolset entstanden Anfang der 90er Jahre am vom Prof. August-Wilhelm Scheer geleiteten Institut für Wirtschaftsinformatik an der Universität Saarland. Mit Hilfe der Gründung der IDS Scheer GmbH im Jahre 1992 sollten diese Ideen in ein kommerzielles Softwareprodukt zur Modellierung und Analyse von Geschäftsprozessen fließen. 1993 wurde auf der CeBit das ARIS Toolset Version 1.0 vorgestellt. Die ständige Weiterentwicklung des Tools sowie der Drang nach der effizienteren Gestaltung von Geschäftsprozessen verhalfen dem Werkzeug zum Marktdurchbruch. Wesentlich zum heutigen Erfolg verhalf die Entscheidung der SAP AG das ARIS-Toolset zur Referenzmodellierung seines R/3 Systems zu verwenden.

4.1.1 Konzeption von ARIS

ARIS bedeutet Architektur Integrierter Informationssysteme und repräsentiert ein Rahmenwerk zur Beschreibung von Organisationen und Anwendungssystemen. Das ARIS-Konzept findet Verwendung bei der Modellierung der Aufbau- und Ablaufstruktur einer Organisation. ARIS eignet sich darüber hinaus zur Darstellung von Referenzmodellen. Um die Modellierung zu ermöglichen greift die ARIS-Architektur u.a. auf die folgenden Objekte zurück: Funktionen, Daten, Organisationseinheiten, Ereignisse, Ressourcen und Leistungen.

ARIS ermöglicht es die Objekte und ihre Abhängigkeiten untereinander darzustellen. Es können Beziehungen erzeugt und mittels Modelltypen dargestellt werden. Die ARIS-Architektur unterteilt sich in fünf Sichten. Diese Sichten werden in Organisations-, Da-

ten-, Funktions-, Leistungs- und Steuerungssicht unterteilt und sollen die Komplexität des Modells verringern und die Geschäftsprozessmodellierung einfacher gestalten.



Quelle: In Anlehnung an: Scheer (2002) S.41

Abb. 4.1: ARIS-Haus mit den einzelnen Sichten und Ebenen

Die Sichten im ARIS-Konzept sind:[65]

- Organisationssicht: Die Elemente der Aufbauorganisation werden beschrieben. Elemente sind u.a. Abteilungen, Stellen, Personen. Auf die Beziehungen der Elemente untereinander wird zusätzlich eingegangen. Modelltyp für die Aufbauorganisation ist das Organigramm.

- Funktionssicht: Vorgänge (Funktionen) und deren Zusammenhänge werden beschrieben. Zur Modellierung werden Funktionshierarchiebäume herangezogen.

- Datensicht: Die Datensicht repräsentiert Zustände und Ereignisse des Realitätsausschnitts. Modelliert wird die Datensicht mittels Entity-Relationship-Modellen.

- Leistungssicht: Leistungen werden in ARIS als Ergebnisse von Prozessen bezeichnet. Der Leistungsbegriff umfasst Leistungsarten wie Sach- und Dienstleistungen.

---

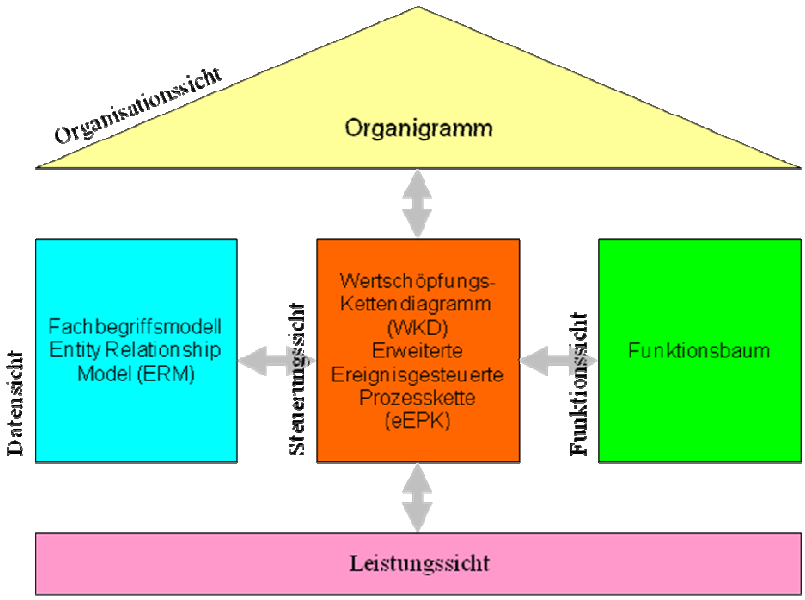
65 Vgl. Hansen/Neumann (2001), S.197f

- Steuerungssicht: Die Steuerungssicht verbindet die oben genannten Sichten und ermöglicht die Verbindung der Sichtenelemente. Erweiterte ereignisgesteuerte Prozessketten dienen als Hilfsmittel zur Beschreibung der Steuerungssicht.

Alle Sichten zusammen bilden das ARIS-Haus, welches in Abb. 4.1 abgebildet ist. Die äußeren Sichten bilden das Grundgerüst. Sie repräsentieren die statischen Sichten wie Organisations-, Daten-, Leistungs- und Funktionssicht. Die Steuerungssicht repräsentiert als Zentrum des Haus, das Zusammenwirken der statischen Sichten in einer dynamischen Umgebung. Die Steuerungssicht integriert die statischen Sichten. Sie repräsentiert die Zusammenhänge aller Objekte miteinander und stellt die wesentliche Sicht des ARIS-Konzepts dar.

Die einzelnen Sichten des ARIS-Hauses werden in drei Beschreibungsebenen unterteilt. Diese Ebenen sind das Fachkonzept, das Datenverarbeitungs-Konzept (DV-Konzept) und die Implementierungsebene.

Das Fachkonzept stellt den Prozess mittels DV-fremden Beschreibungsmodellen strukturiert dar. Aussagen über Informationen, Regeln, Funktionen und grundlegende Verarbeitungsschritte, welche das zukünftige System enthält, werden getroffen. Abhängig von der zugrundeliegenden Sicht werden Modelle wie Entity-Relationship-Model (ERM), erweiterte ereignisgesteuert Prozesskette (eEPK), Organigramm oder Funktionsbaum verwendet. Abb. 4.2 stellt die Modelltypen der fachkonzeptionellen Ebene, innerhalb der einzelnen Sichten des ARIS-Hauses, vor.



Quelle: In Anlehnung an: Landon et al. (2006), S.583

Abb. 4.2: Modelltypen des ARIS-Hauses

Das DV-Konzept repräsentiert die Umsetzung des Fachkonzepts in DV-nahe Beschreibungsmodelle. Abhängig von der jeweiligen Sicht werden Relationen, Struktogramme oder Topologien verwendet. Im Fachkonzept werden die relevanten Rahmenbedingungen beschrieben. Diese werden aber von Softwareentwicklern nur unzureichend verstanden, da das Fachkonzept in der Sprache des Anwendungsgebiets beschrieben ist. Deshalb ist es notwendig die fachlichen Funktionen in DV-Funktionen umzuwandeln. Diese sollten auch ohne das fachliche Spezialwissen verstanden und umgesetzt werden können.

Die Implementierungsebene beschreibt die DV-technische Realisierung der beschriebenen Prozessteile. In Abhängigkeit von der Sicht geschieht das mittels Erstellung von Programmcode, Datenbanksystemen oder Einsatz von Protokollen.[66]

4.1.2 ARIS-Toolset

Das ARIS-Toolset ist ein Softwarewerkzeug der IDS Scheer AG zur Erstellung, Pflege und Optimierung von Geschäftsprozessen. Es basiert auf dem im vorherigen Abschnitt vorgestellten ARIS-Konzept und unterstützt:

- Die Betrachtung von Geschäftsprozessen in den unterschiedliche Bereichen (Organisations-, Funktions-, Daten-, Steuerungs- und Leistungssicht)

  Speziell für die unterschiedlichen Bereiche angepasste Modelltypen ermöglichen diese differenzierte Betrachtungsweise.

- Die Verbindung der Steuerungssicht mit den anderen Sichten (Verbindung der statischen Sichten mit der dynamischen)

  Mit Hilfe der erweiterten ereignisgesteuerten Prozesskette als Modelltyp können Objekte (z.B. Organisationseinheiten) aus den statischen Sichten in die dynamische Sicht übertragen werden.

- Die Daten werden in einer gemeinsamen Datenbank vorgehalten.

  Die ARIS-Datenbank ermöglicht es alle Objekte der Modellierung zentral vorzuhalten.

- Die ganzheitliche Modellierung

---

[66] Rautenstrauch/Schulze (2003), S.228

Modellierung mittels mehrerer Sichten

- Die Konsistenzprüfung der Modelle

  Semantikvergleiche ermöglichen die Konsistenz von Objekten der Modellierung.

- Einen einfachen Überblick über die Modelle

  Das Tool bietet umfangreiche Navigationsmöglichkeiten.

Technische Gesichtspunkte

Beim ARIS-Toolset handelt es sich um ein datenbankbasiertes Modellierungstool. Es ermöglicht die Beschreibung und Analyse von Prozessen. Geschäftsobjekte (Aktivitäten, Personen, IT-Systeme usw.) werden als Knoten und die Verbindungen zwischen ihnen (z.B. „verwendet“) als Kanten innerhalb des Modells abgebildet. Konfigurierbare Attribute können zu Knoten und Kanten gepflegt werden. Diese sind z.B. Objektname und Bearbeitungsdauer. Die Abb. 4.3 stellt ein Abbild der ARIS-Toolset Oberfläche dar.

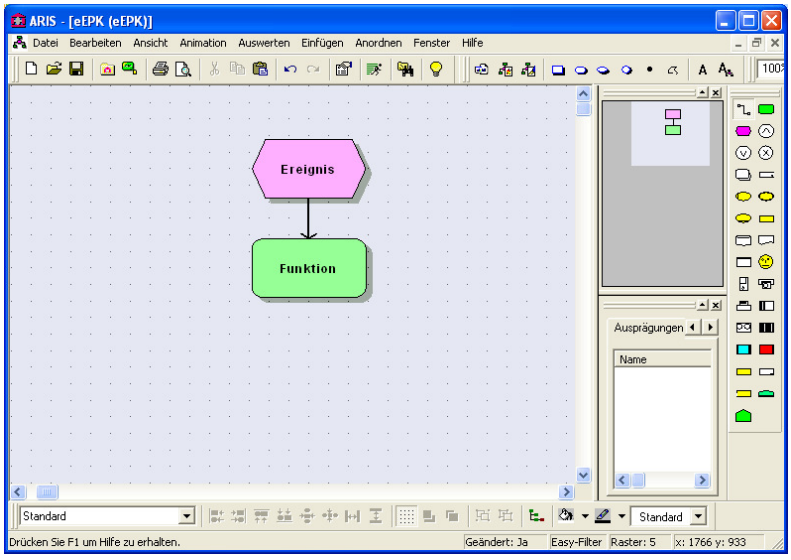


Abb. 4.3: ARIS-Toolset eEPK Modellierung

Komponenten

Die folgenden Komponenten umfasst das ARIS-Toolset:

- Datenbankverwaltung
- Objektverwaltung

- Modelleditor (abgebildet in Abb. 4.3)
- Modellverwaltung
- Benutzerverwaltung
- Modellgenerierung
- Oberflächengestaltung

ARIS-Plattform

Das ARIS-Toolset ist wie alle ARIS-bezogenen Produkte in der ARIS Plattform zusammengeführt. Die ARIS-Plattform umfasst alle ARIS-Produkte für das gesamte Geschäftsprozessmanagement. Dies umfasst von der Strategie über die Implementierung bis hin zum Controlling alle Aspekte.

4.2 Modellierungskonventionen

Die Konventionen der Modellierung lassen sich im ARIS-Toolset mit durch den Methodenfilters umsetzen. Mit dem Methodenfilter können Modelltypen, deren Anwendung und Attribute festgelegt werden. Er ermöglicht die Vielzahl vom ARIS-Toolset zur Verfügung gestellten Modelltypen zu reduzieren und auf die wesentlichen zu beschränken. Die Wahl fiel auf die Modelltypen:

- Wertschöpfungskettendiagramm (WKD)
- Organigramm
- Erweiterte ereignisgesteuerte Prozesskette (eEPK)
- Funktionsbaum

Die einzelnen Modelltypen sowie deren Auswahlbegründung werden im Weiteren beschrieben.

Das Wertschöpfungskettendiagramm

Zur Darstellung von Geschäftsprozessen einer Organisation wird das Wertschöpfungskettendiagramm (WKD) verwendet. Es findet hauptsächlich auf hohem Abstraktionsniveau Anwendung und bietet die Möglichkeit einen Überblick über den Gesamtprozess darzustellen. Detailfragen spielen in diesem Modelltyp eine untergeordnete Rolle. Der Modellersteller muss sich auf die wesentlichen Abläufe fokussieren. Die Kernge-

schäftsprozesse einer Organisation sind zu identifizieren und in chronologischer Abfolge darzustellen. Ein Kerngeschäftsprozess ist ein Vorgang, der direkt an der Wertschöpfung einer Organisation beteiligt ist.

Mittels des Wertschöpfungskettendiagramms ist eine höhere Abstraktionsebene zu realisieren. Sie wird als fachliches Überblicksmodells der Managementsicht auf die Geschäftsprozesse verwendet.

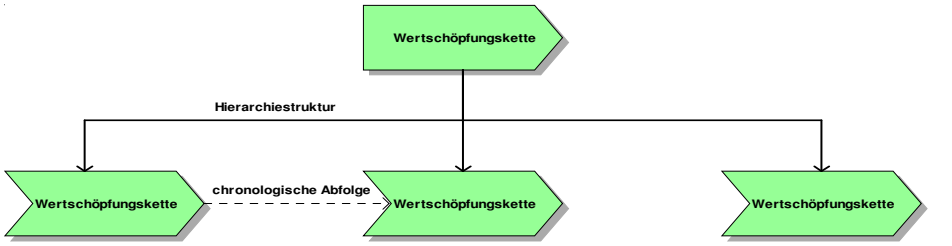


Abb. 4.4: Wertschöpfungskettendiagramm (WKD)

Das WKD nutzt das Wertschöpfungskettensymbol und die Darstellung von Beziehungen mittels Kanten. Diese Kanten können sowohl in gestrichelter als auch in durchgezogener Form genutzt werden. Die Einfachheit des Modelltyps reduziert die Fehlerquote und ermöglicht einen leichten Zugang zu den Inhalten.

Das Organigramm

Mit Hilfe des Organigramms wird die Aufbaustruktur einer Organisation abgebildet. Das Organigramm lässt sich in unterschiedliche Abstraktionsebenen unterteilen. Es wird möglich die übergreifenden Aufbauorganisationen mit lokalen zu kombinieren. Das Organigramm verwendet die Elemente für die Organisationseinheit, der Stelle und der Gruppe. Die Organisationseinheit wird hierbei als Ellipse dargestellt, die auf der linken Hälfte eine durchgezogene Linie aufweist. Das Stellenelement stellt sich als Rechteck dar, welches in der linken Hälfte eine durchgezogene Linie aufzeigt. Die Gruppe spiegelt sich als Ellipse mit einer inneren Ellipse wider. Die Abb. 4.5 stellt die Elemente grafisch dar.

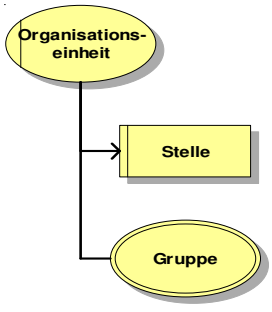


Abb. 4.5: Beispiel-Organigramm

Erweiterte ereignisgesteuerte Prozesskette

Der Modelltyp der erweiterten ereignisgesteuerten Prozesskette (eEPK) findet bei der Modellierung der Ablauforganisation einer Organisation Anwendung. Die eEPK baut auf der ereignisgesteuerten Prozesskette (EPK) auf. Diese stellt Arbeitsprozesse in einer semiformalen Modellierungssprache dar. Betriebliche Vorgänge können analysiert werden um Verbesserungspotentiale aufzudecken. Eine eEPK entsteht wenn eine EPK um die Elemente aus der Organisations-, Daten- und Leistungssicht ergänzt wird. Zusätzliche Informationen wie Verantwortliche, verwendete Dokumente, Informationssysteme usw. lassen sich ergänzen. Die Verbindung der statischen Sichten des ARIS-Hauses mit der dynamischen Sicht wird ermöglicht.

Ein eEPK besitzt die Elemente: Ereignis, Funktion, Prozessschnittstelle, logische Operatoren sowie durchgezogene Kanten zur Verbindung. Zusätzliche Elemente sind u.a. Organisationseinheiten, Fachbegriffe und Dokumente.

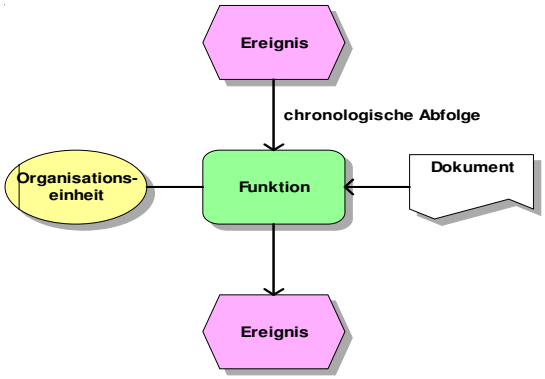


Abb. 4.6: Darstellung eEPK

Funktionen, in denen ein Zwischenprozess innerhalb des Gesamtprozesses dargestellt wird, werden mit einer Hinterlegung gekennzeichnet. (Siehe Abb. 4.7)

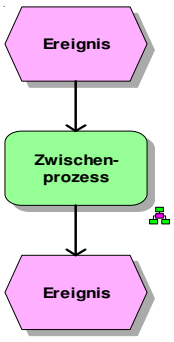


Abb. 4.7: Darstellung Zwischenprozess innerhalb eines eEPKs

Funktionsbaum

Der Funktionsbaum ist ein Modelltyp, welcher die Abhängigkeiten von Funktionen beschreibt. Die Reduzierung der Komplexität von Funktionen wird durch Funktionsbäume realisiert.[67] Übergeordnete Funktionen geben eine höhere Stellung innerhalb des Funktionsbaumes wider. Dieser Sachverhalt ermöglicht es, Problemstellungen bis hin zu ihren Grundfunktionen zu zerlegen. So ist es möglich alle Teilaufgaben eines Prozesses einer übergreifenden Funktion unterzuordnen.

Ein Funktionsbaum besitzt die Elemente: Funktion (dargestellt durch ein abgerundetes Rechteck) sowie durchgezogene Kanten zur Verbindung.

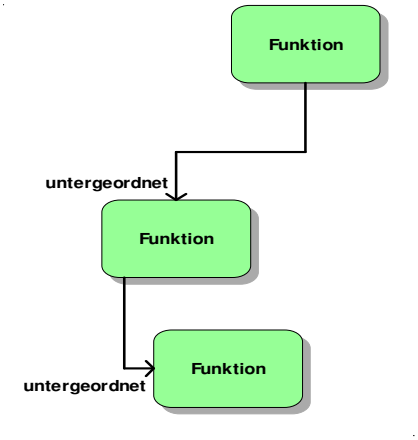


Abb. 4.8: Darstellung Funktionsbaum

Attribute und Gruppenstruktur

Für die Objekte wird das Attribut Name verwendet. Wird das Referenzmodell in eine Organisation angewendet, lassen sich die organisationspezifischen Attribute genauer festlegen.

Die Gruppenstruktur im ARIS-Explorer gibt den Rahmen zur Struktur der Modelle vor.

Ebenen des Modells

Das zu modellierende Referenzmodell wird drei Ebenen enthalten. Die erste Ebene ist das Gesamtmodell. Auf der zweiten Ebene werden die Kapitel des BSI-Standards 100-2 Version 2.0 sowie die Organisationmodelle strukturiert. Ebene drei beschreibt die Sichten des Referenzmodells zu den Kapiteln des Standards.

---

[67] Vgl. Scheer (1997), S.19

Sichten im Referenzmodell

Das Referenzmodell behandelt die Sichten: Arbeitsschritte, Funktionsübersicht und Managementbetrachtung. Diese sind den Kapiteln des BSI-Standards 100-2 Version 2.0 untergeordnet.

Modelldarstellung

Für alle Modelle des Referenzmodells der Arbeit gilt grundsätzlich:

- Anlegen von Modelle erfolgt links oben
- Im Verlauf befinden sich die Modelle am linken Rand der Modellfläche
- Eine Hinterlegung an einem Symbol erfolgt rechts unter dem Symbol an der Kante
- Symbolbezeichnung ist im Symbol zentriert und überschreitet dessen Umfang nicht
- Konstanter Abstand zwischen den Symbolen wird gewährleistet

Für die eEPKs gilt:

- Der gerichtete Graph (Leitpfad) ist mittig angeordnet
- Verzweigungen besitzen den gleichen Abstand zum zentralen Pfad

5 Referenzstruktur und Komplettierung

In diesem Kapitel wird die Referenzmodellierung des BSI-Standards 100-2 Version 2.0 nach dem Vorgehensmodell behandelt. Das Kapitel reiht sich in die Vorgehensweise der Referenzmodellierung in den Phasen drei „der Konstruktion des Referenzmodellstruktur“ und Phase vier „der Komplettierung“ ein. Im ersten Abschnitt des Kapitels wird die IT-Grundschutz-Vorgehensweise näher beschrieben. Auf die einzelnen Phasen des Sicherheitsprozesses wird näher eingegangen. Im Anschluss wird das Referenzmodell anhand von ausgewählten Prozessmodellen näher vorgestellt. Der dritte Teil des Kapitels wird sich mit der Verbindung der IT-Grundschutz-Vorgehensweise und der ISO 27001 auseinandersetzen. Ziel ist es aufzuzeigen wie die IT-Grundschutz-Vorgehensweise die Anforderungen der ISO 27001:2005 erfüllt.

5.1 Inhaltliche Beschreibung des BSI-Standards 100-2 Version 2.0

Der BSI-Standard 100-2 Version 2.0 beschreibt detailliert die IT-Grundschutz-Vorgehensweise. Der Standard unterteilt sich in die grundlegenden Phasen des Vorgehensmodells des Sicherheitsprozesses nach IT-Grundschutz. Diese spiegeln sich in den Kapitelüberschriften wider. Die in diesem Abschnitt dargestellten Kapitelnummern beziehen sich vollständig auf die Kapitelnummern des BSI-Standards 100-2 „IT-Grundschutz-Vorgehensweise“.

Der Standard beginnt mit einem Einleitungskapitel. In diesem Kapitel wird auf Versionsänderungen, Zielsetzung, Adressatenkreis sowie auf die Anwendungsweise des Standards näher eingegangen. Ziel ist es den Anwender in die IT-Grundschutz-Thematik einzuführen und den Aufbau und die Einordnung des Standards in das Standardwerk des BSI zu vermitteln.

Kapitel zwei widmet sich dem Informationssicherheits-Management mittels IT-Grundschutz. Das Kapitel geht auf den Informationssicherheitsprozess sowie die Anwendung der IT-Grundschutz-Kataloge ein. Des Weiteren erfolgt eine thematische Abgrenzung, welche die Begrifflichkeiten im Zusammenhang mit Informationssicherheit näher beschreibt. Im Rahmen der Übersicht über den Informationssicherheitsprozess wird auf die einzelnen Phasen des Sicherheitsprozesses näher eingegangen. Die Phasen untergliedern sich in: „Initiierung des Sicherheitsprozesses“, „Erstellung einer Sicher-

heitskonzeption“, „Umsetzung der Sicherheitskonzeption“ und „Aufrechterhaltung und Verbesserung“. Abb. 3.3 spiegelt den Zusammenhang der Phasen wider.[68]

Initiierung des Sicherheitsprozesses

Der Phase „Initiierung des Sicherheitsprozesses“ widmet sich das dritte Kapitel des Standards. Das Kapitel beschreibt wie ein Sicherheitsmanagement aufgebaut und weiterentwickelt werden kann und gibt Einblick auf die mögliche organisatorische Ausgestaltung. Kapitel drei gliedert sich in die Unterkapitel:[69]

- Das Kapitel 3.1 „Übernahme von Verantwortung durch die Leitungsebene“ dient zur Aufklärung der Leitungseben über mögliche Folgen aus einem Mangel an Informationssicherheit. Die Gesamtverantwortung der Leitungsebene im Inforationssicherheitsprozess ist von der Leitungsebene zu übernehmen und der IT-Sicherheitsprozess von ihr zu initiieren. Die Stellungnahme der Leitungsebene zur Informationssicherheit ist Kerngedanke des Kapitels.

- Auf die „Konzeption und Planung des Sicherheitsprozesses“ geht Kapitel 3.2 näher ein. Das Kapitel widmet sich der Etablierung eines kontinuierlichen Informationssicherheitsprozesses, der Festlegung einer Strategie für Informationssicherheit, der Festlegung allgemeiner Sicherheitsziele sowie der Ressourcenbereitstellung für den IT-Sicherheitsprozess. Folgende Teilschritte sind zu beachten: Ermittlung der internen und externen Rahmenbedingungen für die wesentlichen Geschäftsprozesse, Formulierung der allgemeingültigen Informationssicherheitsziele aus den ermittelten Rahmenbedingungen, Einordnung des Sicherheitsniveaus für Geschäftsprozesse bzw. Bereiche der Institution hinsichtlich der Grundwerte: Vertraulichkeit, Integrität und Verfügbarkeit als richtungsweisende Aussage für spätere Phasen.

- Kapitel 3.3 beschreibt die Erstellung einer Leitlinie zur Informationssicherheit. Sie enthält die wesentlichen Aussagen zum Thema Informationssicherheit. Betrachtet werden die Aufgaben: Stellungnahme der Institutionsleitung zum Thema Informationssicherheit und zur Erreichung der Informationssicherheitsziele, abgrenzen und festlegen des Geltungsbereichs und des Inhaltes der Leitlinie, Aufstellung einer Entwicklungsgruppe zur Ausarbeitung der Leitlinie, institutionsweite Einführung der Leitlinie sowie die regelmäßige Überprüfung der Leitlinie.

---

68 Vgl. BSI-Standard 100-2, S.10-15
69 Vgl. BSI-Standard 100-2, S.16-35

- Die Organisation des Sicherheitsprozesses wird in Kapitel 3.4 näher beschrieben. Auf die Etablierung der Informationssicherheitsorganisation wird näher eingegangen. Die folgenden Aufgaben sind werden beschrieben: Sicherstellung der Integration der Informationssicherheit in allen Abläufen und Prozessen der Institution, Aufbau einer Informationssicherheitsorganisation, Zuteilung der Aufgaben-, Verantwortungs- und Kompetenzbereiche der IS-Organisation sowie Rollenverteilung und -anforderungen in der IS-Organisation.

- Kapitel 3.5 setzt sich mit der Bereitstellung von Ressourcen für die Informationssicherheit auseinander. Der Aufwand für die Informationssicherheit ist mit dem angestrebten Sicherheitsniveau in Einklang zu bringen. Das Kapitel legt die folgenden Aufgabengebiete fest: Abwägen von Wirtschaftlichkeitsaspekten sowie des Ressourceneinsatzes und dem angestrebten Sicherheitsniveau, Bereitstellung von Ressourcen zur Aufgabenerfüllung der IS-Organisation, Einplanung von Ressourcen zur Überwachung der Informationssicherheit sowie die Sicherstellung von Ressourcen für den IT-Betrieb.

- Die Einbindung aller Mitarbeiter in den Sicherheitsprozess wird in Kapitel 3.6 näher vorgestellt. Folgende Aufgabenbereiche sind zu betrachten: Planung von Schulungs- und Sensibilisierungsmaßnahmen, Festlegung der Ansprechpartner zu Sicherheitsfragen sowie die Betrachtung des Mitarbeiteraustritts bzw. eines Aufgabenwechsels, hinsichtlich der Wahrung der Informationssicherheit

Erstellung einer Sicherheitskonzeption

Mit Abschluss des dritten Kapitels ist die Initiierungsphase beendet und Kapitel vier „Erstellung einer Sicherheitskonzeption nach IT-Grundschutz“ schließt sich an. Um eine Sicherheitskonzeption zu erstellen, sind eine Reihe von Schritten notwendig. Diese Schritte gliedern sich in die folgenden Unterkapitel, die im Einzelnen vorgestellt werden: [70]

- Kapitel 4.1 widmet sich der „Definition des Geltungsbereichs“. Dieser Informationsverbund beschreibt den Anwendungsbereich der Sicherheitskonzeption. Die Größe des Informationsverbundes kann von einem einfachen Geschäftsprozess bis hin zur gesamten Institution reichen.

- Im Anschluss an die Definition des Geltungsbereichs schließt sich die Strukturanalyse in Kapitel 4.2 an. Für die Anwendung der IT-Grundschutz-Kataloge ist

[70] Vgl. BSI-Standard 100-2, S.36-75

es notwendig, dass Zusammenwirken von Geschäftsprozessen, Anwendungen und Informationstechnik zu analysieren und zu dokumentieren. Die Strukturanalyse unterteilt sich in die Aufgaben: Reduzierung der Komplexität durch geeignete Gruppenbildung gleichartiger Objekte, Erfassung der Anwendungen, Erhebung eines Netzplans, Erhebung der IT-Systeme sowie die Erfassung der Räume.

- Kapitel 4.3 beschreibt die Schutzbedarfsfeststellung. Jedem erfassten Objekt aus der Strukturanalyse ist der Schutzbedarf bzgl. Vertraulichkeit, Verfügbarkeit und Integrität zu zuordnen. Die folgenden Aufgaben sind zu betrachten: Festlegung der Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ , mittels vordefinierter Schadenszenarien, Feststellung des Schutzbedarfs für die IT-Anwendungen, Feststellung des Schutzbedarfs für IT-Systeme, Feststellung des Schutzbedarfs für Räume, Feststellung des Schutzbedarfs für Kommunikationsverbindungen sowie die Sichtung der Ergebnisse der vorherigen Schutzbedarfsfeststellungen.

- Im Anschluss an die Schutzbedarfsfeststellung schließt sich mit Kapitel 4.4 die „Auswahl und Anpassung von Maßnahmen“ an. Ziel dieses Kapitels ist es den Informationsverbund mittels der vorhandenen Bausteine des IT-Grundschutz-Katalogs nachzubilden. Das Kapitel unterteilt sich in: Vorstellung der IT-Grundschutz-Kataloge, Beschreibung der Modellierung des IT-Verbundes, mittels der Zuordnung der IT-Grundschutz-Bausteine zu den Zielobjekten sowie die Prüfung der Maßnahmen hinsichtlich Wirksamkeit, Eignung, Praktikabilität, Akzeptanz und Wirtschaftlichkeit, gegebenenfalls sind Maßnahmenanpassungen vorzunehmen.

- Der „Basis-Sicherheitscheck“ in Kapitel 4.5 schließt sich nach der „Auswahl und Anpassung der Maßnahmen“ an. Die im vorherigen Schritt durchgeführte Modellierung des IT-Verbundes wird als Prüfplan zur Durchführung eines Soll-Ist-Vergleichs verwendet. Ergebnis des Soll-Ist-Vergleichs ist der Umsetzungsgrad der Maßnahmen aus den zugeordneten IT-Grundschutz-Bausteinen. Die folgenden Arbeitsschritte werden betrachtet: Vorarbeiten zur Durchführung des Basis-Sicherheitschecks, Durchführung des Soll-Ist-Vergleichs sowie die Dokumentation der Ergebnisse.

- Die „Ergänzende Sicherheitsanalyse“ im Kapitel 4.6 schließt sich an den Basis-Sicherheitscheck an. In diesem Schritt werden die Objekte betrachtet, die nicht mit Standard-Sicherheitsmaßnahmen des IT-Grundschutz-Katalogs abgedeckt werden können. Die Aufgaben, die sich bei der ergänzenden Sicherheitsanalyse

ergeben, sind: Festlegung des Zeitpunktes für die Risikoanalyse, Festlegung der relevanten Objekte für die ergänzende Sicherheitsanalyse sowie die Durchführung der Risikoanalyse.

Umsetzung der Sicherheitskonzeption

Mit der ergänzenden Sicherheitsanalyse endet die Erstellung der Sicherheitskonzeption und die Umsetzung der Sicherheitskonzeption beginnt. Diese Phase wird in Kapitel fünf näher beschrieben und gliedert sich in die folgenden Kapitel:[71]

- Die Sichtung der Untersuchungsergebnisse ist der erste Schritt bei der Umsetzung der Sicherheitskonzeption. Dieser Schritt wird in Kapitel 5.1 näher untersucht. Die Ergebnisse des Basis-Sicherheitschecks und der eventuell schon durchgeführten Risikoanalyse sind aufzubereiten.

- Das Kapitel 5.2 „Konsolidierung der Maßnahmen“ beschreibt wie zusätzliche Sicherheitsmaßnahmen aus der Risikoanalyse die Maßnahmen des IT-Grundschutz-Katalogs ergänzen bzw. ersetzen.

- Auf die „Kosten und Aufwandsschätzung“ geht Kapitel 5.3 näher ein. Die Wirtschaftlichkeit sowie der Ressourceneinsatz, der noch umzusetzenden Maßnahmen, spielen eine zentrale Rolle.

- Liegen die finanziellen und personellen Ressourcen zur sofortigen Umsetzung der Maßnahmen nicht vor, gibt Kapitel 5.4 „Festlegung der Umsetzungsreihenfolge der Maßnahmen“ Hinweise wie man auf diesen Zustand zu reagieren hat.

- Nachdem die Umsetzungsreihenfolge festgelegt ist, werden die Aufgaben und Verantwortungen den verantwortlichen Personen für die Maßnahmenumsetzung zugeordnet. Kapitel 5.5 spiegelt die Informationen wider, die dabei erfasst werden.

- Auf realisierungsbegleitende Maßnahmen, die während der Umsetzung von Maßnahmen ergriffen werden sollen, geht Kapitel 5.6 näher ein.

---

[71] Vgl. BSI-Standard 100-2, S.76-81

Aufrechterhaltung und kontinuierliche Verbesserung

Kapitel sechs des Standards richtet sich an die „Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit“. Ziel ist es den Informationssicherheitsprozess sowie die Informationsflüsse im Sicherheitsprozess zu dokumentieren, zu überwachen und zu verbessern.[72]

- Der „Überprüfung des Informationssicherheitsprozesses in allen Ebenen“ widmet sich Kapitel 6.1. Die Praxistauglichkeit von Strategie, Maßnahmen und organisatorischen Abläufen sind zu untersuchen. Die einzelnen Teilbereiche der Überprüfung sind: Festlegung von Verfahren und Prozessen zur Überprüfung des Informationssicherheitsprozesses, Überprüfung der Einhaltung und Umsetzung von Sicherheitsmaßnahmen, Prüfung der Informationssicherheitsstrategie hinsichtlich der Aktualität der Sicherheitsziele, der Rahmenbedingungen, der Wirtschaftlichkeit und der Sicherheitskonzeption sowie die Auswertung von Prüfungsergebnissen.

- Der Aufbereitung von Informationen, die während des Informationssicherheitsprozesses entstehen, widmet sich Kapitel 6.2 „Informationsfluss im Informationssicherheitsprozess“. Folgende Teilbereiche sind zu betrachten: Anfertigung von Berichten an die Institutionsleitung, Bereitstellung von Dokumentation im Informationssicherheitsprozess wie technische Dokumente, Mitarbeiteranleitungen usw. und die Dokumentation des Informationsflusses und der Meldewege.

Im Kapitel 7 des Standards werden die Zertifizierungsaspekte und die Anforderungen bei der Zertifizierung aufgezeigt. Die Vorteile einer Zertifizierung werden hervorgehoben.[73]

Der Standard verfügt zusätzlich über einen Anhang, der Hilfestellung für das Kapitel 4.3.1 „Definition der Schutzbedarfskategorien“ gibt. Die Schadenszenarien werden mit Fragestellungen unterlegt, welche die Schutzbedarfsfeststellung der Anwendungen erleichtert.[74]

---

72 Vgl. BSI-Standard 100-2, S.82-87
73 Vgl. BSI-Standard 100-2, S.88f
74 Vgl. BSI-Standard 100-2, S.90-95

5.2 Das Referenzmodell

Das Referenzmodell, welches auf die inhaltliche Beschreibung des BSI-Standards 100-2 Version 2.0 „IT-Grundschutz-Vorgehensweise“ zurückgreift, wird in diesem Kapitel vorgestellt. Der erste Abschnitt dieses Kapitels widmet sich der Struktur des Referenzmodells. Die Phase „Erstellung einer Sicherheitskonzeption“ der IT-Grundschutz-Vorgehensweise wird im zweiten Abschnitt dieses Kapitels beschrieben und anhand von ausgewählten Modellen vorgestellt. Das vollständige Referenzmodell ist dem Anhang der Arbeit zu entnehmen.

Struktur des Referenzmodells

Das erstellte Referenzmodell gliedert sich in seiner Struktur an die des BSI-Standards 100-2 „Vorgehensweise des IT-Grundschutzes“ an. Kapitelnummerierungen und die Kapitelüberschriften des Standards werden für die Beschriftung der Modelle sowie der Gruppenstruktur verwendet. So lautet beispielsweise Kapitel 3 des Standards „Initiierung des Sicherheitsprozesses“. Der Modellordner welches für die Modellierung des dritten Kapitels angelegt wurde, heißt demzufolge „3 Initiierung des Sicherheitsprozesses“. Alle Teilkapitel, die sich dem dritten Kapitel unterordnen, sind als Modelle in diesem Ordner wiederzufinden. Alle Unterkapitel sind in gleicher Weise aufgebaut wie die Hauptkapitel. Sie sind an die Kapitelnummerierungen und Überschriften des Standards angelehnt. Der einzige Ordner, der von der Nummerierung abweicht ist der Ordner für die Organisationsmodelle. Er hat als Nummerierung die Null bekommen und beinhaltet Beispiel-Organigramme für eine kleine, mittelgroße und große Organisation. Eingeleitet wird das Referenzmodell vom Modell „Der IT-Sicherheitsprozess“. Es stellt den Ausgangspunkt für das Referenzmodell dar. Über dieses Modell sind alle Gruppenmodelle verknüpft. So wird sichergestellt, dass es einen Ausgangspunkt für die Betrachtung gibt und ein schneller Einstieg ermöglicht wird. Jeder Gruppenordner, mit Ausnahme „0 Organisationsmodelle“ verfügt über drei Unterordner. Diese werden als „Arbeitsschritte“, „Funktionsübersicht“ und „Managementbetrachtung“ bezeichnet. Die verwendeten Modelltypen sind in diesen drei Unterordnern wiederzufinden. Alle erweiterten ereignisgesteuerten Prozessketten befinden sich im Unterordner „Arbeitsschritte“. Der Name des Orders wurde gewählt, da sich dort explizite Aufgabenbeschreibungen zum IT-Sicherheitsprozess befinden. Der zweite Unterordner „Funktionsübersicht“ beinhaltet den Funktionsbaum des Kapitels. In ihm werden alle Funktionen der Arbeitsschritte zusammengeführt und in Modellen veranschaulicht. Im dritten Unterordner „Managementbetrachtung“ werden die Wertschöpfungskettendiagramme eingeordnet. Sie sind übergreifende Prozessablaufketten deren Hinterlegungen auf die eEPKs des Unterordners „Arbeitsschritte“ verweisen. Die Bezeichnung „Managementbetrachtung“ verdeut-

licht, dass es sich hierbei um übergeordnete Ablaufmodelle handelt, die den Prozessweg auf einer höheren Ebene beschreiben. Die Abb. 5.1 verdeutlicht die Struktur des Referenzmodells und veranschaulicht die zuvor angesprochenen Aspekte.

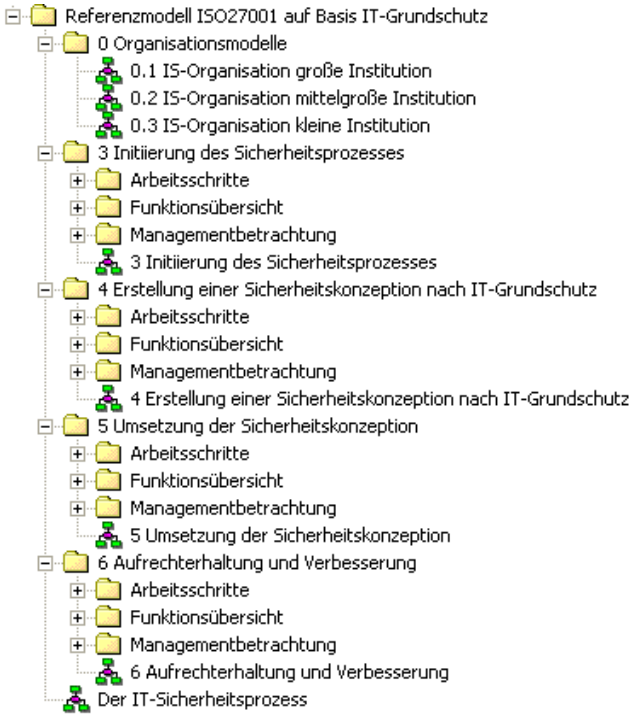


Abb. 5.1: Struktur des Referenzmodells

Wie bereits bei der Ordnerstruktur angesprochen ist das Modell des IT-Sicherheitsprozesses keinem Unterordner zugewiesen. Das Modell trägt die Bezeichnung „Der IT-Sicherheitsprozess“. Es ist dem Modell der IT-Grundschutz-Vorgehensweise nachempfunden und wird als Ausgangspunkt für alle weiteren Modelle verwendet. Bei dem Modell handelt es sich um ein Wertschöpfungskettendiagramm mit vier Modellelementen. Der Zyklus der Vorgehensweise ist durch die Kantenführung nachgestellt. So wird verdeutlicht, wie die vier Phasen des Informationssicherheitsprozesses nach IT-Grundschutz zusammenwirken. Jede Phase ist dem Kapitel des BSI-Standards 100-2 „Vorgehensweise nach IT-Grundschutz“ mit Kapitelnummer und Kapitelbezeichnung nachempfunden. Zu den einzelnen Phasen liegen Hinterlegungen vor, die zu den Wertschöpfungskettendiagrammen der einzelnen Phasen führen. Zu erkennen sind die Hinterlegungen an dem verkleinerten Symbol eines EPKs unterhalb eines jeden Phasenelements. Abb. 5.2 stellt die zuvor aufgeführten Aussagen grafisch dar und veranschaulicht das Ausgangsmodell des Referenzmodells.

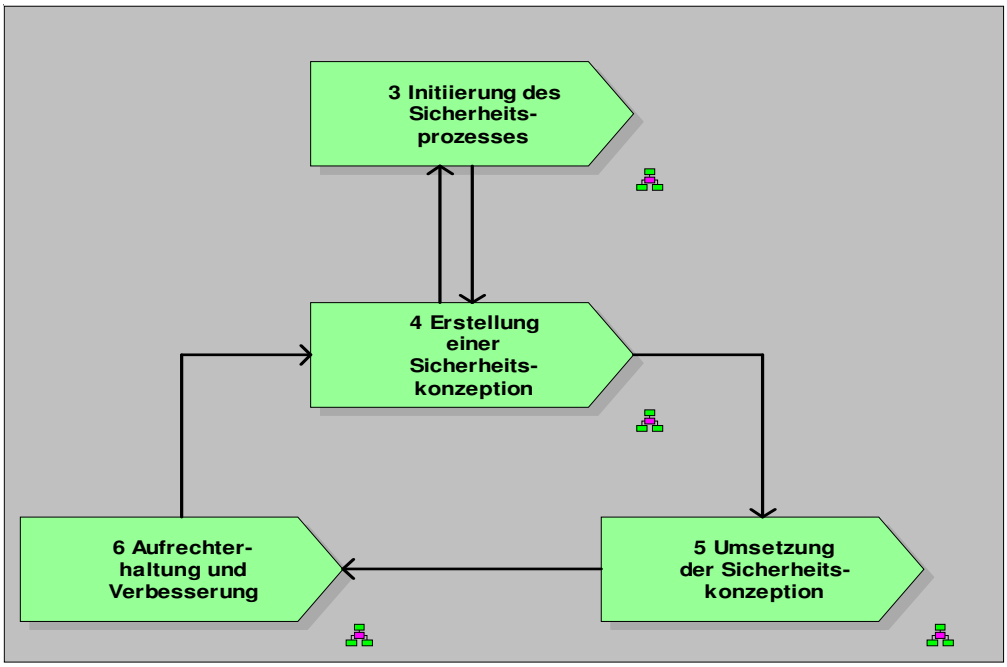


Abb. 5.2: IT-Sicherheitsprozess nach IT-Grundschutz-Vorgehensweise

Vorstellung des Referenzmodells

Das Referenzmodell wird anhand der zweiten Phase „Erstellung einer IT-Sicherheitskonzeption“ der IT-Grundschutz-Vorgehensweise vorgestellt. Die erstellten Modelle und verwendeten Modelltypen werden beschrieben und dargestellt. Zuvor wird kurz auf eines der Beispiel-Organisationsdiagramme eingegangen. Das Organigramm, welches hier vorgestellt wird, stellt die Aufbauorganisation einer mittelgroßen Institution dar. Die Institutionsleitung wird als oberste Instanz dargestellt. Ihr untergeordnet ist die IT-Sicherheitsorganisation. Die Stelle des IT-Sicherheitsbeauftragten wird der IT-Sicherheitsorganisation zugeordnet. Da es sich um eine mittelgroße Institution handelt wird zusätzlich zu der eben beschriebenen „Gesamtorganisationebene“ die „System-/Projektebene“ geschaffen. Bei dieser Institutionsgröße wird zusätzlich eine IT-Sicherheitsorganisation auf System- und Projektebene aufgebaut, diese wiederrum weist eine Stelle des System/Projekt-IT-Sicherheitsbeauftragten auf, die der IT-Sicherheitsorganisation auf der Gesamtorganisationseben unterstellt ist. In mittelgroßen Organisationen müssen Maßnahmen für Informationssicherheit mit den Vertretern der IT-Anwendungen, mittels eines IT-Koordinationsausschusses, abgesprochen werden. Diesem sitzt zudem die Institutionsleitung als höchste Instanz vor. Die Abb. 5.3 soll die oben genannten Sachverhalte näher verdeutlichen.

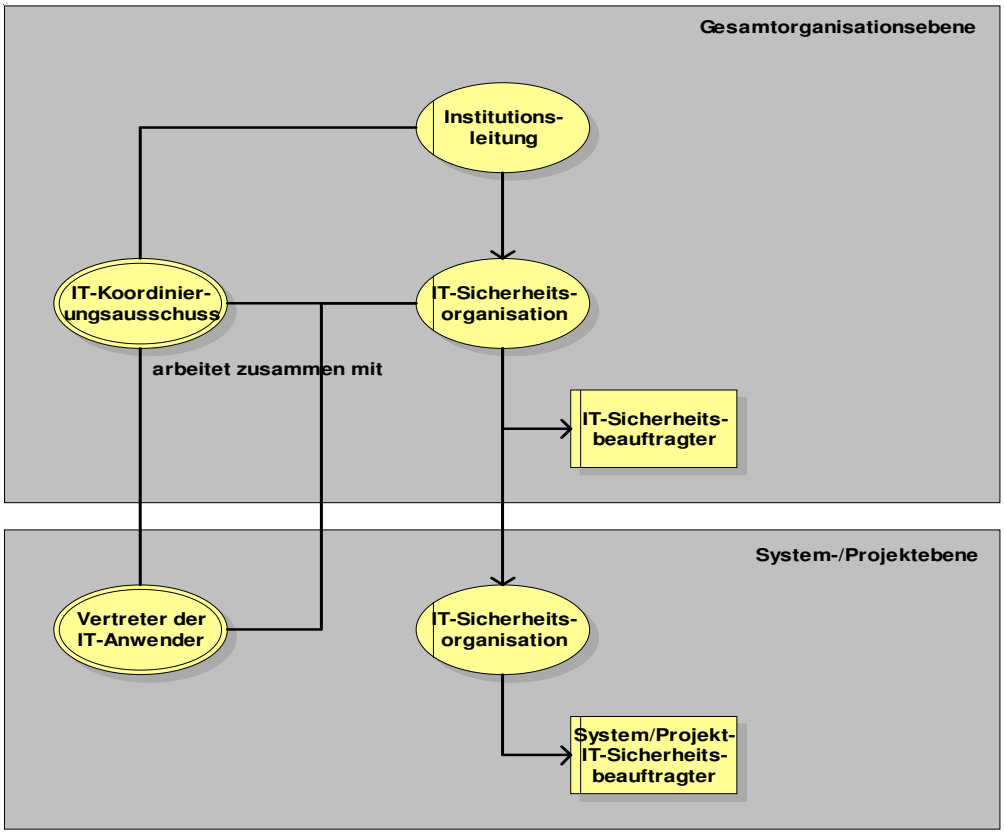


Abb. 5.3: Organigramm mittelgroße Organisation

Über das Modell „Der IT-Sicherheitsprozess“, welches in Abb. 5.2 näher vorgestellt wurde gelangt man in das Wertschöpfungskettendiagramm „4 Erstellung einer IT-Sicherheitskonzeption“. In diesem werden die einzelnen Phasen zu Erstellung einer Sicherheitskonzeption dargestellt. Ausgangspunkt ist die Phase „Definition des Geltungsbereichs“. Weitere Phasen sind die Strukturanalyse, die Schutzbedarfsfeststellung, die Auswahl und Anpassung der Maßnahmen, der Basis-Sicherheitscheck sowie als abschließende Phase die ergänzende Sicherheitsanalyse. Die Kanten zwischen den einzelnen Phasen stellen den zeitlichen Ablauf der Phasen dar. Das Vorgängerobjekt wird zur Voraussetzung des Nachfolgerobjektes. Ohne die „Definition des Geltungsbereichs“ erfolgt keine Strukturanalyse, da die Definition des Geltungsbereiches Grundvoraussetzung für die Strukturanalyse ist. Die Abb. 5.4 stellt das im Vorfeld angesprochene Modell grafisch dar. Die einzelnen Phasen des WKD „4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz“ sind mit Hinterlegungen versehen. Diese Hinterlegungen führen zu eEPKs oder zu weiterführenden WKDs.

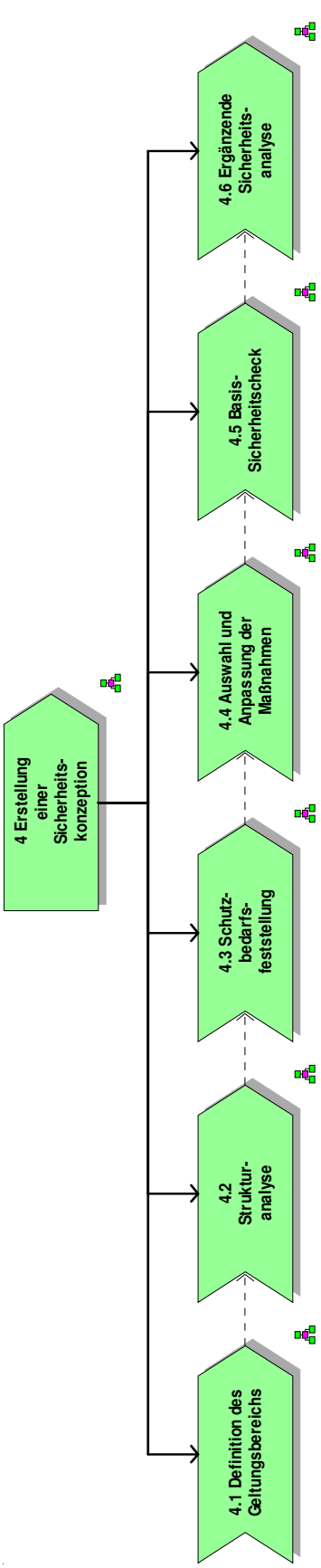


Abb. 5.4: WKD: 4 Erstellung einer Sicherheitskonzeption

Der erste Schritt zur Erstellung einer Sicherheitskonzeption ist die Definition des Geltungsbereiches. Dieses Objekt ist mit einer eEPK hinterlegt, die im Folgenden beschrieben wird. Das Modell „4.1 Definition des Geltungsbereichs“ legt den Bereich fest für den später die Sicherheitskonzeption angewendet wird. Er ist Ausgangspunkt für die gesamte Erstellung der Sicherheitskonzeption. Folgende Aufgaben ergaben sich aus der Analyse des Standards. Zuerst sind die kritischen Geschäftsprozesse zu betrachten. Diese sind dem Dokument „Rahmenbedingungen“ zu entnehmen, welches in der Initiierungsphase des IT-Sicherheitsprozesses erstellt wurde. Der Geltungsbereich beinhaltet die kritischen Geschäftsprozesse, eine Vorbetrachtung ist deshalb notwendig. Nach der Untersuchung der kritischen Geschäftsprozesse sind die Teile der Institution, die sich im Geltungsbereich befinden werden, festzuhalten. Im Folgeschritt wird die Abgrenzung des Geltungsbereiches vorgenommen. Der Schritt vermeidet eine spätere Überarbeitung der Konzeption aufgrund von Unklarheiten. Auf die Einbeziehung von externen Schnittstellen geht Schritt vier des Modells ein. Die externen Schnittstellen sind in den Geltungsbereich mit einzubeziehen. Schnittstellen sind bspw. ausgelagerte Prozesse oder IT-Systeme sowie Abhängigkeiten von und zu Dritten. Sind diese vier Schritte abgearbeitet, so liegen alle Informationen für den Geltungsbereich vor und dieser kann dokumentiert werden. Im Anschluss an die Definition des Geltungsbereichs schließt sich die Strukturanalyse an. Dieser Sachverhalt wird mittels des Symbols für eine Prozessschnittstelle verdeutlicht und weißt daraufhin hin, dass ohne die Definition des Geltungsbereichs die Strukturanalyse nicht durchgeführt werden kann. Der ganze Prozess der Definition des Geltungsbereichs wird von der IT-Sicherheitsorganisation, welche durch das Organigramm-Symbol mit der gleichnamigen Bezeichnung „IT-Sicherheitsorganisation“ gekennzeichnet ist, durchgeführt. Zum besseren Verständnis ist das Modell in Abb. 5.5 näher einzusehen.

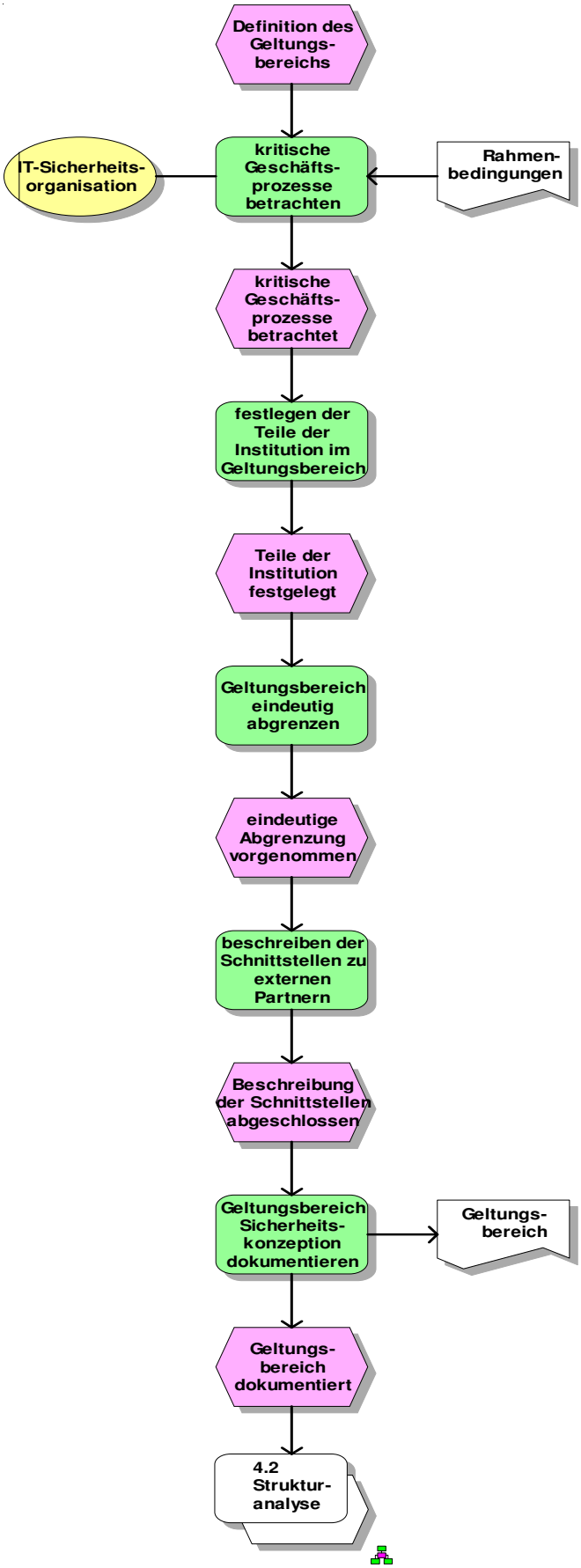


Abb. 5.5: eEPK: 4.1 Definition des Geltungsbereichs

Sie dient als Informationssammlung für alle später anzuwenden Schritte, da sie die Zielobjekte für die Informationssicherheit erhebt. Zu diesen Zielobjekten müssen später Maßnahmen definiert werden, die die Informationssicherheit sicherstellen. Im Anschluss an die Strukturanalyse folgt die Schutzbedarfsfeststellung, welche den Schutzbedarf zu den vorher aufgestellten Zielobjekten erhebt. Das Modell gibt die sechs Teilschritte in die die Schutzbedarfsfeststellung unterteilt wird wider. Erster Schritt ist die Ermittlung der Schutzbedarfskategorien. Diese Kategorien legen fest, welche Schadenshöhen eintreten können, wenn es zu einem Verlust in den Grundwerten: Vertraulichkeit, Verfügbarkeit und Integrität kommt. Im Anschluss erfolgt anhand dieser Kategorien die Schutzbedarfsfeststellung der Anwendungen. Ist der Schutzbedarf der Anwendungen definiert, so lässt er sich auf die IT-Systeme übertragen, auf denen diese Anwendungen zur Geltung kommen. Es schließt sich die Schutzbedarfsfeststellung der Räume an. Der Schutzbedarf eines jeden Raums wird abgeleitet von den im Raum befindlichen IT-Systemen. Im Anschluss erfolgt die Schutzbedarfsfeststellung der Kommunikationsverbindungen. Außenverbindungen, zugelassene und nicht zugelassene Kommunikationsverbindungen sind hinsichtlich der drei Grundwerte zu untersuchen. In der letzten Phase der Schutzbedarfsfeststellung werden die Ergebnisse aus den vorherigen Betrachtungen näher untersucht. Alle Objekte, die einen erhöhten Sicherheitsbedarf in mindestens einem der drei Grundwerte aufweisen, sind für die ergänzende Sicherheitsanalyse vorzumerken. Des Weiteren sind Überlegungen zu treffen, ob diese Objekt in Sicherheitszonen zusammengeführt werden können. Diese Sicherheitszonen mit Zielobjekten höheren Schutzbedarfs lassen sich räumlich, technisch oder personell zentrieren und mit Maßnahmen absichern. Ziel dieser Sicherheitszonen ist es Risiken und Kosten zu begrenzen. Die Abb. 5.6 stellt das Modell grafisch dar.

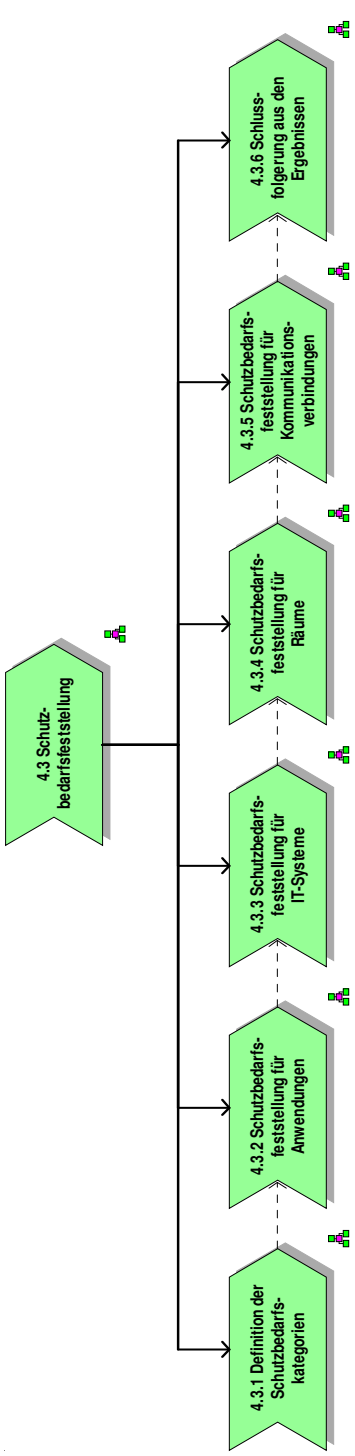


Abb. 5.6: WKD: 4.3 Schutzbedarfsfeststellung

Im Anschluss an das WKD für die Schutzbedarfsfeststellung wird das Modell für die erste Phase der Schutzbedarfsfeststellung “Definition der Schutzbedarfskategorien“ näher vorgestellt. Nachdem die Strukturanalyse abgeschlossen ist, müssen die IT-Sicherheitsorganisation und die Institutionsleitung die Schadenszenarien festlegen. Diese Schadenszenarien sind dem Anhang des BSI-Standards 100-2 zu entnehmen. Zu jedem Schadenszenario wird die Schadenshöhe festgelegt. Zwischen normaler, hoher und

sehr hoher Schadenshöhe ist zu unterscheiden. Diese drei Tätigkeiten können simultan zu jedem Schadenszenario durchgeführt werden und werden durch drei parallel angeordnete Funktionen, die mit einem UND-Operator verknüpft sind, dargestellt. Die Ergebnisse der Schadenshöhen sind zu dokumentieren. Die drei Schadenskategorien normal, hoch und sehr hoch werden in diesem Schritt festgelegt. In ihnen finden sich die Schadenszenarien mit den festgelegten Schadenshöhen wieder. Schadenskategorie Normal spiegelt alle festgelegten normalen Schadenshöhen je Schadenszenario wieder. Die Schutzbedarfsfeststellung der Anwendungen erfolgt nach der Definition der Schutzbedarfskategorien. Dies wird mittels des Prozessschnittstellen-Symbols verdeutlicht. In Abb. 5.7 wird das im Vorfeld beschriebene Modell dargestellt.

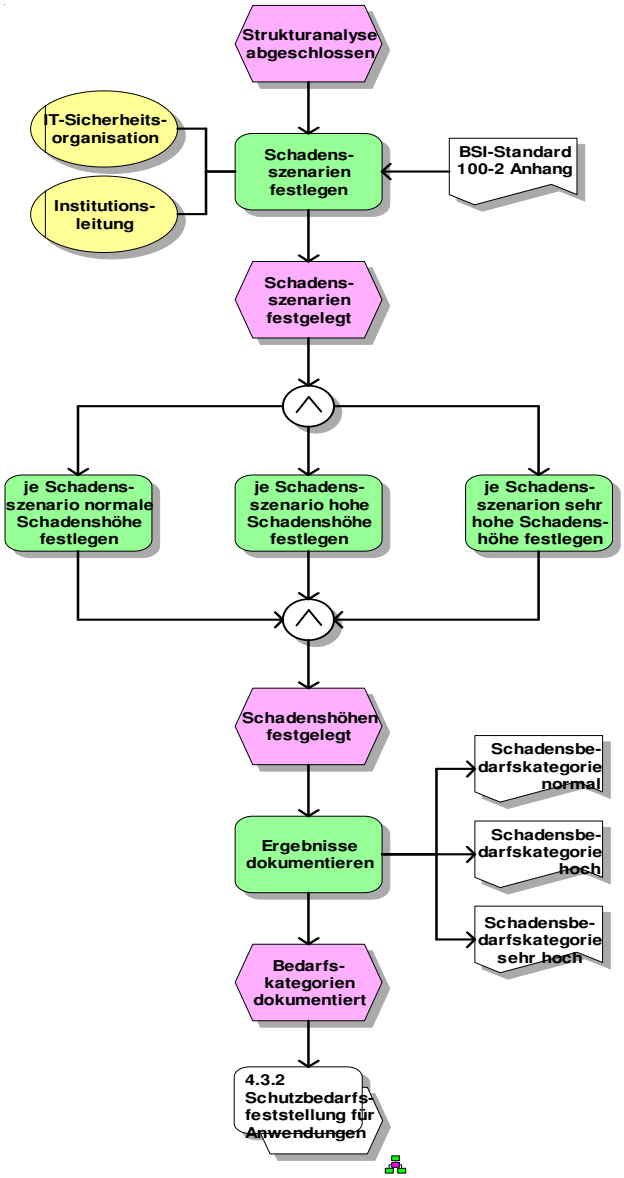


Abb. 5.7: eEPK: 4.3.1 Festlegung der Schutzbedarfskategorien

Als nächstes wird das Modell für die Schutzbedarfsfeststellung der Anwendungen vorgestellt. Das Modell trägt die Bezeichnung 4.3.2 „Schutzbedarfsfeststellung der Anwendungen“. Die Schutzbedarfsfeststellung der Anwendungen ist die zweite Phase der Schutzbedarfsfeststellung und schließt sich an die Festlegung der Schutzbedarfskategorien an. Bei der Analyse des Textes sind folgende Teilschritte identifiziert wurden. Erster Schritt ist die Erstellung von Fragenkatalogen. Auf die Übersicht der Anwendungen, welche während der Strukturanalyse erstellt wurde, wird zurückgegriffen. Zusätzlich werden im Anhang des BSI-Standards 100-2 Fragestellungen vorgegeben für die Feststellung des Schutzbedarfs der Anwendungen. Ergebnis ist ein Fragenkatalog zur Erhebung des Schutzbedarfs, der von der IT-Sicherheitsorganisation erstellt wird. Im zweiten Schritt werden zusammen mit dem Anwendungsverantwortlichen die Schutzbedarfskategorien zu Vertraulichkeit, Verfügbarkeit und Integrität den Anwendungen zugeordnet. Als Input dienen dafür die Schadenbedarfskategorien normal, hoch und sehr hoch sowie die zuvor erstellten Fragenkataloge. Die Zuordnung der Schutzbedarfskategorien zu Vertraulichkeit, Verfügbarkeit und Integrität ist für jede Anwendung durchzuführen und wird im Modell, mittels dreier Funktionen die parallel angeordnet sind, dargestellt. Die zugeordneten Schadenskategorien sowie die Begründung der Zuordnung sind als Schutzbedarf der Anwendungen zu dokumentieren. Die Dokumentation beendet den Prozess „Schutzbedarfsfeststellung für Anwendungen“. Als nächster Prozess folgt die „Schutzbedarfsfeststellung der IT-Systeme“. Mittels des Prozessschnittstellen-Symbols wird er als Folgeprozess dargestellt. Abb. 5.8 veranschaulicht den zuvor beschriebenen Prozess.

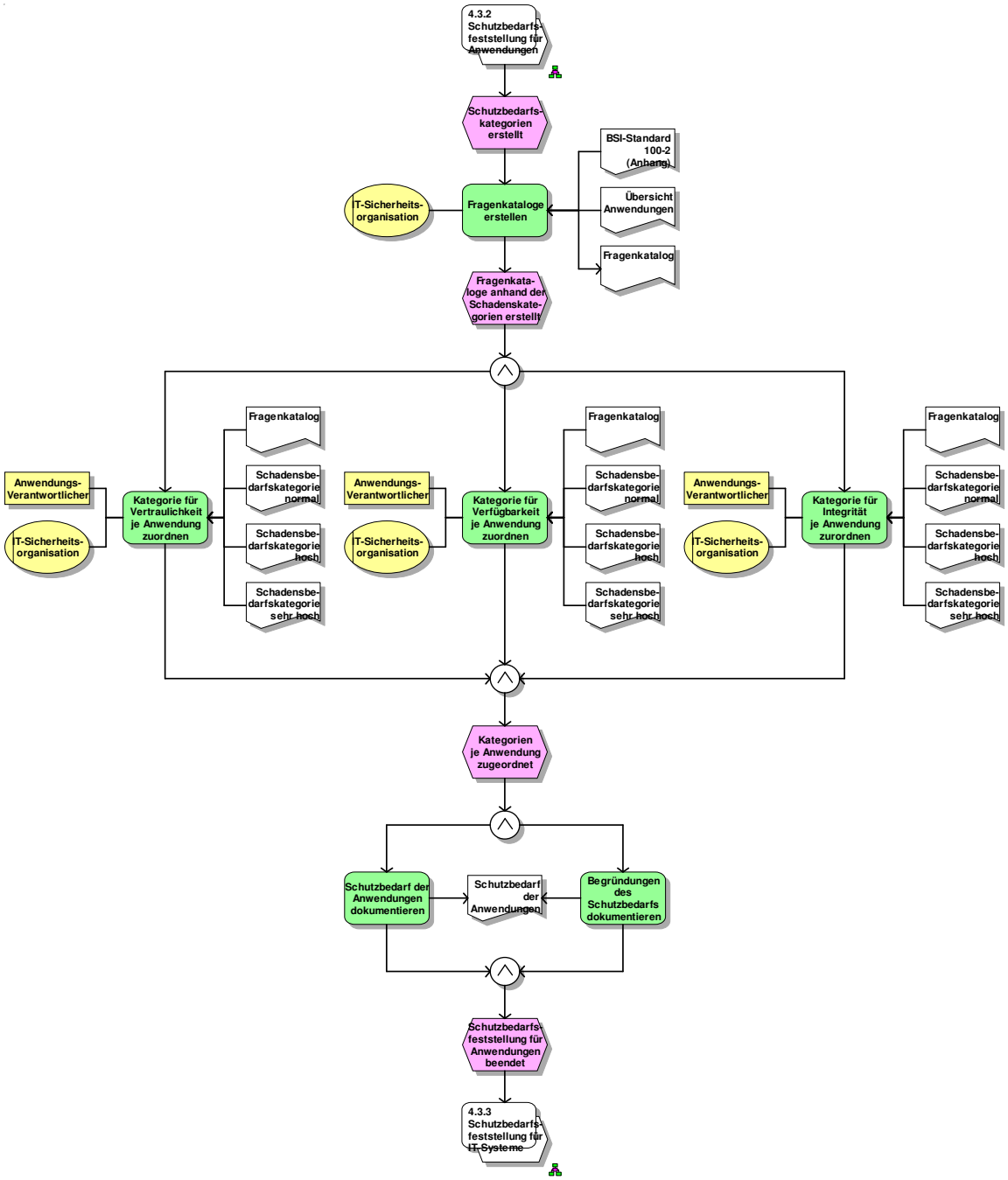


Abb. 5.8: eEPK: 4.3.2 Schutzbedarfsfeststellung für Anwendungen

Der Funktionsbaum zur Erstellung einer Sicherheitskonzeption stellt die Tätigkeiten der Phase zwei der IT-Grundschutzweise grafisch dar. Zu beachten ist, dass Funktionsbäume zur Unübersichtlichkeit neigen, da sehr viele Teilaufgaben und dazugehörende untergeordnete Teilaufgaben dargestellt werden müssen (Aufgabenhierarchie). Zur Bewahrung der Übersichtlichkeit werden zusätzliche Funktionsteilbäume angelegt. Diese Modelle sind durch ein (FB) im Anschluss an die Kapitelnummerierung gekennzeichnet. Liegen keine untergeordneten Teilaufgaben vor so werden die Tätigkeiten direkt an

die übergeordnete Teilaufgabe angehängt. Die Erstellung einer Sicherheitskonzeption zerlegt sich in die Aufgaben:

- 4.1 Definition des Geltungsbereichs
- 4.2 (FB) Strukturanalyse
- 4.3 (FB) Schutzbedarfsfeststellung
- 4.4 (FB) Auswahl und Anpassung der Maßnahmen
- 4.5 (FB) Basis-Sicherheitscheck
- 4.6 (FB) ergänzende Sicherheitsanalyse

Anhand der Abb. 5.9 können diese Schritte nachvollzogen werden. Die Teilaufgabe „4.1 Definition des Geltungsbereiches“ unterteilt sich nicht in weitere übergeordnete Teilschritte. Die Tätigkeiten im Prozess können direkt angeordnet werden, ohne eine weitere Hierarchieebene betrachten zu müssen. In der Teilaufgabe „Schutzbedarfsfeststellung“ wird eine weitere Hierarchieebene benötigt. Weitere Teilschritte sind zu betrachten. Aus diesem Grund wird ein Funktionsbaum mit der Bezeichnung „4.3 (FB) Schutzbedarfsfeststellung“ angelegt.

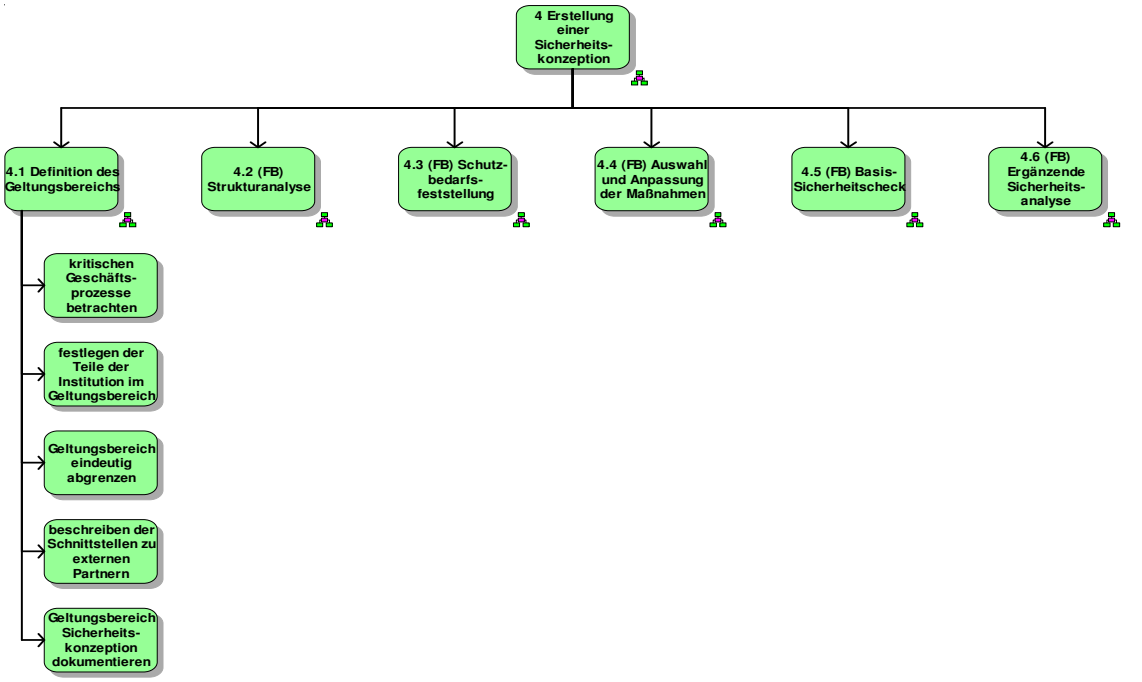


Abb. 5.9: Funktionsbaum: 4 Erstellung einer Sicherheitskonzeption

Der Funktionsbaum für die Schutzbedarfsfeststellung wird in Abb. 5.10 dargestellt.

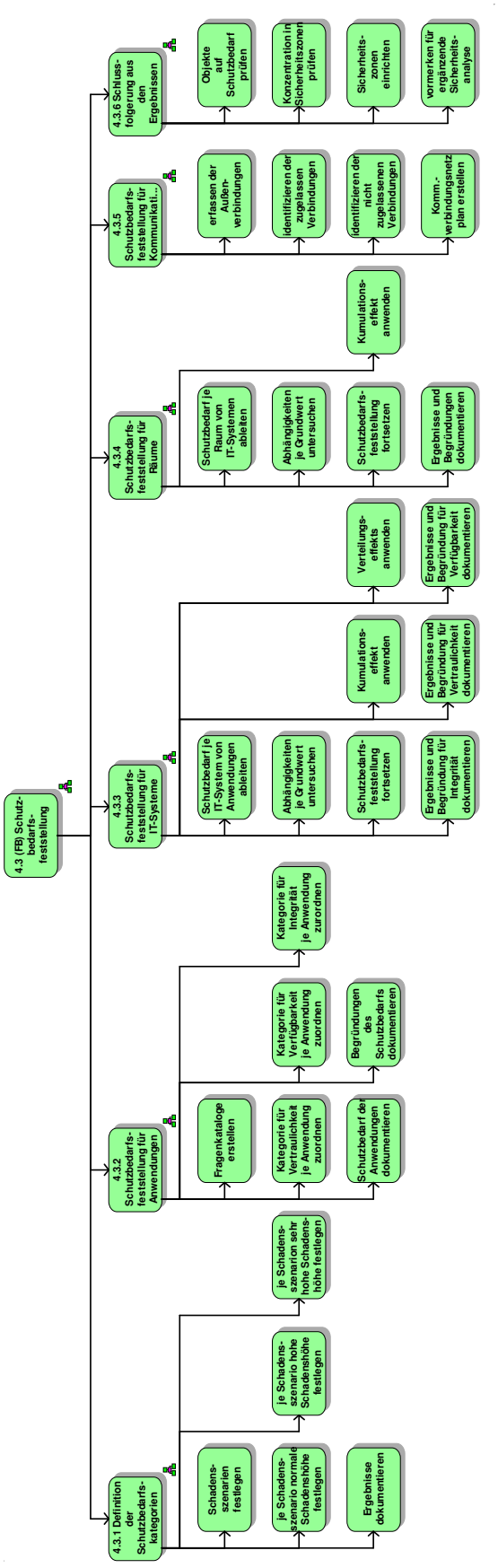


Abb. 5.10: Funktionsbaum: 4.3 (FB) Schutzbedarfsfeststellung

Bei der Erstellung des Referenzmodells werden die folgenden Kapitel nicht modelliert: Kapitel 4.4.1 „Die IT-Grundschutz-Kataloge“ sowie Kapitel 4.6.1 „zweistufiger Ansatz der IT-Grundschutz-Vorgehensweise“. Beide Kapitel besitzen informativen Charakter, beschreiben aber keine relevanten Arbeitsschritte. Im Weiteren werden die Teilkapitel des Kapitels 3.4 als in einem Modell aufbereitet. Der Grund ist, dass die wesentlichen Aufgaben bei der Schaffung der Sicherheitsorganisation im Einführungsteil des Kapitels sowie im Unterkapitel 3.4.1 beschrieben werden. Beide Teile geben den Vorgang der Sicherheitsorganisationgestaltung wieder und werden in einem Modell zusammengefasst. Die Unterkapitel 3.4.2 bis 3.4.8 geben Informationen über die mögliche Organisationsstruktur bzw. Beschreibungen über die Stellen dieser Struktur wider. Sie beschreiben aber keine Vorgänge. Aus diesem Grund wurde auf eine Modellierung verzichtet.

5.3 Betrachtung IT-Grundschutz und ISO 27001:2005

Um die Modellierung des Referenzmodells abzurunden werden in diesem Kapitel die Anforderungen an ein ISMS nach ISO 27001:2005 mit dem IT-Grundschutz verglichen. Schließlich muss die Vorgehensweise nach IT-Grundschutz den Anspruch ISO 27001 konform zu sein erfüllen. Zur Veranschaulichung werden die Anforderungen der ISO 27001 kapitelweise mit der IT-Grundschutz-Methodik verglichen. Die Inhalte der Kapitel der ISO 27001:2005 werden beschrieben und den Kapiteln der Standards des Bundesamts für Informationstechnik zugeordnet.

Tab. 5.1: Zuordnung ISO 27001 zu IT-Grundschutz

Kapitel ISO 27001:2005 mit Inhaltsbeschreibung	**Abgebildet im IT-Grundschutz unter**
Kapitel 1 „Scope“ Erklärung des Anwendungsbereiches	BSI-Standard 100-2 Version 2.0 Kapitel 1
Kapitel 2 „Normative references“ Betrachtung von Referenzstandards	BSI-Standard 100-2 Version 2.0 Kapitel 1.5
Kapitel 3 „Terms and definitions“ Definition der Begrifflichkeiten	Glossar im IT-Grundschutz-Katalog
Kapitel 4.1 „General requirements“	BSI-Standard 100-2 Ver-

Kapitel ISO 27001:2005 mit Inhaltsbeschreibung	**Abgebildet im IT-Grundschutz unter**
Allgemeine Anforderungen eines ISMS werden beschrieben. Ein dokumentiertes ISMS, welches nach dem PDCA-Modell entwickelt, umgesetzt, aufrechterhalten und kontinuierlich verbessert wird, ist aufzubauen und auf Geschäftsaktivitäten und Risiken auszurichten.	sion 2.0 Kapitel 2
Kapitel 4.2 „Establishing and managing the ISMS“	
Kapitel 4.2.1 „Establish the ISMS“ In diesem Kapitel werden die Festlegungen für die Etablierung eines ISMS beschrieben. Diese sind: • Gültigkeitsbereich und Grenzen des ISMS • Leitlinie erstellen • Methode der Risikoanalyse • Risikoidentifikation • Risikoanalyse und -Bewertung • Risikobehandlung • Maßnahmenauswahl zur Behandlung der Risiken • Einholen der Managementfreigabe von Restrisiken • Einholen der Managementbefugnis zur Etablierung und Steuerung des ISMS • Entscheidungen dokumentieren	BSI-Standard 100-2 Version 2.0 Kapitel 3 und 4 BSI-Standard 100-3 Version 2.5
Kapitel 4.2.2 „Implement and operate the ISMS“ Folgende Schritte für die Umsetzung und Durchführung des ISMS werden gefordert: • Formulierung Risikobehandlungsplan • Umsetzung Risikobehandlungsplans	BSI-Standard 100-2 Version 2.0 Kapitel 3; 4 & 5

Kapitel ISO 27001:2005 mit Inhaltsbeschreibung	**Abgebildet im IT-Grundschutz unter**
• Umsetzung ausgewählter Maßnahmen • Messung der Effizienz der umgesetzten Maßnahmen • Schulungs- und Sensibilisierungsmaßnahmen sind zu treffen • Verwaltung von Ressourcen • Verfahren und Maßnahmen zur Aufdeckung von Sicherheitsvorfällen	
Kapitel 4.2.3 „Monitor and review the ISMS“ Bei der Überwachung und Überprüfung fordert der Standard die folgenden Punkte: • Etablierung von Überwachungsverfahren • Überprüfung der Effizienz des ISMS • Maßnahmen auf Effektivität und Zielerreichung • Überprüfung des Restrisikos und der akzeptablen Risikoniveaus • Regelmäßige ISMS Überprüfungen • Managementbewertung des ISMS durch das Management	BSI-Standard 100-2 Version 2.0 Kapitel 6
Kapitel 4.2.4 „Maintain and improve the ISMS“ Die Folgenden Anforderungen sind bei der Aufrechterhaltung und Verbesserung des ISMS zu erfüllen: • Umsetzung der Verbesserungen • Ergreifung geeigneter Korrekturmaßnahmen • Vermittlung von Verbesserungen und Aktivitäten an die Interessensvertreter • Sicherstellung der beabsichtigten Ziele	BSI-Standard 100-2 Version 2.0 Kapitel 6

Kapitel ISO 27001:2005 mit Inhaltsbeschreibung	**Abgebildet im IT-Grundschutz unter**
Kapitel 4.3 „Documentation requirements“	
Kapitel 4.3.1 „General“ Die ISMS Dokumentation sollte beinhalten: • Dokumentierte Erklärung zur ISMS-Strategie und Zielen • Geltungsbereich des ISMS • Verfahren und Maßnahmen zur Unterstützung des ISMS • Beschreibung der Methode zur Risikobewertung • Risikobewertungsbericht • Risikobehandlungsplan • Dokumentierte Verfahren zur Sicherstellung der wirksamen Planung, Durchführung und Kontrolle des Sicherheitsprozesses und der Effektivitätsbewertung von Maßnahmen • Aussage zur Machbarkeit	BSI-Standard 100-2 Version 2.0 Kapitel 6.2
4.3.2 „Control of documents“ Schutz und Kontrolle der Dokumente des ISMS werden gefordert. Ein Dokumentationsverfahren, welches die Aktualität und Qualität der Dokumentationen sicherstellt, ist zu etablieren.	BSI-Standard 100-2 Version 2.0 Kapitel 6.2
4.3.3 „Control of records“ Stellt Forderungen an Unterlagen die während des ISMS zu erstellen sind.	BSI-Standard 100-2 Version 2.0 Kapitel 6.2
5 „Management responsibility“	
5.1 „Management commitment“ Verpflichtungen des Management sind: • Festlegung der Informationssicherheitspolitik	BSI-Standard 100-2 Version 2.0 Kapitel 3

Kapitel ISO 27001:2005 mit Inhaltsbeschreibung	**Abgebildet im IT-Grundschutz unter**
• Sicherstellung der Erreichung der ISMS-Ziele und -Pläne • Festlegen von Rollen und Verantwortlichkeiten • Wichtigkeit der Sicherheitsziele organisationsweit vermitteln • Bereitstellung ausreichender Ressourcen in allen Phasen • Entscheidung über das Risikoniveau treffen • Bewertung des ISMS durch interne Kontrolle	
Kapitel 5.2 „Ressource Management“	
Kapitel 5.2.1 „Provision of ressources“ Management von Ressourcen	BSI-Standard 100-2 Version 2.0 Kapitel 3.5
Kapitel 5.2.2 „Training, awareness and competence“ Ermittlung und Bereitstellung von Ressourcen zur Sensibilisierung und Schulung von Mitarbeitern.	BSI-Standard 100-2 Version 2.0 Kapitel 3.6
Kapitel 6 „internal ISMS Audits“ Regelmäßige Managementbewertung des ISMS hinsichtlich Sicherheitsziele, Maßnahmen und Verfahren	BSI-Standard 100-2 Version 2.0 Kapitel 6
Kapitel 7 „Management review of the ISMS“	
Kapitel 7.1 „General“ Forderung regelmäßiger Überprüfungen des ISMS zur Sicherstellung der weiteren Handhabung, Angemessenheit und Effektivität	BSI-Standard 100-2 Version 2.0 Kapitel 6.1
Kapitel 7.2 „Review input“ Beschreibt die Inputfaktoren zur Managementüberprüfung	BSI-Standard 100-2 Version 2.0 Kapitel 6.1
Kapitel 7.3 „Review output“	BSI-Standard 100-2 Version 2.0 Kapitel 6.1

Kapitel ISO 27001:2005 mit Inhaltsbeschreibung	**Abgebildet im IT-Grundschutz unter**
Ergebnisse der Managementüberprüfung sollten Verwendung finden für: • Effektivitätsverbesserung des ISMS • Aktualisierung der Risikobewertung und des Risikobehandlungsplans • Korrektur der Verfahren und Maßnahmen • Ressourcenanforderung • Verbesserung der Effektivität von Maßnahmen	
Kapitel 8 „ISMS improvement“	
Kapitel 8.1 „Continual improvement“ Forderung nach kontinuierliche Verbesserung des ISMS	BSI-Standard 100-2 Version 2.0 Kapitel 6
Kapitel 8.2 „Corrective action“ Behandelt die Forderungen zu notwendigen korrigierenden Handlungen	BSI-Standard 100-2 Version 2.0 Kapitel 6
Kapitel 8.3 „präventive action“ Behandelt die Forderungen zu vorbeugenden Handlungen	BSI-Standard 100-2 Version 2.0 Kapitel 6

6 Anwendung

In diesem Kapitel wird die Phase fünf „Anwendung“ der Referenzmodellierung betrachtet. Zu Beginn des Kapitels wird das Referenzmodell anhand der Grundsätze ordnungsgemäßer Modellierung sowie die Eignung des Referenzmodells untersucht. Im Anschluss an die Bewertung werden die Anwendungsgebiete für das Referenzmodell näher vorgestellt.

6.1 Bewertung des erarbeiteten Referenzmodells

Das Referenzmodell hat zum Ziel einer Institution bei der Einführung eines ISMS zu unterstützen und auf die Schritte vorzubereiten, die die Einführung mit sich bringt. Die Qualität sowie die Eignung des Modells zur Einführung eines ISMS sind sicherzustellen. Die qualitativen Aspekte werden im ersten Teil des Kapitels näher betrachtet. Im Anschluss wird die Eignung des Referenzmodells näher untersucht.

6.1.1 Bewertung der Qualität des Referenzmodells

Zur Bewertung der Qualität des Referenzmodells werden die Grundsätze ordnungsgemäßer Modellierung herangezogen. Wie bereits in Kapitel 2.1 „Grundsätze ordnungsgemäßer Modellierung“ beschrieben, stellen die GoM einen Ordnungsrahmen, welcher die Erhöhung der Modellqualität verfolgt, vor.[75] Die Modellqualität wird dabei als Maß verstanden, in wie weit die Anforderungen des Modelladressaten erfüllt wurden. In einer frühen Phase des Entwurfs sollen später auftretende Probleme behoben werden. Ziel ist die Reduktion der Subjektivität in der Modellierung.[76]

Als erster Grundsatz wird der Grundsatz der Richtigkeit herangezogen. In ihm wird die syntaktische und semantische Richtigkeit des Referenzmodells näher untersucht. Die syntaktische Richtigkeit wird gewährleistet, in dem sich bei der Modellierung an das Metamodell des ARIS-Konzeptes sowie der in ihm enthaltenen Modelltypen gehalten wurde. Alle verwendeten Objekte und Regeln werden durch diese Architektur unterstützt. Zusätzlich wird durch das verwendete Modellierungswerkzeug, welches auf diesem Metamodell basiert, dieser Sachverhalt unterstützt. Der Modellersteller bekommt die Modellelemente je Modelltyp vorgegeben. Auf Modellaktualität, Erstelldatum und die zeitliche Gültigkeit geht die semantische Richtigkeit näher ein. Das Referenzmodell

---

75 Vgl. Rosemann (1996), S.2
76 Vgl. Rosemann (1996), S.85

ist nach dem Standard (BSI-Standard 100-2) in der Versionsnummer 2.0 aus dem Jahr 2008 modelliert wurden. Die Aktualität des Referenzmodells ist gewährleistet.

Der Grundsatz der Relevanz legt fest, wie viele Informationen ein Modell enthalten soll. Ziel des Referenzmodells ist es, alle Schritte die bei der Einführung eines ISMS vorkommen abzubilden. Erst mit einem kompletten Durchlauf des Managementzyklus kann ein Managementsystem als in der Institution eingeführt angesehen werden. Der zugrunde liegende Standard definiert alle Schritte, die in allen Phasen dieses Zyklus zu beachten sind. Das Referenzmodell richtet sich nach dem Standard, die Relevanz des Referenzmodells hinsichtlich seiner Aufgabenerfüllung ist sichergestellt.

Der nächste Grundsatz, dem sich das Referenzmodell stellen muss, ist der Grundsatz der Wirtschaftlichkeit. Dieser Grundsatz spiegelt die obere Grenze der Modellierung wieder. Die Frage nach Dauerhaftigkeit und Anpassungsfähigkeit sind zu betrachten. Durch den Einsatz eines Modellierungswerkzeuges kann das Modell und der Datenbestand ohne größeren Aufwand übernommen und angepasst werden. Die Anpassungsfähigkeit ist gewährleistet. Das erstellte Referenzmodell ist basierend auf dem aktuellen Stand des Standards (2008) erstellt worden und besitzt einen gewissen Grad an Dauerhaftigkeit. Änderungen hinsichtlich der IT-Grundschutz-Vorgehensweise sind dennoch möglich, können aber zu diesem Zeitpunkt nicht vorhergesagt werden.

Ästhetischen Merkmale wie Strukturiertheit, Verständlichkeit und Übersichtlichkeit werden unter dem Grundsatz der Klarheit vereint. Das Referenzmodell hält sich an die im Kapitel 4.2 definierten Modellierungskonventionen. Alle Modeltypen und Elemente sowie die Anordnung der Elemente in den einzelnen Modellen werden in den Konventionen vorgegeben. Jedes Modell des Referenzmodells ist nach diesen Konventionen ausgerichtet. Die Klarheit der Modelle im Referenzmodell ist gewährleistet.

Der Grundsatz der Vergleichbarkeit fordert, dass zum Einen Modelle, die auf unterschiedlichen Metamodellen basieren ineinander überführbar sind und zum Anderen Modelle, die auf einem Metamodell beruhen über konventionsgerechte Objektbenennungen und Modellierungskonstrukte verfügen.[77] Bei der Referenzmodellierung wurde das ARIS-Konzept mit seinen Modelltypen als Metamodell verwendet. Das Metamodell gibt die Modellierungskonstrukte sowie Attribute für die Objektbeschreibung vor. Jedes Modell des Referenzmodells ist diesem Metamodell untergeordnet. Alle Modelle des Referenzmodells sind hinsichtlich ihrer Konstrukte und Objektattribute vergleichbar. Die Vergleichbarkeit zwischen unterschiedlichen Metamodellen wird nicht näher betrachtet.

---

[77] Vgl. Rosemann (1996), S.103

Der Grundsatz des systematischen Aufbaus fordert ein sichtenübergreifendes Metamodell.[78] Dieses Metamodell soll ermöglichen Modelle, die aus verschiedenen Sichtweisen modelliert werden, zu verbinden. Das ARIS-Konzept, welches bei der Referenzmodellierung als Metamodell Verwendung fand, ermöglicht die sichtenübergreifende Modellierung. In Kapitel 4.1.1 „Konzeption von ARIS“ wird das Metamodell näherbeschrieben. Das Referenzmodell, welches sich dem ARIS-Konzept unterordnet, wird dem Grundsatz des systematischen Aufbaus gerecht.

Das Referenzmodell, welches in dieser Arbeit erstellt wurde, ordnet sich den Gestaltungsregeln der GoM unter und spiegelt einen gewissen Grad an Modellqualität wider.

6.1.2 Eignung des Referenzmodells zur Einführung eines ISMS

Das erstellte Referenzmodell soll dem Anspruch ein ISMS in eine Institution einzuführen genügen. Um diesem Anspruch gerecht zu werden, muss man im ersten Schritt die Anforderungen an das Referenzmodell näher beschreiben, um im Anschluss einen Vergleich mit dem erstellten Referenzmodell vornehmen zu können.

Die folgenden Anforderungen sind im Vorfeld an das Referenzmodell gestellt worden:

- Verwendung eines Standards, der die wesentlichen Anforderungen an ein ISMS beschreibt
- Verwendung eines Metamodells, welches die Modellierung von Prozessabläufen unterstützt und intuitiv zu verstehen ist
- Einhaltung der Grundsätze ordnungsgemäßer Modellierung
- Abbildung der Prozessschritte im ISMS
- Visualisierung der beteiligten Organisationseinheiten und des Dokumentenflusses

Anhand dieser Anforderungen wird die Eignung des Referenzmodells zur Einführung eines ISMS gezeigt.

Zu allererst wird auf die Anforderung eingegangen, dass das Referenzmodell auf einen Standard zurückgreifen soll. Das Referenzmodell basiert sowohl auf dem internationalen Standard ISO 27001:2005 als auch auf den nationalen Quasistandard des BSI, den

[78] Vgl. Rosemann (1996), S.103

BSI-Standard 100-2. Als Ausgangspunkt für die Modellierung wird der Quasistandard BSI-Standard 100-2 herangezogen. Dieser Standard setzt die Anforderungen des ISO 27001 Standards um. Die beiden Standards werden in den Kapiteln 3.3.2 „ISO 27001:2005“ sowie im Kapitel 5.1 „Inhaltliche Beschreibung des BSI-Standards 100-2 Version 2.0“ vorgestellt. Auf die Konformität der IT-Grundschutz-Methodik zum ISO 27001 Standard wird in Kapitel 5.3 „Betrachtung IT-Grundschutz und ISO 27001:2005“ näher eingegangen. Die genannten Punkte führen dazu, dass die Anforderung an das Referenzmodell sich an einen Standard zu halten, der die wesentlichen Anforderungen eines ISMS beschreibt, erfüllt ist.

Anforderung zwei besteht darin sich einem Metamodell unterzuordnen, welches die Modellierung von Prozessabläufen unterstützt und zugleich intuitiv zu verstehen ist. Das Metamodell, welches zur Verwendung kam, ist das ARIS-Konzept mit seinen Modelltypen. Es wird im Kapitel 4.1.1 „Konzeption von ARIS“ näher vorgestellt. ARIS findet vielfältige Verwendung bei der Erstellung von Referenz-, Prozess- und Unternehmensmodellen. Desweiteren wird dem Konzept nach gesagt, eine hohe Anschaulichkeit zu besitzen.[79] Modellanwender, die sich vorher nicht mit ARIS beschäftigt haben, kommt dieser Sachverhalt zu gute.

Die Einhaltung der Grundsätze ordnungsgemäßer Modellierung, also die qualitativen Ansprüche an das Referenzmodell, werden im Kapitel 6.1.1 „Bewertung der Qualität des Referenzmodells“ näher beschrieben. Als Ergebnis dieser Untersuchung zeigt sich, dass hinsichtlich der Modellierung die Vorgaben der GoM erfüllt sind.

Anforderung Nummer vier ist die Abbildung aller Prozessschritte eines ISMS. Das Referenzmodell bildet alle Schritte des vorliegenden Standards BSI-Standard 100-2 ab. Dabei sind vom IT-Sicherheitsprozess, dem übergeordneten Managementprozess bis hin zum einzelnen Arbeitsschritt alle Teilschritte modelliert worden. Als Teil dieser Modellierung wurden die beteiligten Organisationseinheiten und die Dokumentationen, die während der Prozesse erstellt und verwendet werden, dargestellt. Das Referenzmodell gibt die vielfältigen Aufgaben, die ein ISMS erfordert, wieder und stellt den Dokumentenfluss im ISMS dar.

---

[79] Vgl. Rosemann (1996), S.75

6.2 Anwendungsgebiete des Referenzmodells

In diesem Kapitel werden Anwendungsgebiete für das Referenzmodell vorgestellt. Als Anwendungsgebiete werden die institutionelle Einführung und Zertifizierung, die Software-Entwicklung sowie die Entwicklung eines Managementsystemhandbuchs zur Informationssicherheit betrachtet.

6.2.1 Institutionelle Einführung und Zertifizierung

Das erarbeite Modell kann bei Unternehmen die den Sicherheitsprozess in ihre eigene Prozesslandschaft integrieren wollen zur Anwendung kommen. Es beinhaltet alle wesentlichen Aspekte der IT-Grundschutz-Vorgehensweise und der ISO 27001. Das Referenzmodell spiegelt alle Abläufe zur Einführung eines ISMS in der eigenen Institution wider. Insbesondere die Aufgaben der Leitungsebene sowie der IT-Sicherheitsorganisation werden dargestellt. Das Referenzmodell kann an die institutionellen Gegebenheiten angepasst werden und in die Prozessdokumentation der betrieblichen Abläufe integriert werden. Zusätzlich repräsentiert das Referenzmodell den Dokumentenfluss im Informationssicherheitsprozess.

Das vorliegende Referenzmodell kann für die Dokumentation alle Prozessabläufe bei einer Zertifizierung herangezogen werden. Die Zertifizierung des Managementsystems ist der Nachweis der Institution die Anforderungen des zugrunde liegenden Standards zu erfüllen. Interessen an einer Zertifizierung sind:[80]

- Schaffung eines vertrauenswürdigen Nachweises für Dienstleister
- Bereitstellung von Informationen über den Grad der Informationssicherheit zwischen kooperierenden Unternehmen
- Bestrebung zur Nachweispflicht der Informationssicherheit für neue Kooperationspartner
- Repräsentation der Bemühungen zur Informationssicherheit für Kunden bzw. Bürger

Die genannten Punkte spiegeln die Wichtigkeit des Vertrauens wieder. Der Nachweis mit den Informationen von Kunden, Partner oder Bürger sowie mit den eigenen Infor-

[80] Vgl. BSI-Standard 100-2, S. 88

mationen sorgfältig umzugehen steht im Mittelpunkt der Zertifizierungsbestrebungen einer Institution.

Das BSI stellt für die Zertifizierung einer Institution ein Zertifizierungsschema bereit. Dieses Prüfschema für ISO 27001-Audits auf der Basis von IT-Grundschutz richtet sich zum Einen an die Auditoren zur Konformitätsprüfung des ISMS gemäß ISO 27001 auf Basis IT-Grundschutz. Zum Anderen informiert das Schema die IT-Sicherheitsorganisation über die Zertifizierungsanforderungen und gibt einen Überblick welche Dokumente bei der Prüfung bereitgestellt werden müssen.[81]

6.2.2 Software-Entwicklung

Ein weiteres Anwendungsfeld des Referenzmodells bietet sich in der Software-Entwicklung. Die einzelnen Phasen des Management-Zyklus sind in ein Softwareprodukt zu implementieren. Bestrebungen der Software-Unterstützung einzelner Phasen gibt es bereits. Ein Werkzeug ist das IT-Grundschutz-Tool (GSTOOL) des BSI, welches näher vorgestellt werden soll.

Das Grundschutz-Tool

Zur Unterstützung der Erstellung der IT-Sicherheitskonzeption nach IT-Grundschutz stellt das BSI das Grundschutz-Tool (GSTOOL) bereit. Die erste Version wurde im Jahr 1998 vorgestellt. Heute liegt das Tool in Version 4.5 vor. Das GSTOOL unterstützt die folgenden Schritte der IT-Grundschutz-Vorgehensweise:[82]

- IT-Strukturanalyse

  Die Erhebung der Anwendungen, IT-Systeme, Räume und Kommunikationsverbindungen des Geltungsbereichs ist mit anderen Hilfsmitteln zu erarbeiten und kann ins Tool übertragen werden.

- Schutzbedarfsanalyse

  Die Definitionen, Feststellungen und Begründungen des Schutzbedarfs können den Zielobjekten zugeordnet werden.

- Modellierung nach IT-Grundschutz

---

81 Vgl. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, S.7
82 Vgl. GSTOOL-Handbuch, S.2ff

Nachdem der Geltungsbereich (IT-Verbund) durch den Anwender festgelegt wurde und die Zielobjekte in das Tool ein gepflegt sind, erfolgt eine automatische Zuordnung der Zielobjekte zu den Grundschutz-Bausteinen. Dies darf aber nur als Vorschlag gesehen werden und ist zu prüfen.

- Basis-Sicherheitscheck

  Wird vom Tool vollständig unterstützt.

- Ergänzende Sicherheitsanalyse und Risikoanalyse auf Basis IT-Grundschutz (Siehe BSI-Standard 100-3)

  Die Betrachtung von Zielobjekten mit hohem und sehr hohem Schutzbedarf wird unterstützt. Der Anwender kann sowohl Maßnahmen als auch Gefährdungen individuell anpassen und ergänzen.

- Realisierung der IT-Grundschutz-Maßnahmen

  Unterstützt bei der: Sichtung der Untersuchungsergebnisse, Maßnahmenkonsolidierung, Kosten- und Aufwandsabschätzung, Festlegung der Umsetzungsreihenfolge und Festlegung der Aufgaben und Verantwortung

Das GSTOOL bietet ein breites Spektrum an Funktionalitäten, die dem Anwender bei der Erstellung des IT-Sicherheitskonzeptes sowie bei der Koordination der Maßnahmenumsetzung helfen, an. Eine vollständige Unterstützung des IT-Sicherheitsprozesses bietet das Tool nicht.

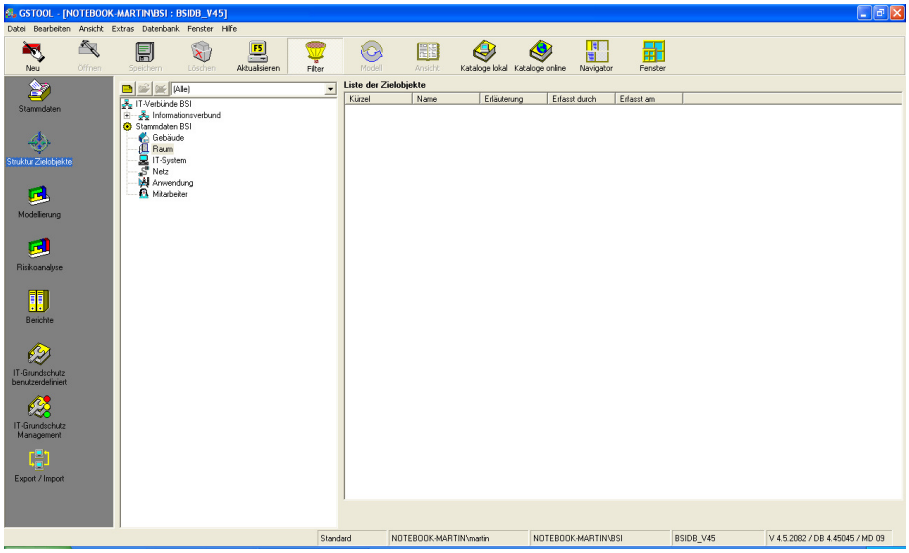


Abb. 6.1: GSTOOL-Oberfläche im Bereich Struktur-Zielobjekte

Weitere Betrachtung

Neben dem GSTOOL gibt es weitere Softwareprodukte, die sich der Thematik widmen. Diese Produkte decken die Funktionalitäten des GSTOOLs vollständig oder nur teilweise ab und unterscheiden sich hinsichtlich ihrer Bedienungsoberflächen. Die Abb. 6.1 spiegelt die GSTOOL Oberfläche wider und gibt einen Einblick in die Funktionsmöglichkeiten des Tools.

Alle Werkzeuge haben gemeinsam, dass sie den gesamten IT-Sicherheitsprozess nicht unterstützen. Auf die Erstellung der Sicherheitskonzeption und die darin enthaltenen Schritte fokussieren sich die Tools zur Grundschutz-Thematik. Das Referenzmodell mit seiner umfangreichen Sicht auf den IT-Sicherheitsprozess kann die Lücke schließen und neuen Tool-Funktionalitäten den Weg ebnen. Ein Werkzeug welches den gesamten Sicherheitsprozess unterstützt, ist anzustreben.

6.2.3 Management-Handbuch zur Informationssicherheit

Ein weiteres Anwendungsfeld, welches betrachtet wird, ist die Erstellung von Management-Handbüchern. In diesem Fall die Erstellung eines Management-Handbuchs zur Informationssicherheit.

Ein Management-Handbuch zur Informationssicherheit sollte folgende Dokumentationen enthalten:

- Informationssicherheitspolitik, -ziele und -methodik
- Management- und Verfahrensanweisungen
- Zuordnung von Kompetenzen und Zuständigkeiten
- Aufbau und Ablauforganisation
- Technische Dokumentationen
- Arbeits- und Verfahrensanweisungen für die Arbeitsplätze

Das zu erstellende Handbuch kann sich im Aufbau in drei Ebenen unterteilen. Die Ebene eins wird die Dokumente zur Informationssicherheitspolitik, -ziele und -Methodik enthalten. Diese Ebene ist auch zur Kommunikation außerhalb der Institution geeignet, da sie die Einstellung zum Thema Informationssicherheit darlegt. Auf der zweiten Ebene ordnen sich die Management- und Verfahrensanweisungen, die Kompetenzen und Zuständigkeiten, die Aufbau und Ablauforganisation des Managementsystems sowie die

technischen Dokumentationen ein. Die dritte Ebene beinhaltet die Arbeits-, Verfahrens- und Prüfanweisungen am Arbeitsplatz. Mit Hilfe des Handbuches wird es möglich, die erstellten Dokumente im IT-Sicherheitsprozess systematisch zu ordnen und abzulegen. Das Referenzmodell bietet den Einblick in die Aufbau- und Ablauforganisation und gibt einen Einblick in die Dokumentationen, die während des IT-Sicherheitsprozesses entstehen. Der Nutzen eines solchen Handbuches spiegelt sich wieder in:

- Zentralen Ablage aller Dokumentationen im Informationssicherheitsprozess
- Vermittlung der Wichtigkeit der Informationssicherheit nach Außen
- Nachweis zur Verpflichtung auf die Informationssicherheit
- Schneller Einstieg für neue Mitarbeiter im Bereich Informationssicherheit
- Reduzierung der Dokumentensuche

Das Management-Handbuch muss nicht in Papierform vorliegen. Die Einführung eines Dokumenten-Managementsystems zur elektronischen Dokumentenverwaltung bietet sich bei Institutionen, die über eine umfangreiche IT-Umgebung oder komplexe Organisationstruktur, mit mehreren Hierarchiestufen, verfügen, an.

7 Fazit

Die Diplomarbeit betrachtet die Erstellung eines Referenzmodells zur Einführung eines Informationssicherheits-Managementsystems. Die Referenzmodellierung selbst wurde nach einem Phasenmodell durchgeführt und umgesetzt. Unterstützt wurde der Erstellungsprozess des Referenzmodells durch das ARIS-Konzept und dem ARIS-Toolset. Die Möglichkeiten, die das ARIS-Konzept bietet, wurden in den Modellierungskonventionen, die die verwendeten Modelltypen, Symbole und Struktur vorgeben, eingegrenzt. Ziel der Modellierung war es, alle Schritte bei der Einführung eines Informationssicherheits-Managementsystem abzubilden. Die IT-Grundschutz-Vorgehensweise, welche die Anforderungen des ISO 27001 Standard erfüllt und eine Schritt für Schritt Anleitung durch den Informationssicherheitsprozess gibt, wurde als Ausgangspunkt für die Modellierung verwendet. Die Anwendungsmöglichkeiten des erstellten Referenzmodells wurden vorgestellt und sollen durch das Referenzmodell unterstützt und gefördert werden.

Es zeigt sich, dass Informationssicherheits-Managementsysteme noch erheblichen Aufholbedarf hinsichtlich ihrer Verbreitung aufweisen. In einer Statistik, die die International Organization for Standardization bereitstellt, wird dies besonders deutlich. Im Dezember 2006 gab es weltweit ca. 5800 ISO 27001:2005 Zertifizierungen. Japan mit ca. 3800 Zertifizierungen nimmt in diesem Zusammenhang eine Vorreiterrolle ein. Deutschland liegt in der Statistik der führenden Länder, nach der Anzahl ihrer Zertifizierungen, auf Platz sechs mit ca. 100 Zertifizierungen. Der Unterschied ist beachtlich und zeigt, dass die Bestrebungen auf diesem Gebiet weiter fortzuführen sind. Die ISO 9001:2000, als Standard für Qualitätsmanagementsysteme, kann als Vorbild gesehen werden. Im Dezember 2006 haben die Zertifizierungen dieses Standards weltweit den Wert von annähernd 900.000 erreicht.[83]

Gründe für diesen Nachholbedarf sind zum Einen, dass Informationssicherheit immer noch als Kostenfaktor gesehen wird und zum Anderen die mangelnde Sensibilisierung in diesem Bereich. Die Auswirkungen bei einem Verlust der Informationssicherheit reichen bis zur existenziellen Bedrohung einer Institution.

Informationen sind als Unternehmenswerte anzusehen und müssen geschützt werden. Dieser Aufgabe haben sich die Informationssicherheits-Managementsysteme zugewendet. Das Referenzmodell wird bei einer institutionsweiten Einführung eines Informationssicherheits-Managementsystems nach ISO 27001 auf Basis IT-Grundschutz helfen und einer Institution die Prozesse eines solchen Managementsystems aufzeigen.

---

[83] Vgl. ISO Survey (2006), S.8 und S.12

Literaturverzeichnis

Ahrens, V.: Allgemeine und ethische Grundlagen von Managementsystemen, in Ahrens, V.; Hofmann-Kamensky, M. (2001): Integration von Managementsystemen, Ansätze für die Praxis, München, S. 3 - 17.

Bundesamt für Sicherheit in der Informationstechnik BSI (Hrsg.): Die Lage der IT-Sicherheit in Deutschland, Bonn 2007.

Bundesamt für Sicherheit in der Informationstechnik BSI (Hrsg.): BSI-Standard 100-1 - Managementsysteme für Informationssicherheit (ISMS) Version 1.5, Bonn 2008.

Bundesamt für Sicherheit in der Informationstechnik BSI (Hrsg.): BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise Version 2.0, Bonn 2008.

Bundesamt für Sicherheit in der Informationstechnik BSI (Hrsg.): BSI-Standard 100-3 - Risikoanalyse auf der Basis von IT-Grundschutz Version 2.5, Bonn 2008.

Bundesamt für Sicherheit in der Informationstechnik BSI (Hrsg.): IT-Grundschutz-Katalog Stand 9. Ergänzungslieferung, http://www.bsi.de/gshb/deutsch/index.htm.

Bundesamt für Sicherheit in der Informationstechnik BSI (Hrsg.): GSTOOL-Handbuch Version 4.5, Bonn 2008.

Bundesamt für Sicherheit in der Informationstechnik BSI (Hrsg.): Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz: Prüfschema für ISO 27001 Audits Version 2.1, Bonn 2008.

Hansen, H. R.; Neumann, G. (2001): Wirtschaftsinformatik I. 8. Aufl., Stuttgart.

Hofmann-Kamensky, M.: Grundelemente, Gestaltungsregeln und Nutzen von Managementsystemen, in: Ahrens, V.; Hofmann-Kamensky, M. (2001): Integration von Managementsystemen, Ansätze für die Praxis, München, S. 19 - 39.

International Organization for Standardization ISO (Hrsg.): ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements. Genua.

International Organization for Standardization ISO (Hrsg.): ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management. Genua.

International Organization for Standardization ISO (Hrsg.): The ISO Survey - 2006: ISO and the ISO Survey. Genua.

Jablonski, S.; Böhm, M.; Schulze, W. (1997): Workflow-Management Entwicklung von Anwendungen und Systemen: Facetten einer neuen Technologie. Heidelberg.

Laudon, K. C.; Laudon J. P.; Schoder D. (2006): Wirtschaftsinformatik: Eine Einführung. München.

Michael, H.; Morawietz, P. (1995): Qualitätsmanagementsysteme nach EN 290001-4 (DIN EN ISO 9001-4), in Hansen, W.; Jansen, H.H.; Kamiske, G. F.: Qualitätsmanagement im Unternehmen – Grundlagen, Methoden und Werkzeuge, Praxisbeispiele. Heidelberg.

Rautenstrauch, C.; Schulze, T. (2003): Informatik für Wirtschaftswissenschaftler und Wirtschaftsinformatiker. Berlin u. a.

Rosemann, M. (1996): Komplexitätsmanagement in Prozessmodellen: Methodenspezifische Gestaltungsempfehlungen für die Informationsmodellierung. Wiesbaden.

Rosemann, M.; Schütte, R. (1999): Multiperspektivische Referenzmodellierung, in Schütte, R (Hrsg.): Referenzmodellierung – State oft the Art und Entwicklungsperspektiven. Heidelberg S. 22 - 44.

Scheer A.W. (1997): Wirtschaftsinformatik: Referenzmodelle für industrielle Geschäftsprozesse. Berlin.

Scheer A.W. (2002): ARIS - Vom Geschäftsprozess zum Anwendungssystem. Berlin.

Vossen, G.; Becker, J. (1996): Geschäftsprozessmodellierung und Workflowmanagement: Modelle, Methoden und Konzepte. Bonn/Albany.

Wikimedia Foundation Inc. (Hrsg.): Wikipedia die freie Enzyklopädie: http://de.wikipedia.org/wiki/hauptseite.

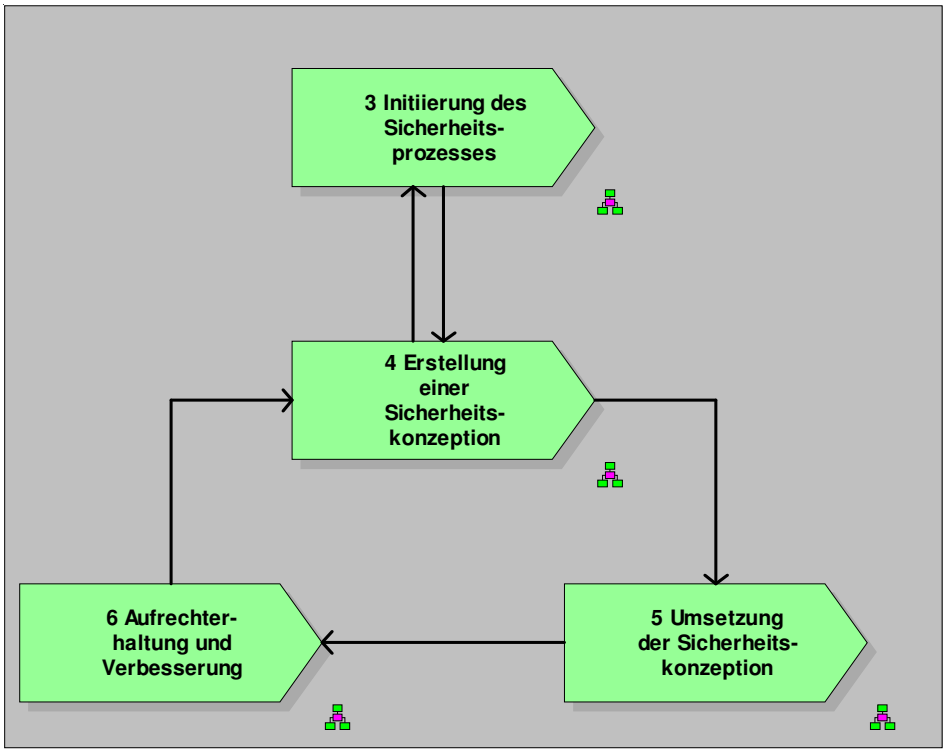
Anhang

Der Anhang gibt das erstellte Referenzmodell wider. Alle Modelle werden dargestellt und hinsichtlich ihrer Gruppenzugehörigkeit eingeordnet.

Ordnerstruktur des Referenzmodells

Der IT-Sicherheitsprozess

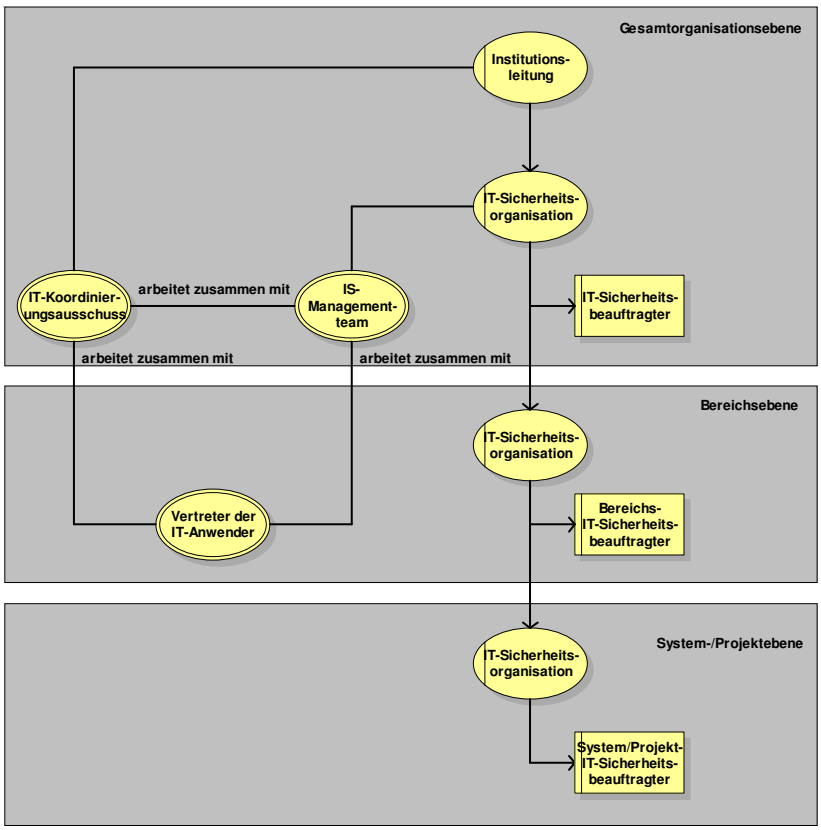
WKD: IT-Sicherheitsprozess



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz

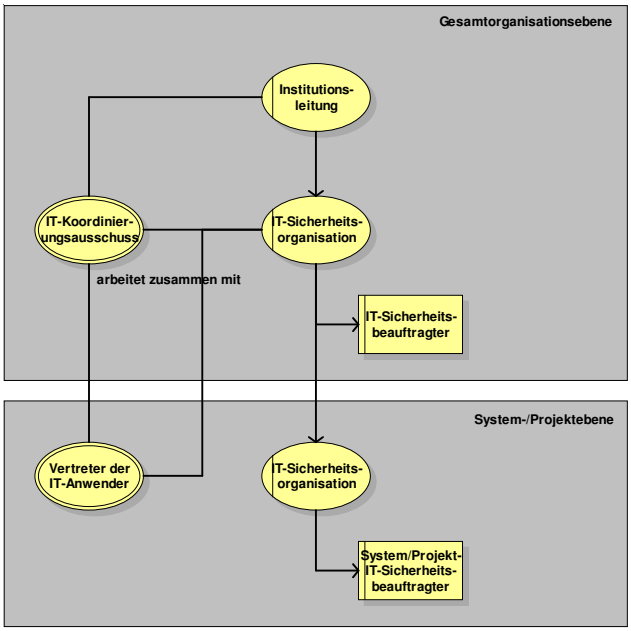
0 Organisationsmodelle

Organigramm: 0.1 IS-Organisation große Institution



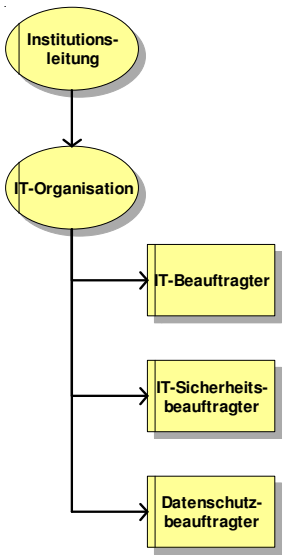
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\0 Organisationsmodelle

Organigramm: 0.2 IS-Organisation mittelgroße Institution



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\0 Organisationsmodelle

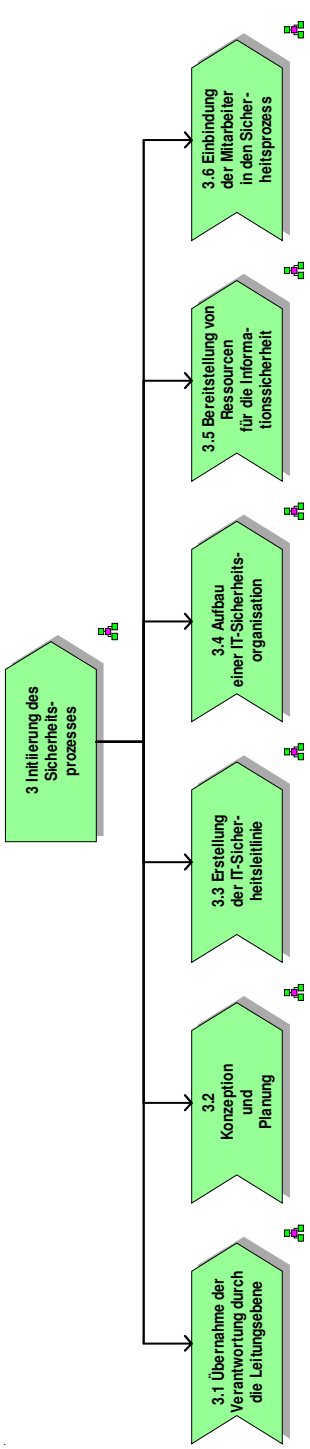
Organigramm: 0.3 IS-Organisation kleine Institution



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\0 Organisationsmodelle

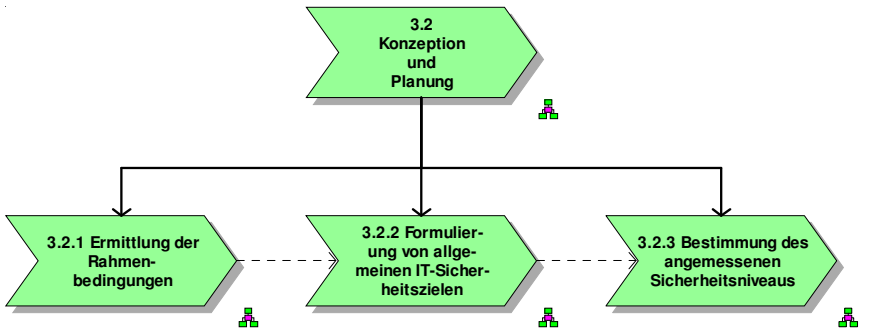
3 Initiierung des Sicherheitsprozesses

WKD: 3 Initiierung des Sicherheitsprozesses



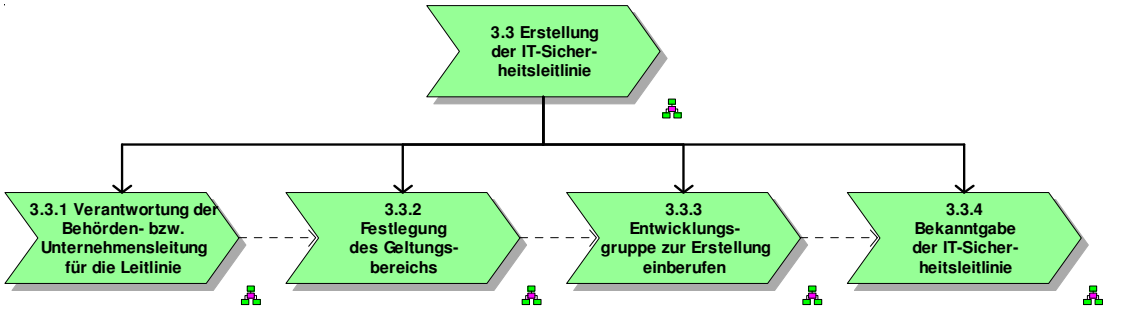
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses

WKD: 3.2 Konzeption und Planung



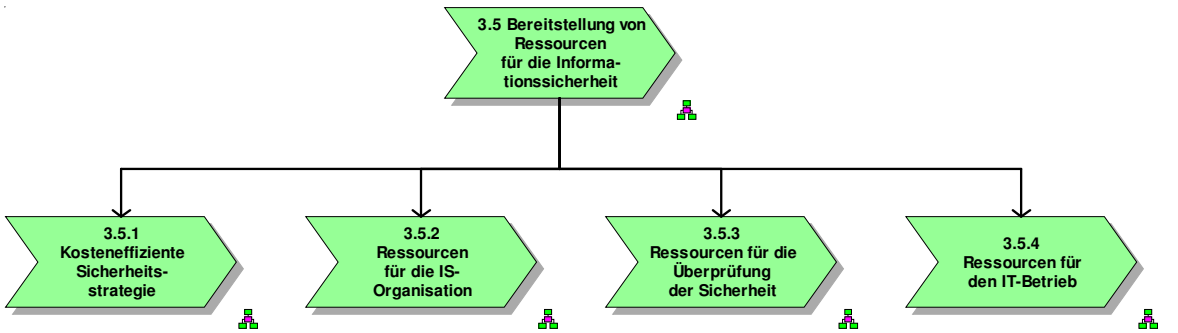
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Managementbetrachtung

WKD: 3.3 Erstellung der IT-Sicherheitsleitlinie



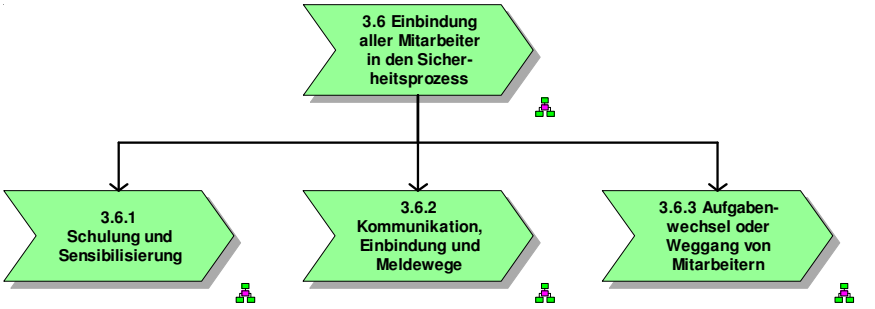
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Managementbetrachtung

WKD: 3.5 Bereitstellung von Ressourcen für die Informationssicherheit



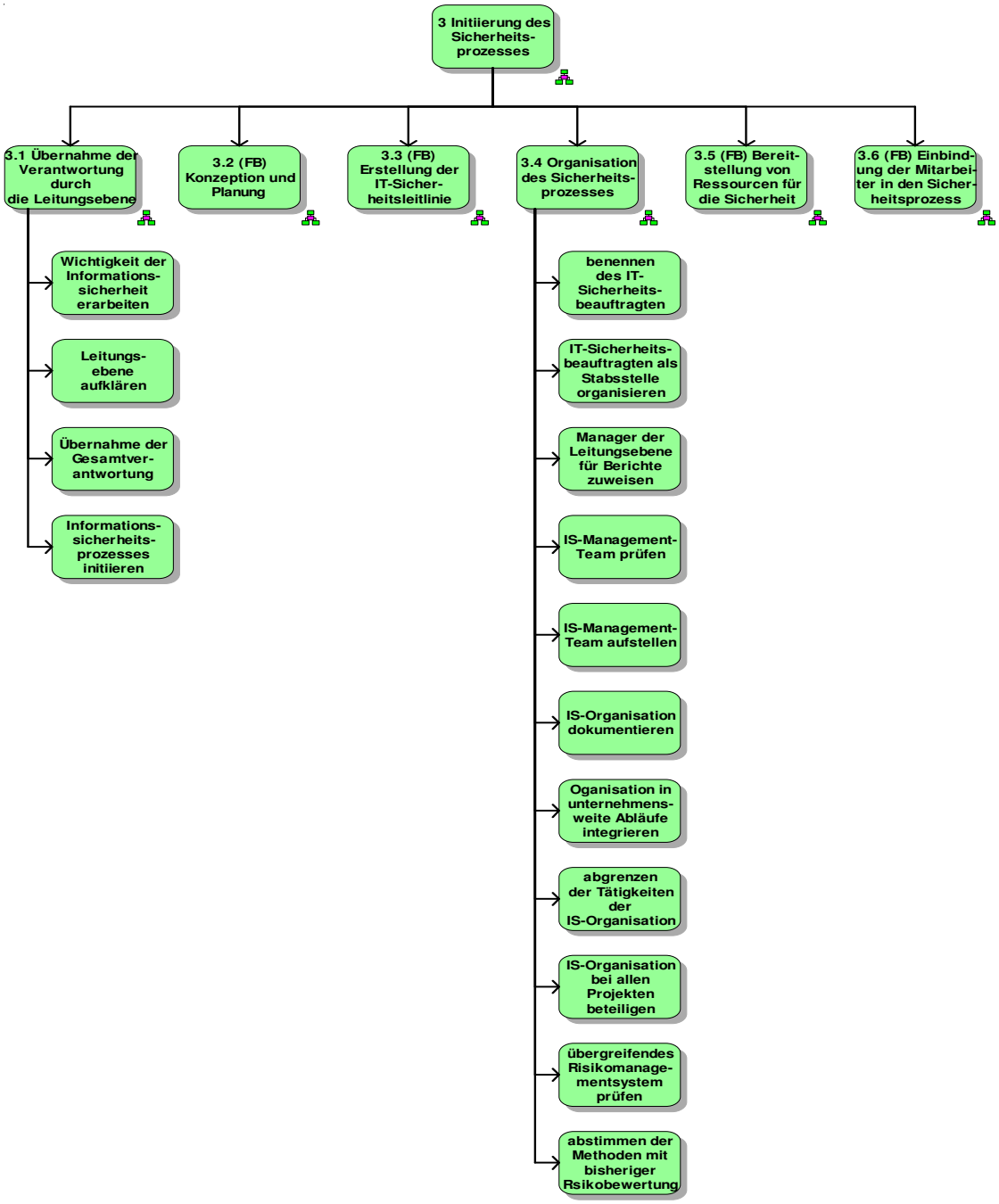
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Managementbetrachtung

WKD: 3.6 Einbindung aller Mitarbeiter in den Sicherheitsprozess



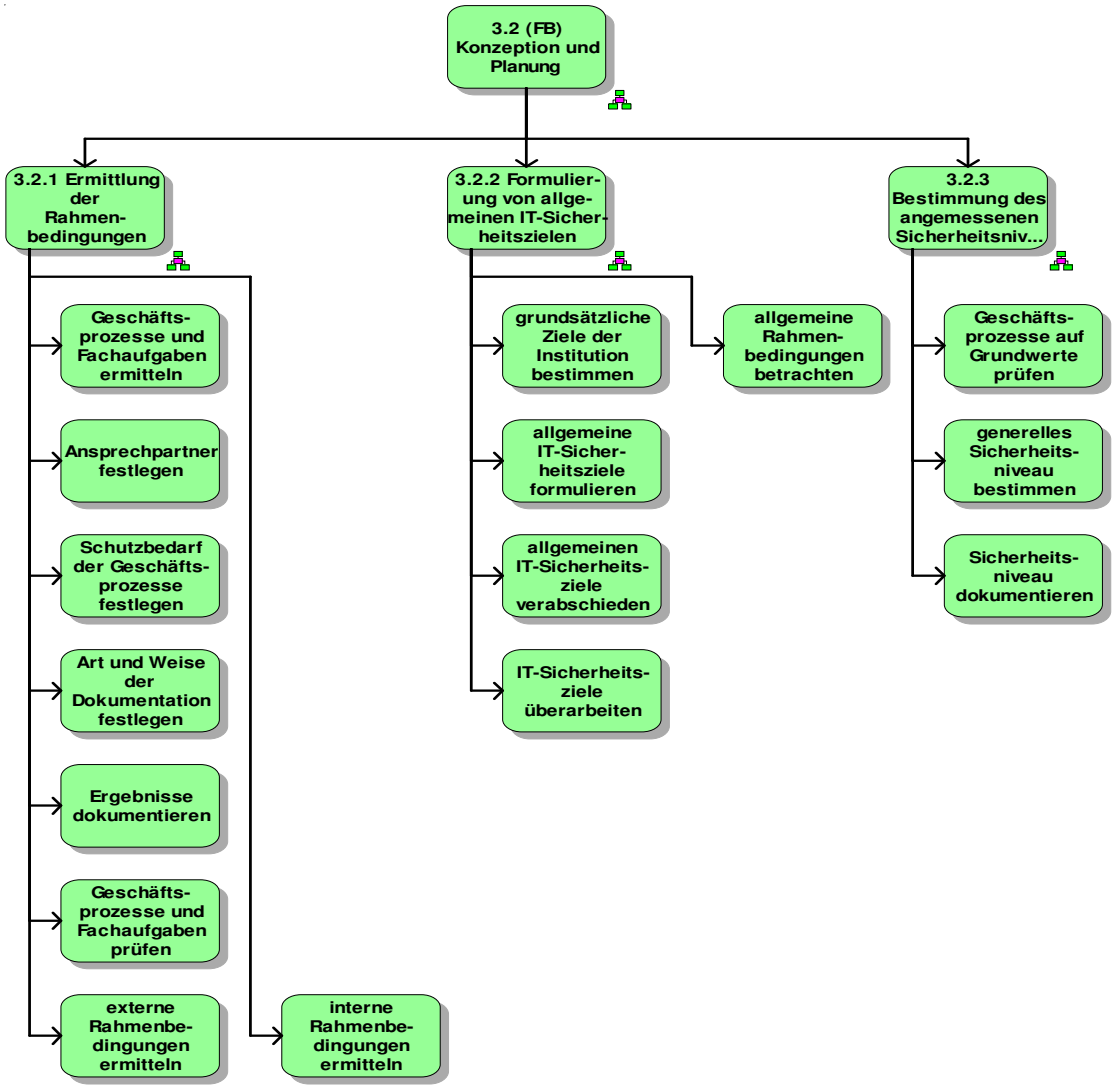
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Managementbetrachtung

Funktionsbaum: 3 Initiierung des Sicherheitsprozess



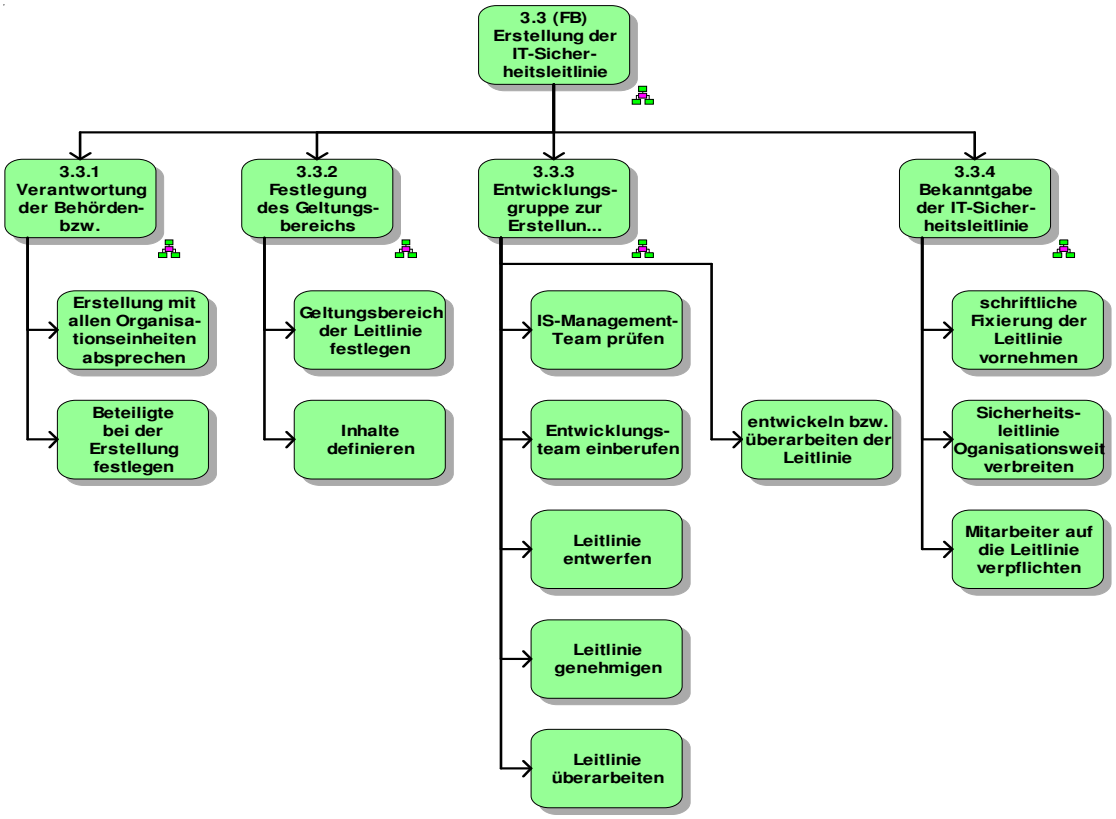
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Funktionsübersicht

Funktionsbaum: 3.2 (FB) Konzeption und Planung



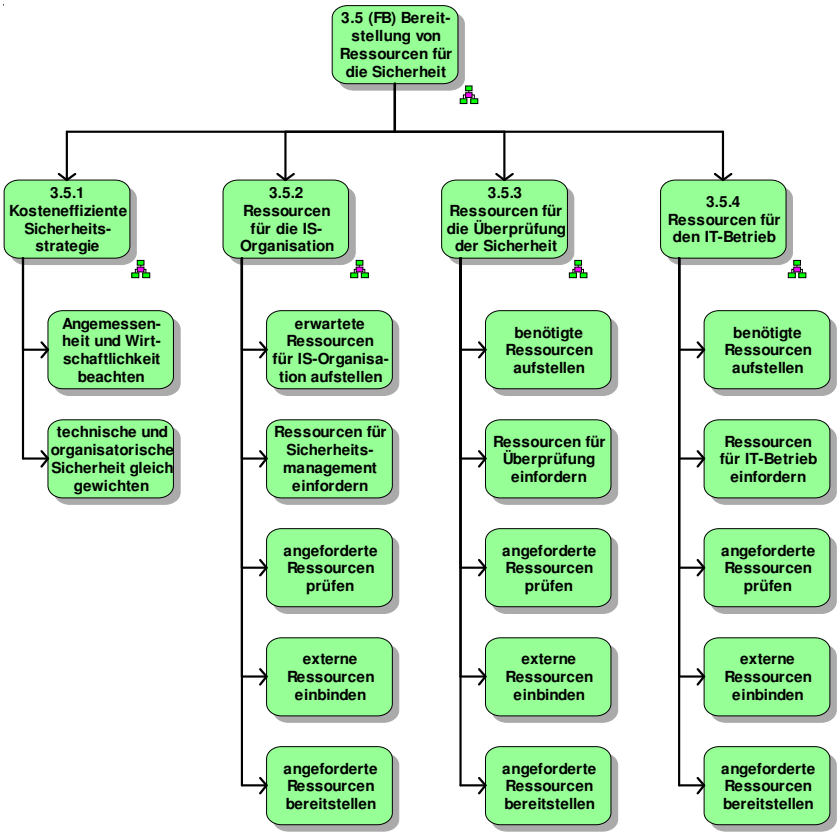
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Funktionsübersicht

Funktionsbaum: 3.3 (FB) Erstellung der IT-Sicherheitsleitlinie



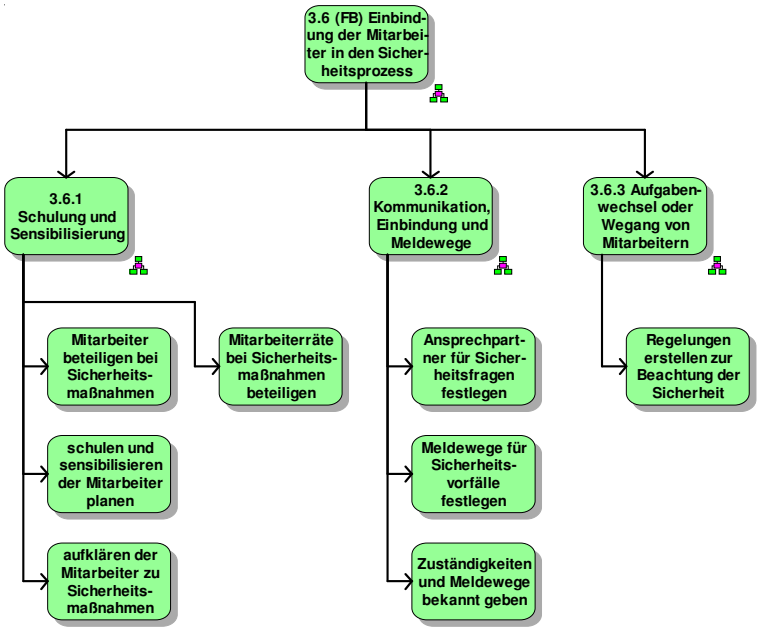
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Funktionsübersicht

Funktionsbaum: 3.5 (FB) Bereitstellung von Ressourcen für die Sicherheit



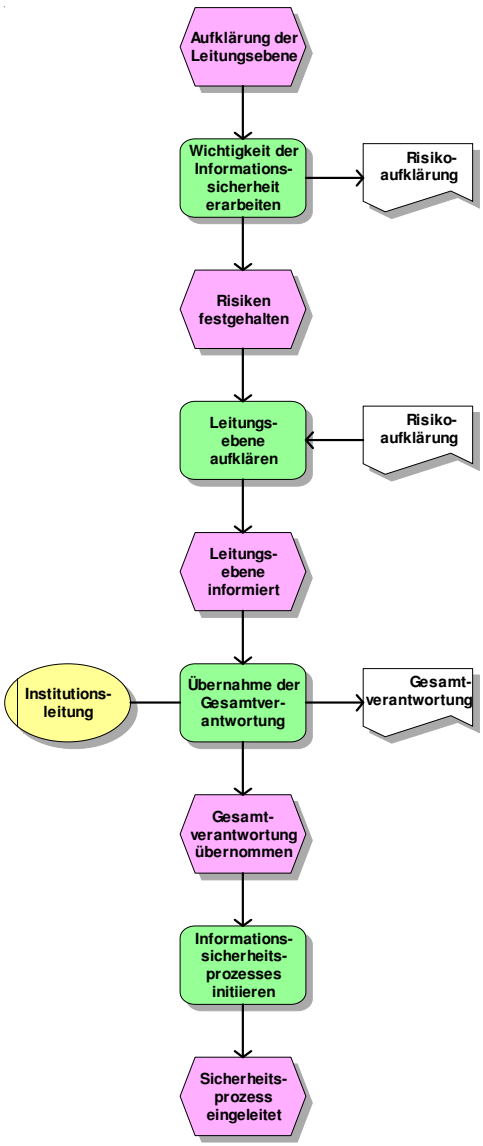
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Funktionsübersicht

Funktionsbaum: 3.6 (FB) Einbindung der Mitarbeiter in den Sicherheitsprozess



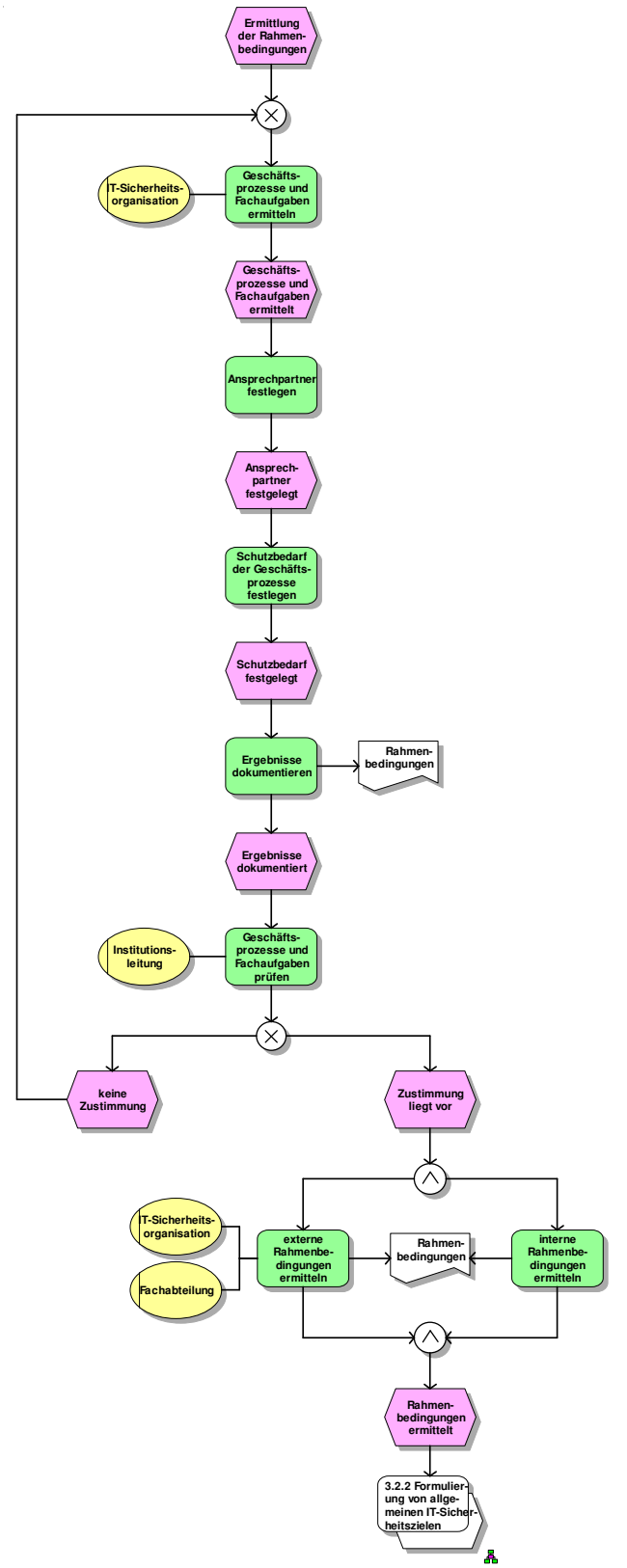
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Funktionsübersicht

eEPK: 3.1 Übernahme der Verantwortung durch die Leitungsebene



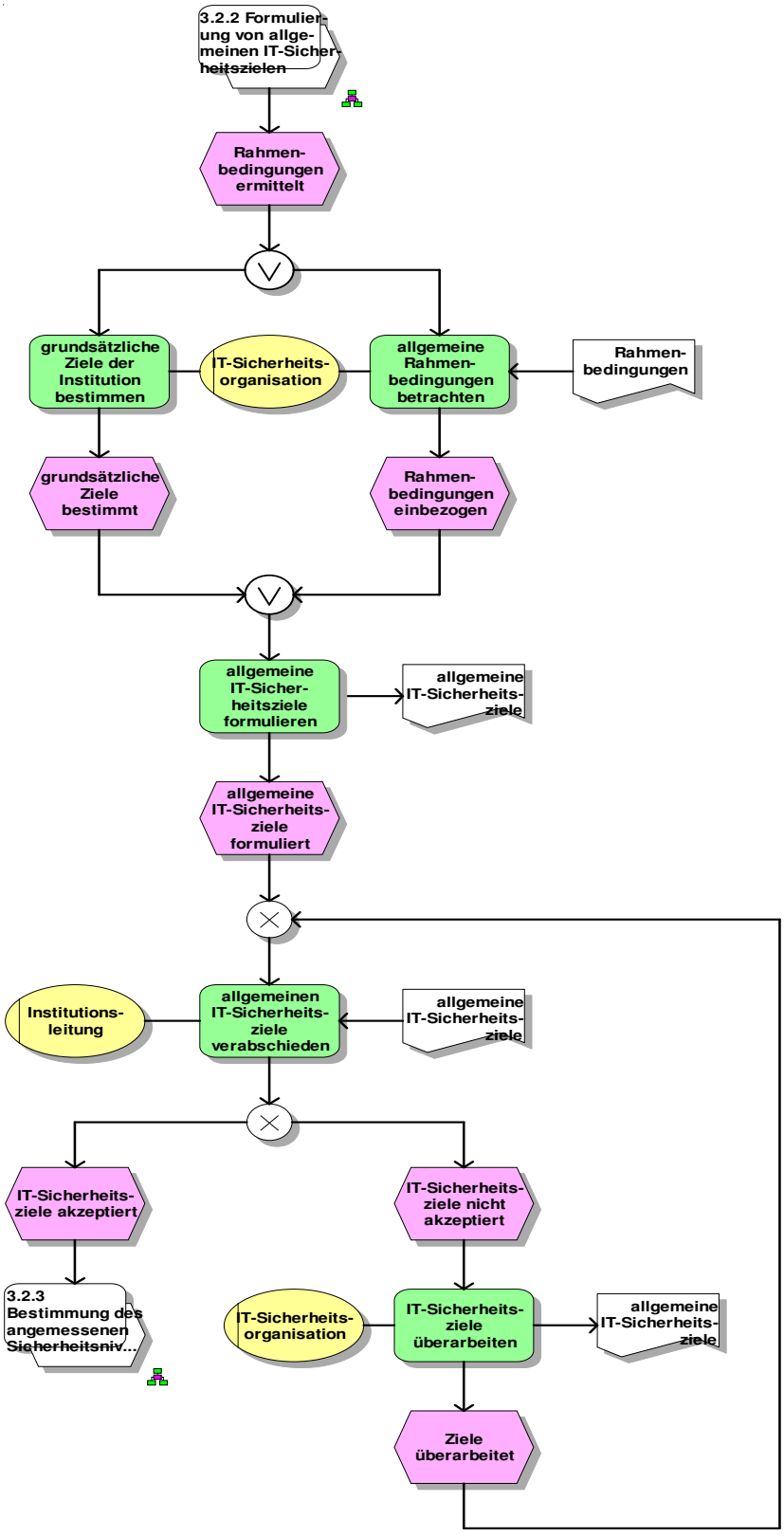
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.2.1 Ermittlung der Rahmenbedingungen



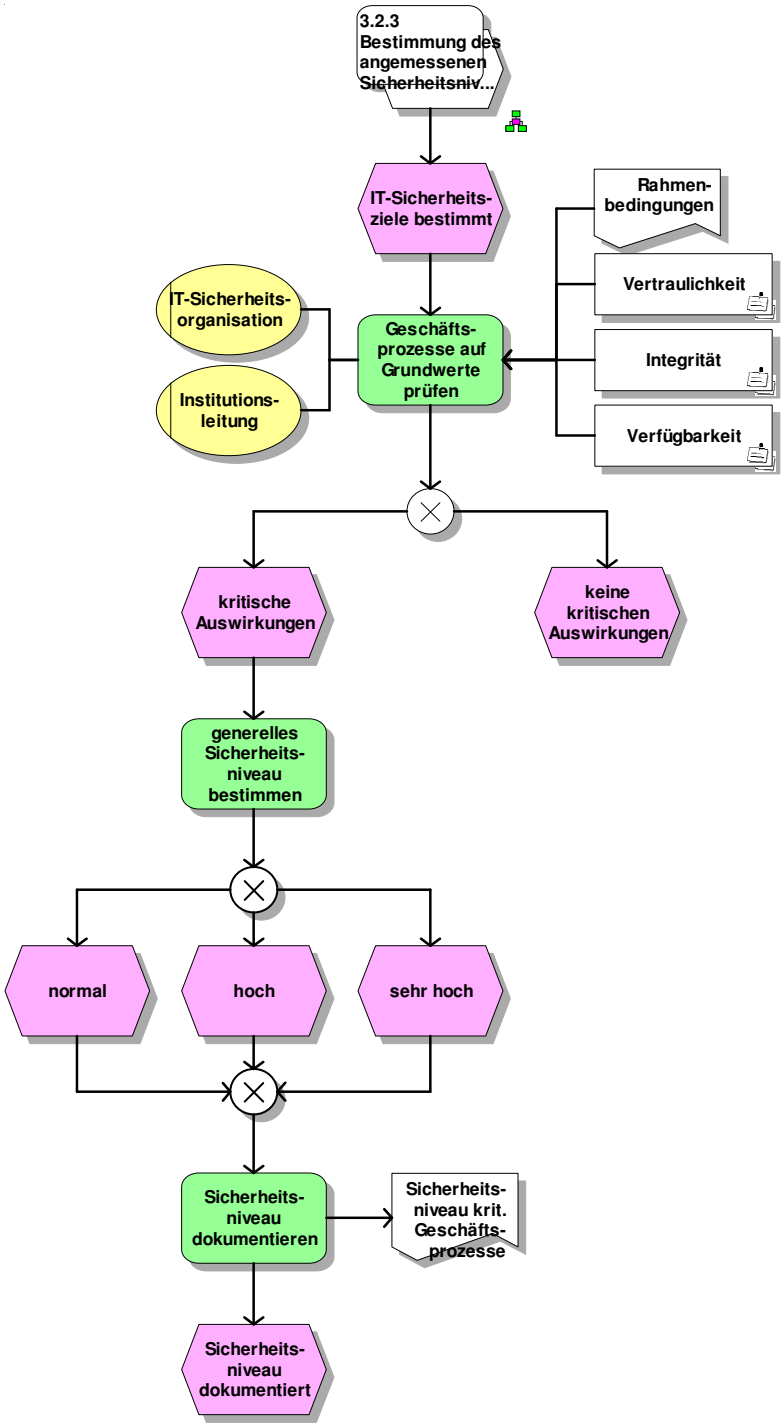
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.2.2 Formulierung von allgemeinen IT-Sicherheitszielen



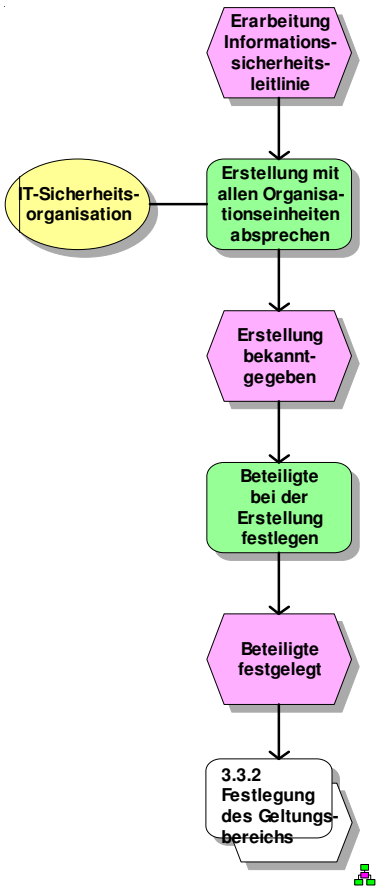
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.2.3 Bestimmung des angemessenen Sicherheitsniveaus



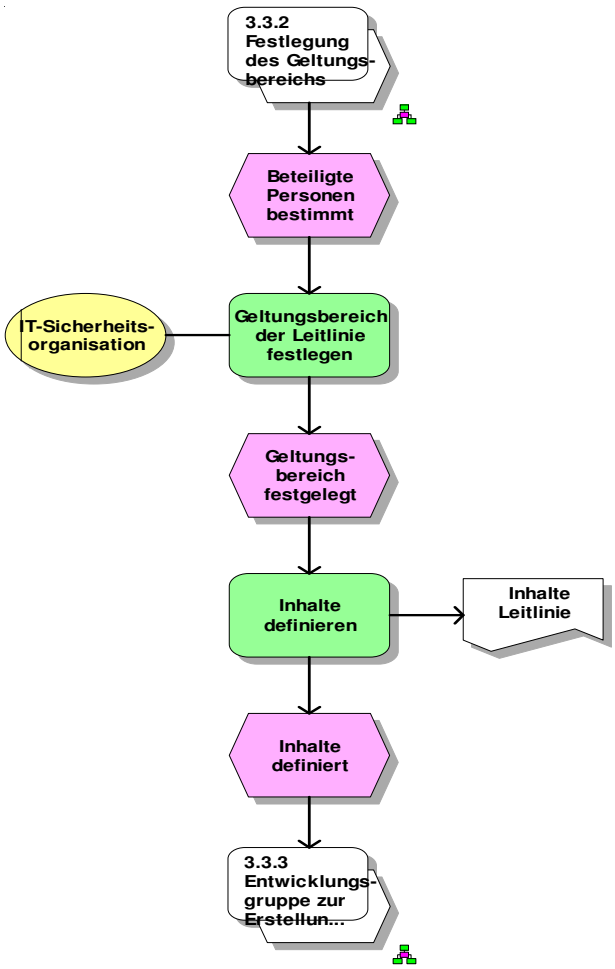
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.3.1 Verantwortung der Behörden- bzw. Unternehmensleitung für die Leitlinie



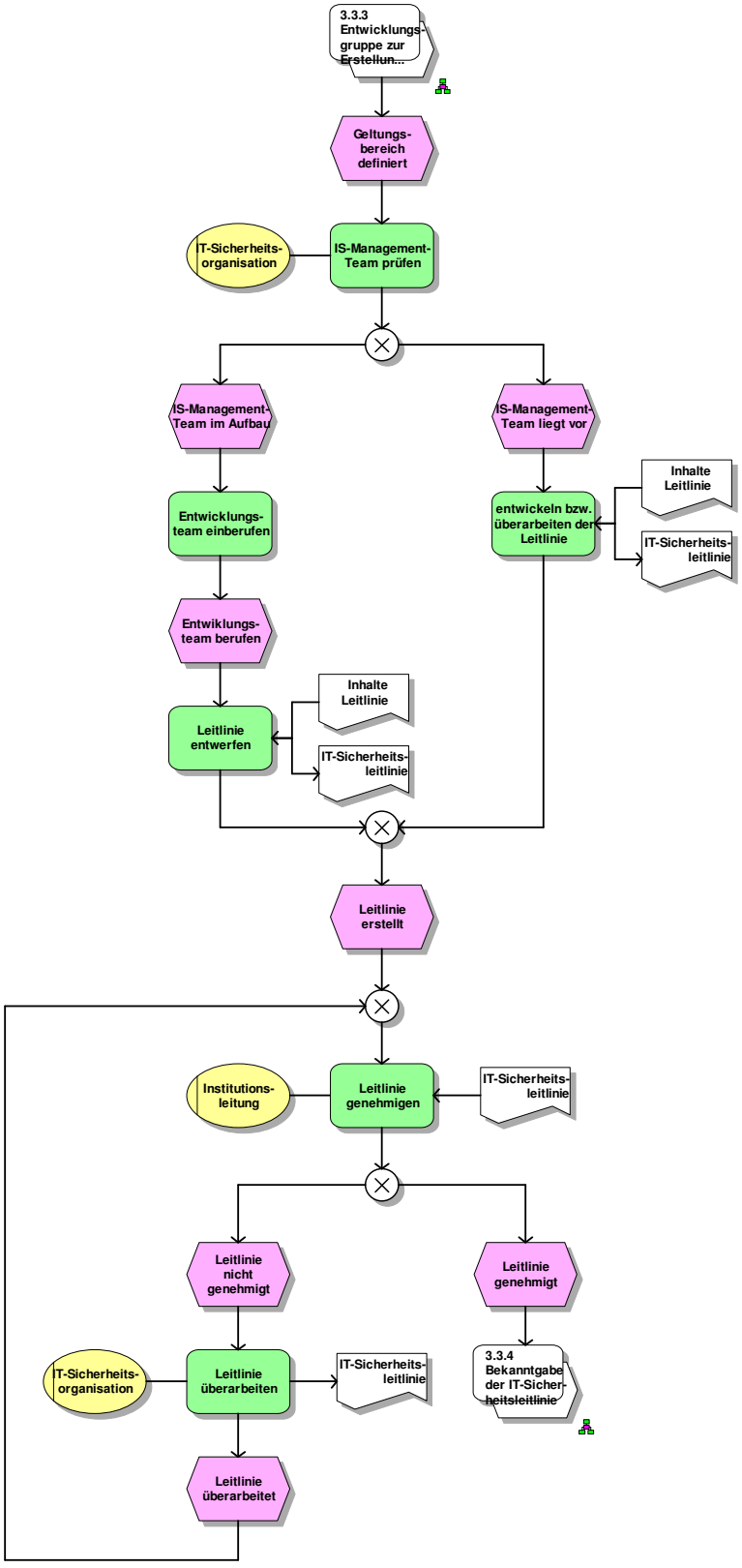
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.3.2 Festlegung des Geltungsbereichs



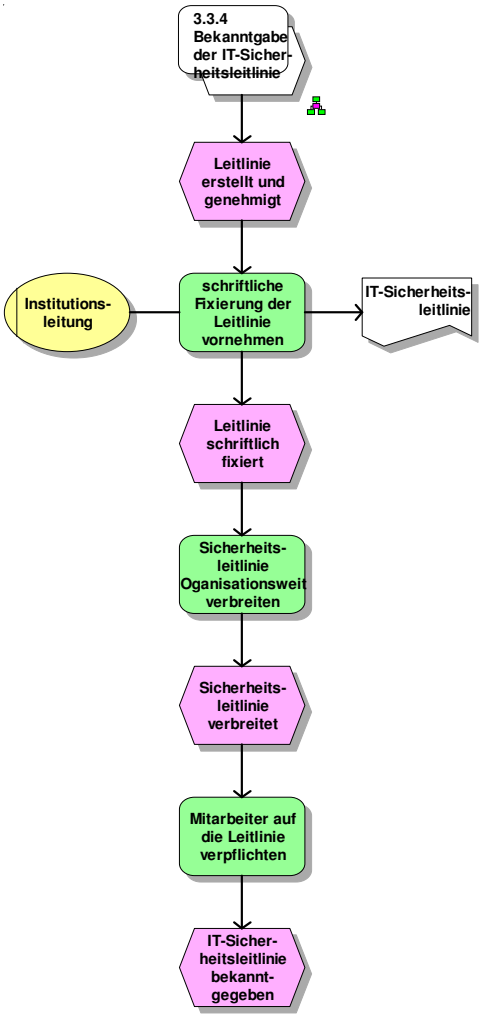
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.3.3 Entwicklungsgruppe zur Erstellung einberufen



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

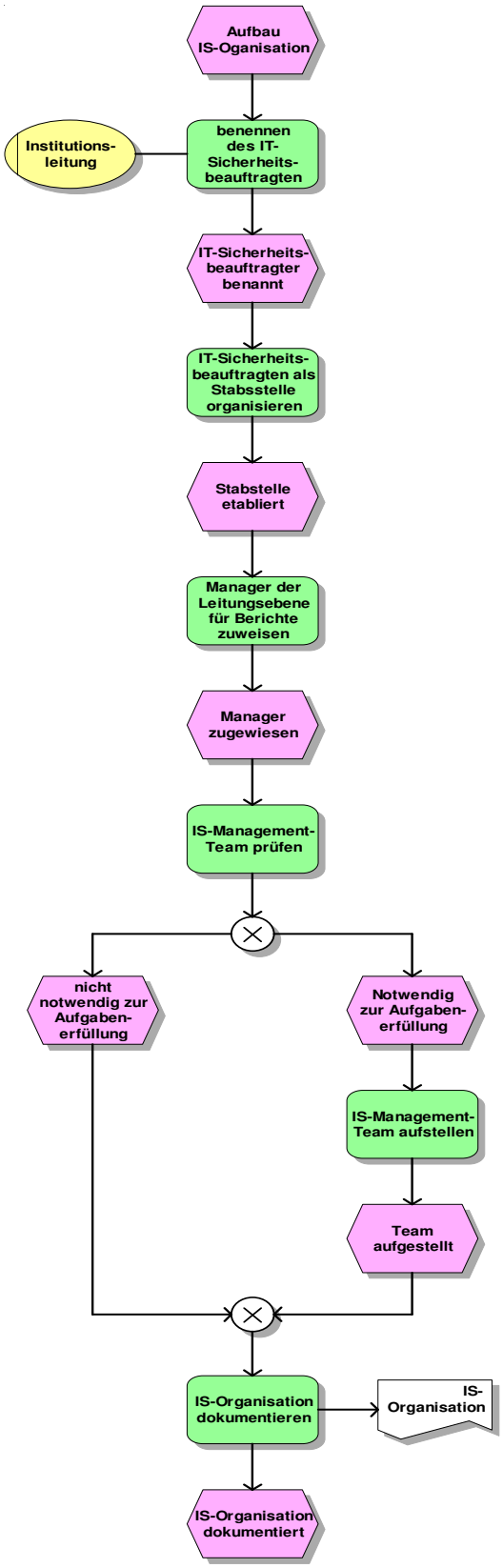
eEPK: 3.3.4 Bekanntgabe der IT-Sicherheitsleitlinie



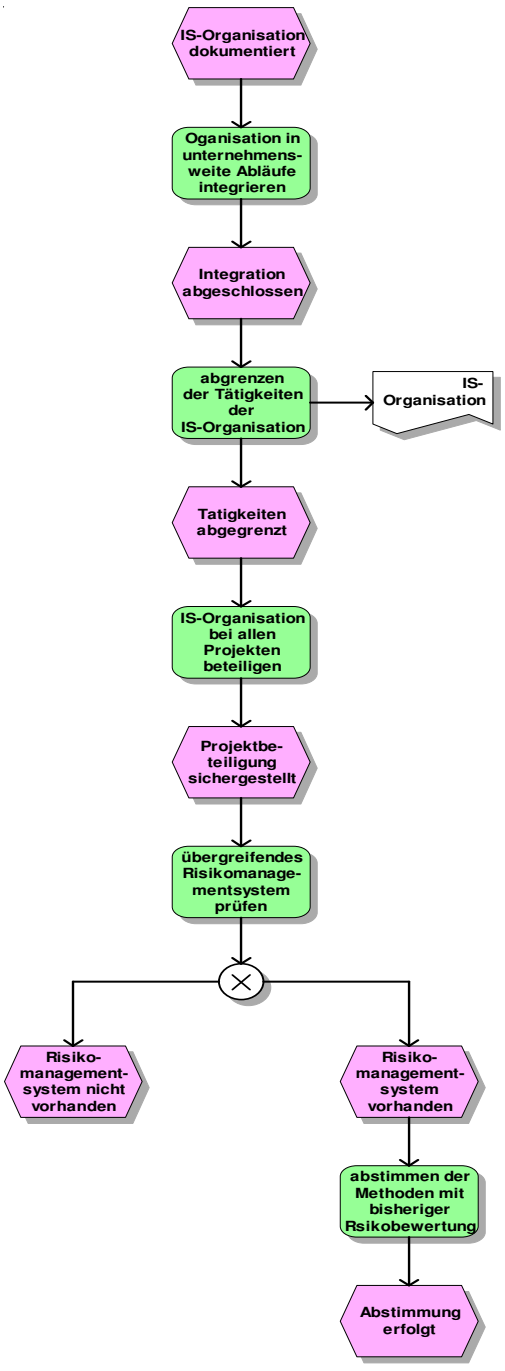
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.4 Organisation des Sicherheitsprozesses

(Teil 1 von 2)

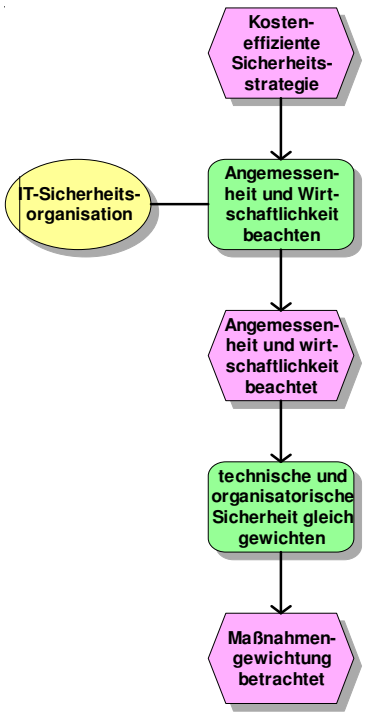


(Teil 2 von 2)



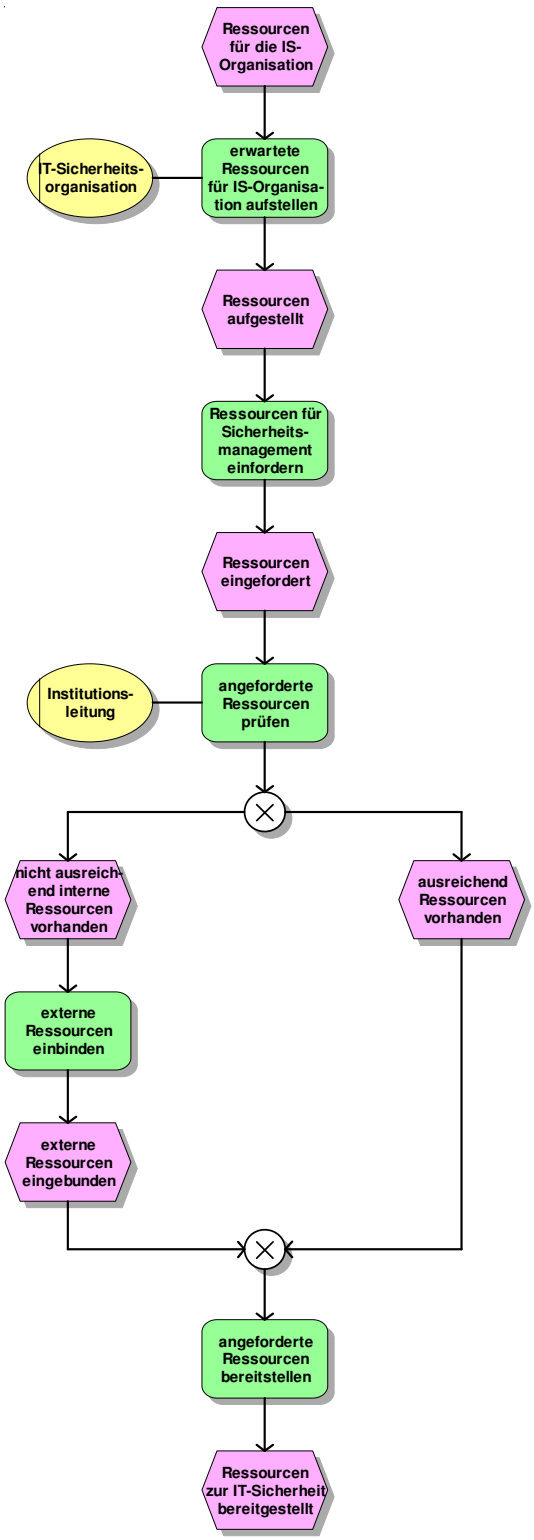
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.5.1 Kosteneffiziente Sicherheitsstrategie



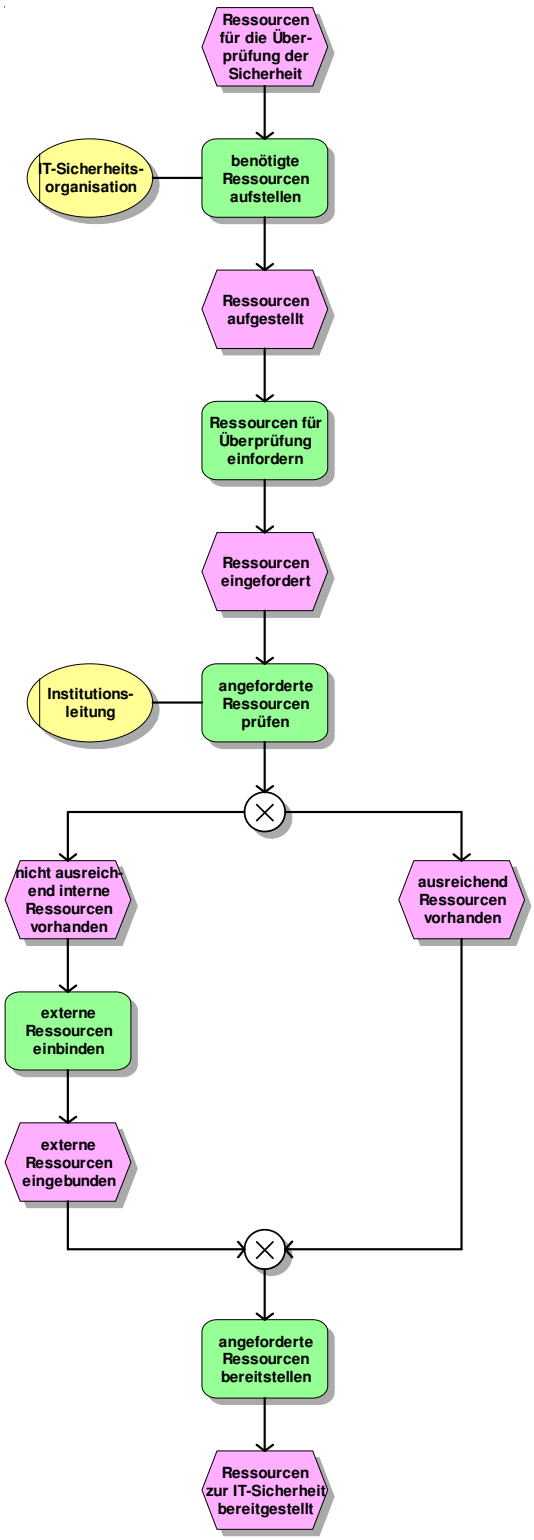
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.5.2 Ressourcen für die IS-Organisation



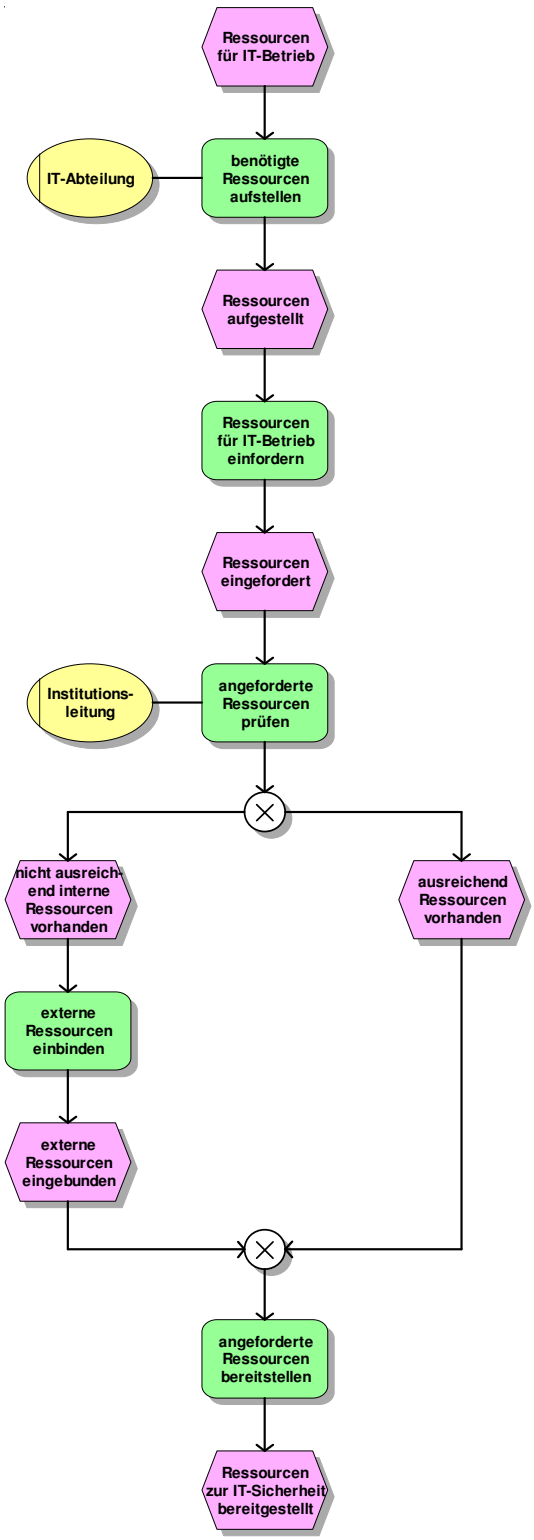
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.5.3 Ressourcen für die Überprüfung der Sicherheit



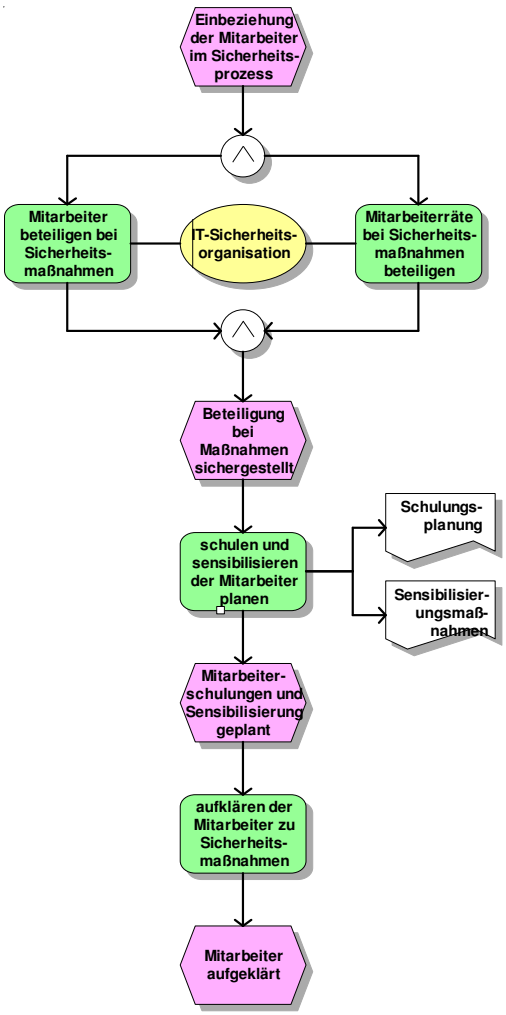
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.5.4 Ressourcen für den IT-Betrieb



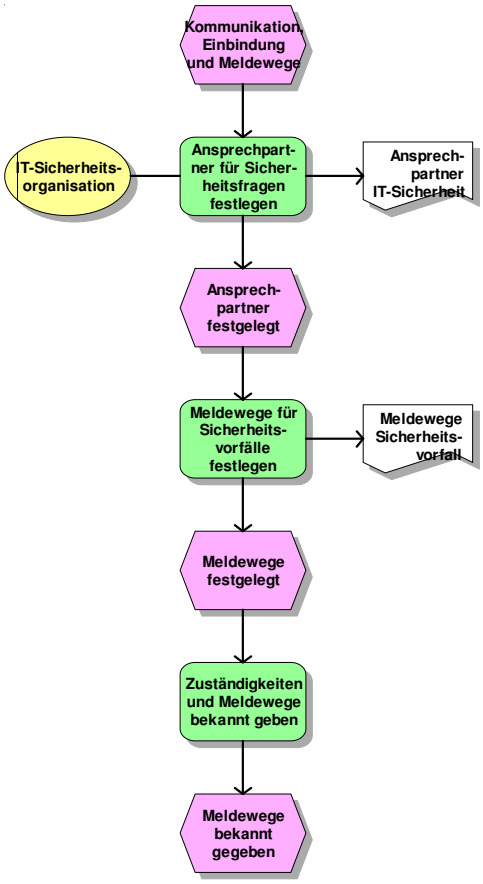
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.6.1 Schulung und Sensibilisierung



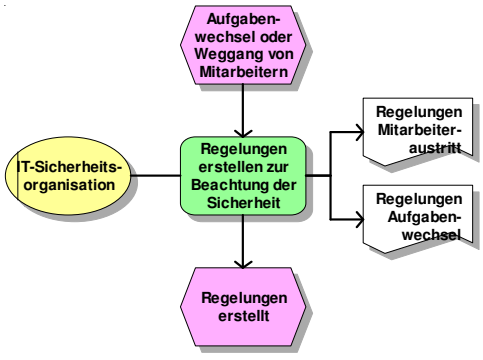
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

eEPK: 3.6.2 Kommunikation, Einbindung und Meldewege



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

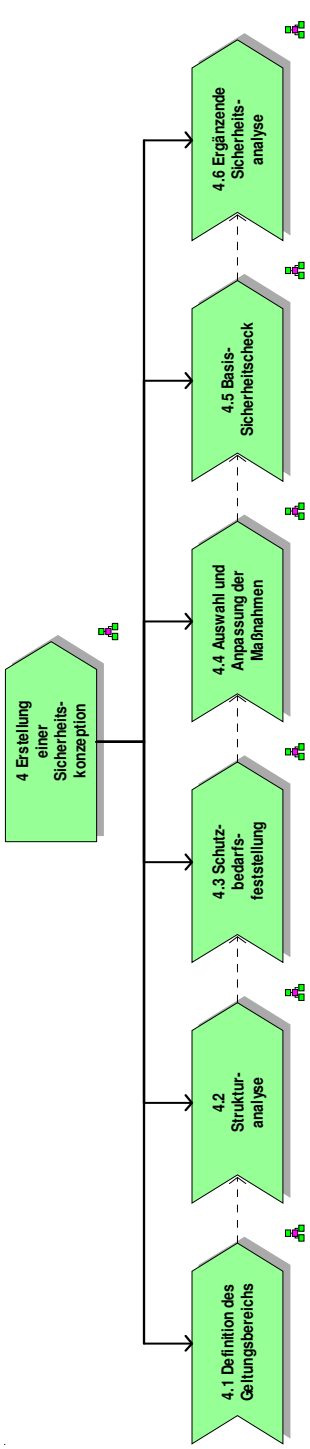
eEPK: 3.6.3 Aufgabenwechsel oder Weggang von Mitarbeitern



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\3 Initiierung des Sicherheitsprozesses\Arbeitsschritte

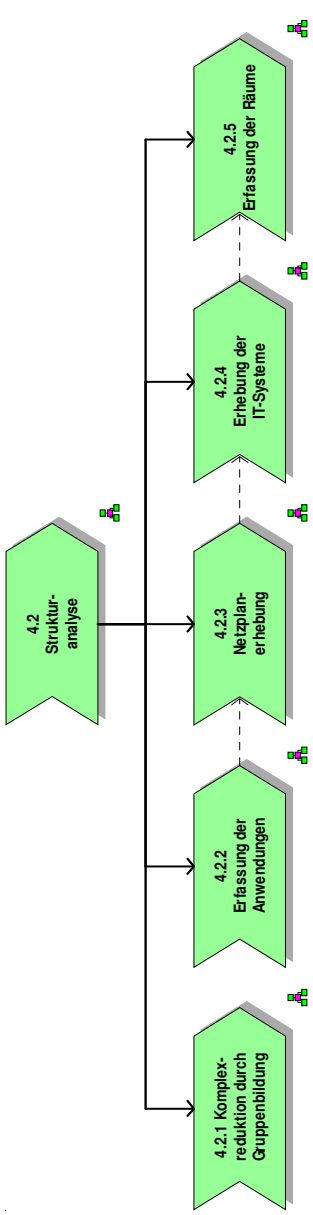
4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz

WKD: 4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz



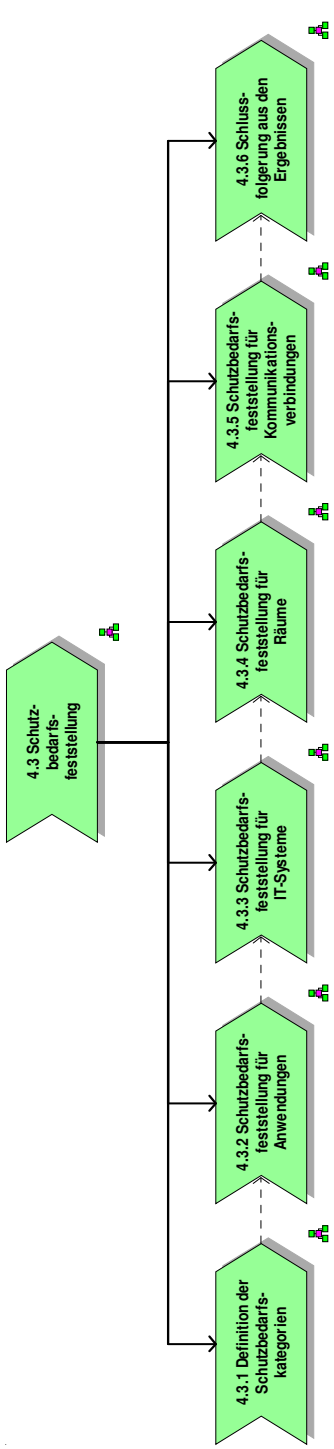
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz

WKD: 4.2 Strukturanalyse



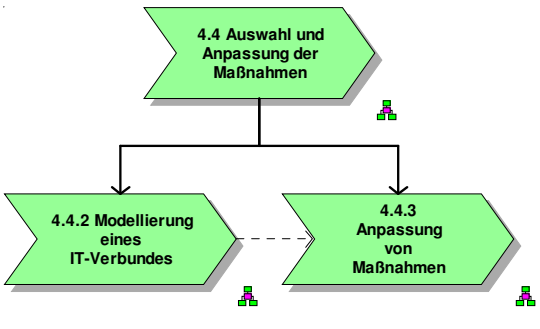
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Managementbetrachtung

WKD: 4.3 Schutzbedarfsfeststellung



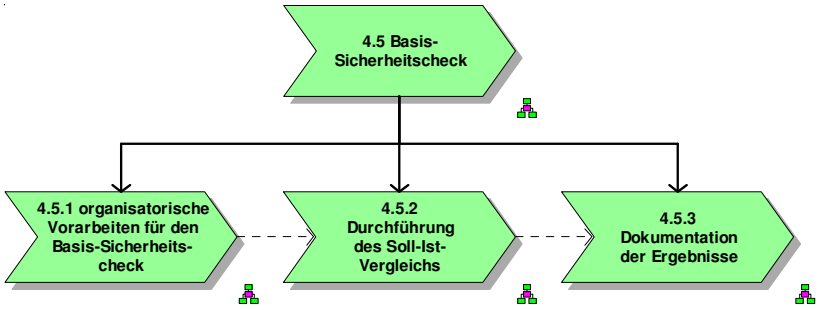
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Managementbetrachtung

WKD: 4.4 Auswahl und Anpassung der Maßnahmen



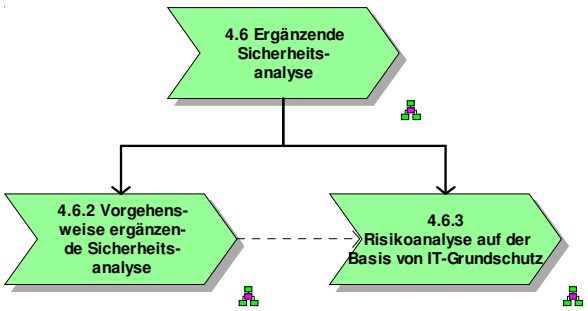
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Managementbetrachtung

WKD: 4.5 Basis-Sicherheitscheck



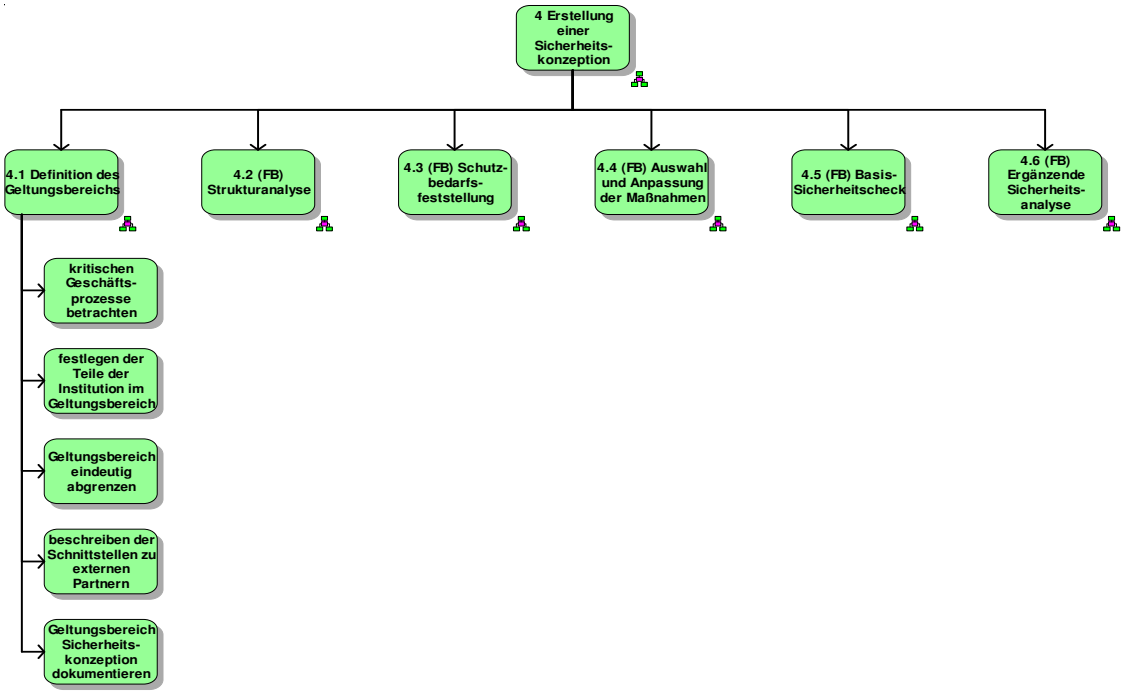
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Managementbetrachtung

WKD: 4.6 Ergänzende Sicherheitsanalyse



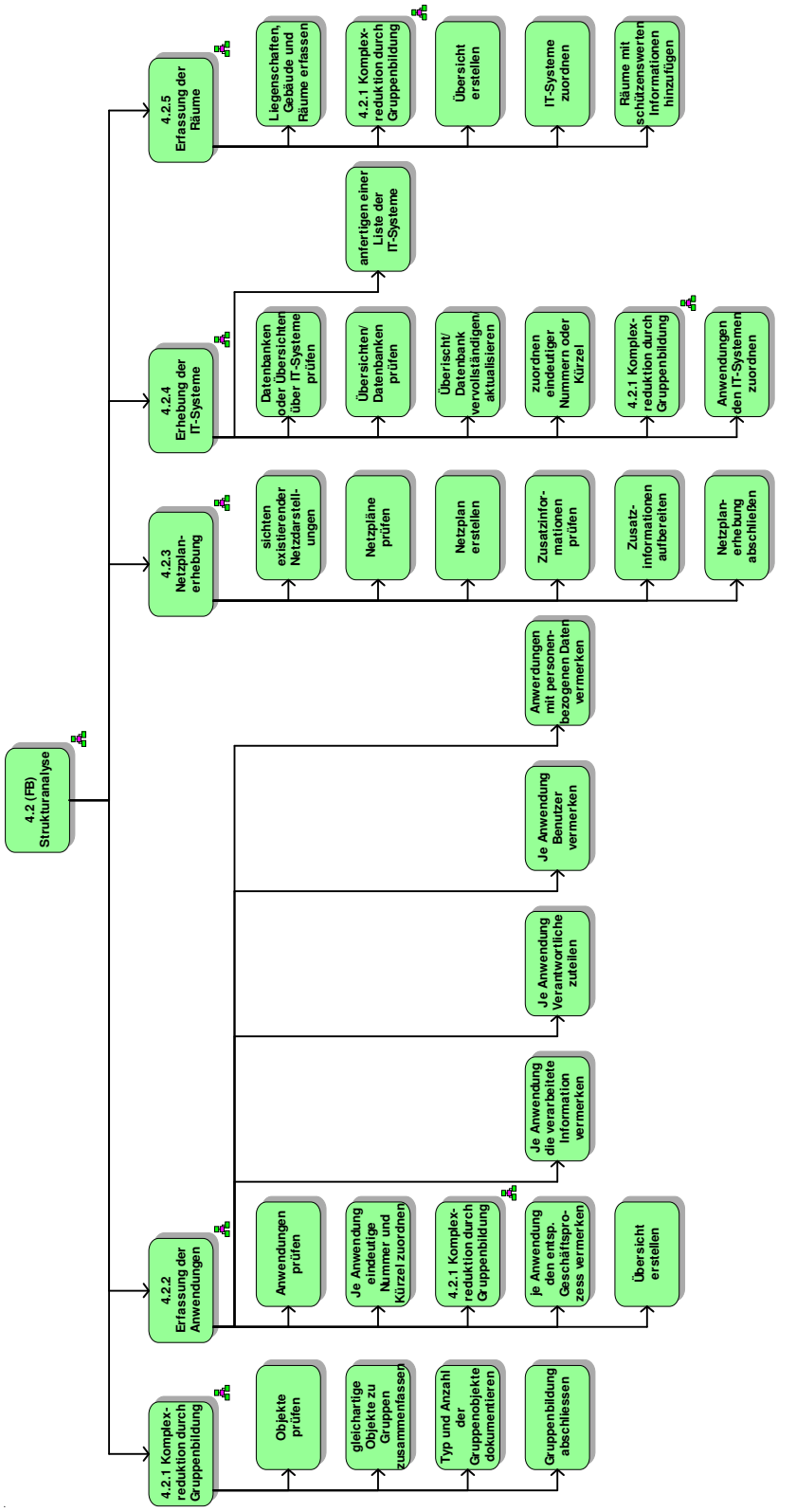
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Managementbetrachtung

Funktionsbaum: 4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz



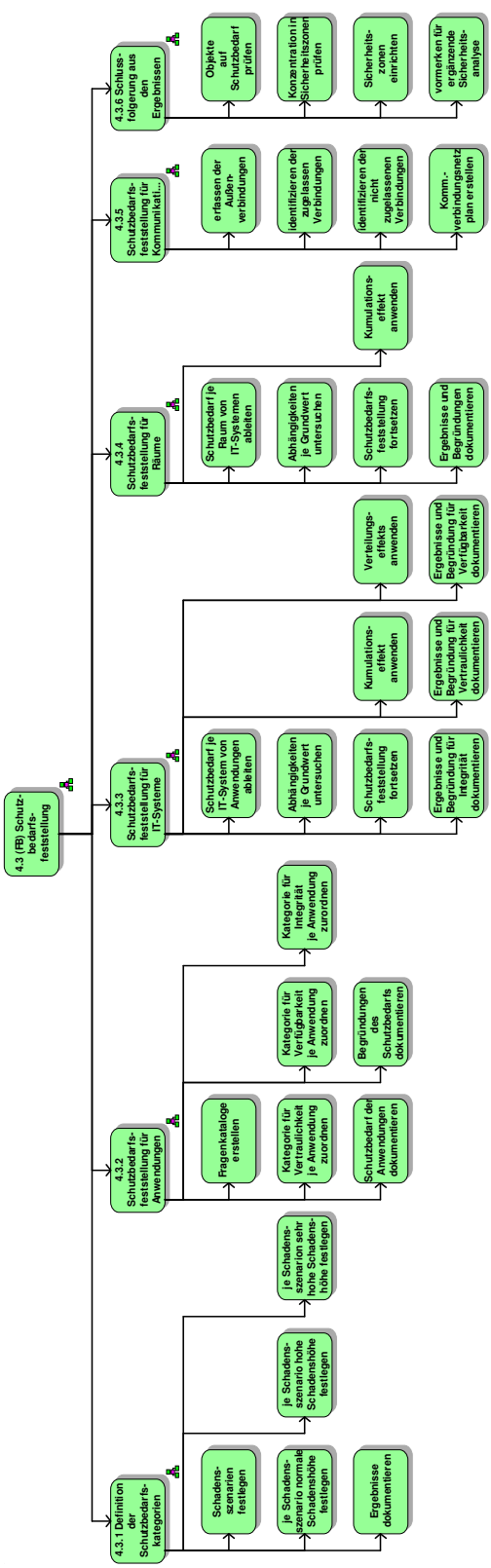
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Funktionsübersicht

Funktionsbaum: 4.2 (FB) Strukturanalyse



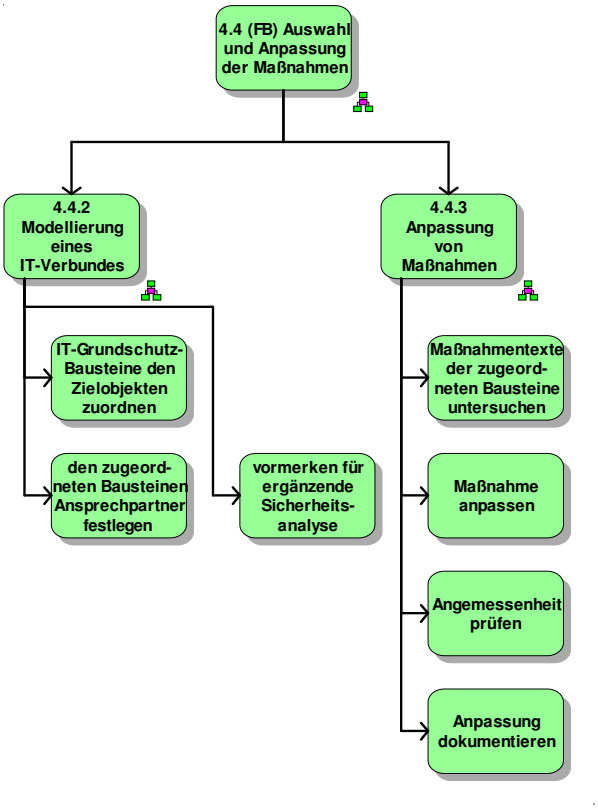
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Funktionsübersicht

Funktionsbaum: 4.3 (FB) Schutzbedarfsfeststellung



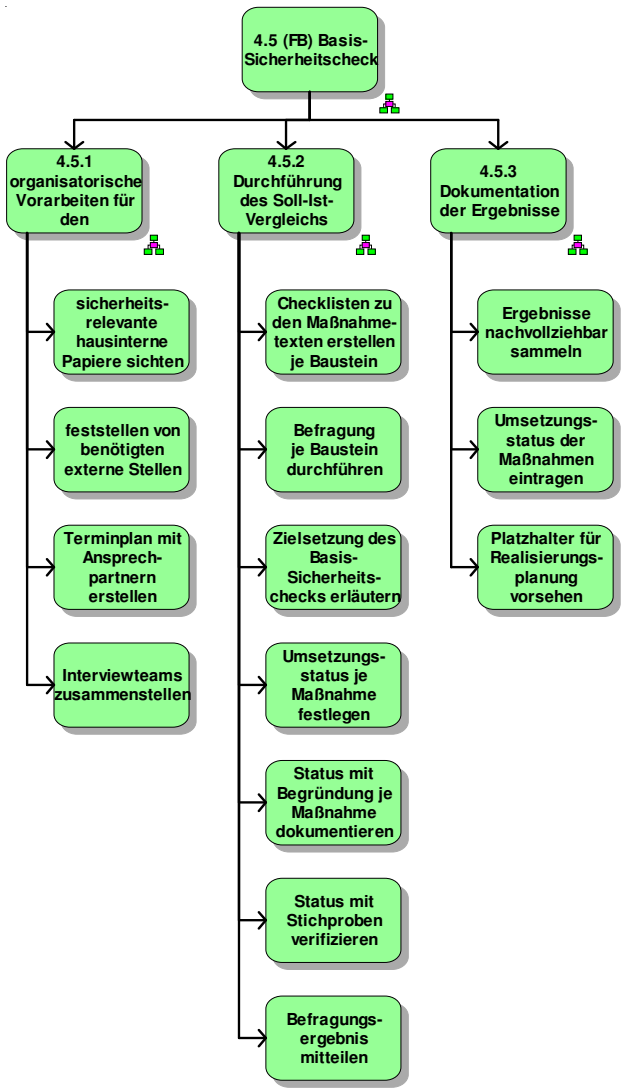
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Funktionsübersicht

Funktionsbaum: 4.4 (FB) Auswahl und Anpassung der Maßnahmen



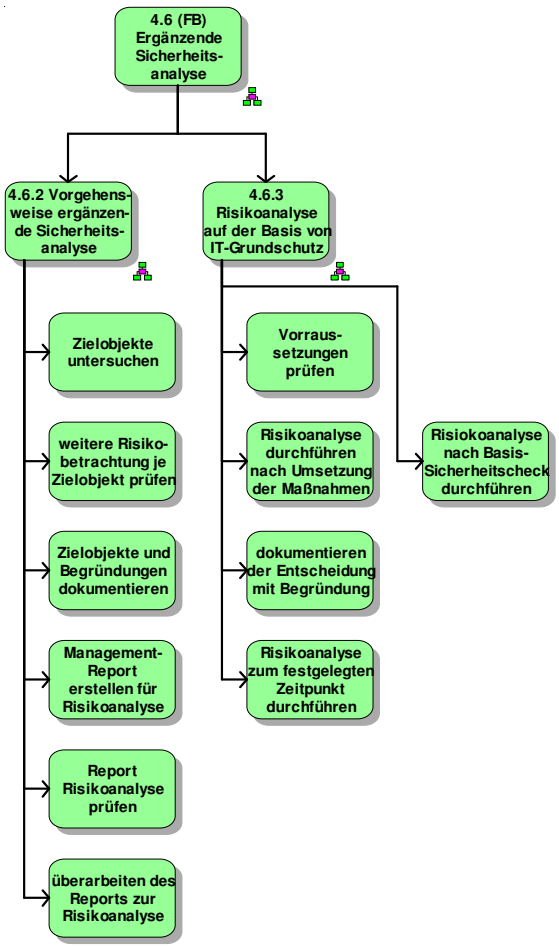
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Funktionsübersicht

Funktionsbaum: 4.5 (FB) Basis-Sicherheitscheck



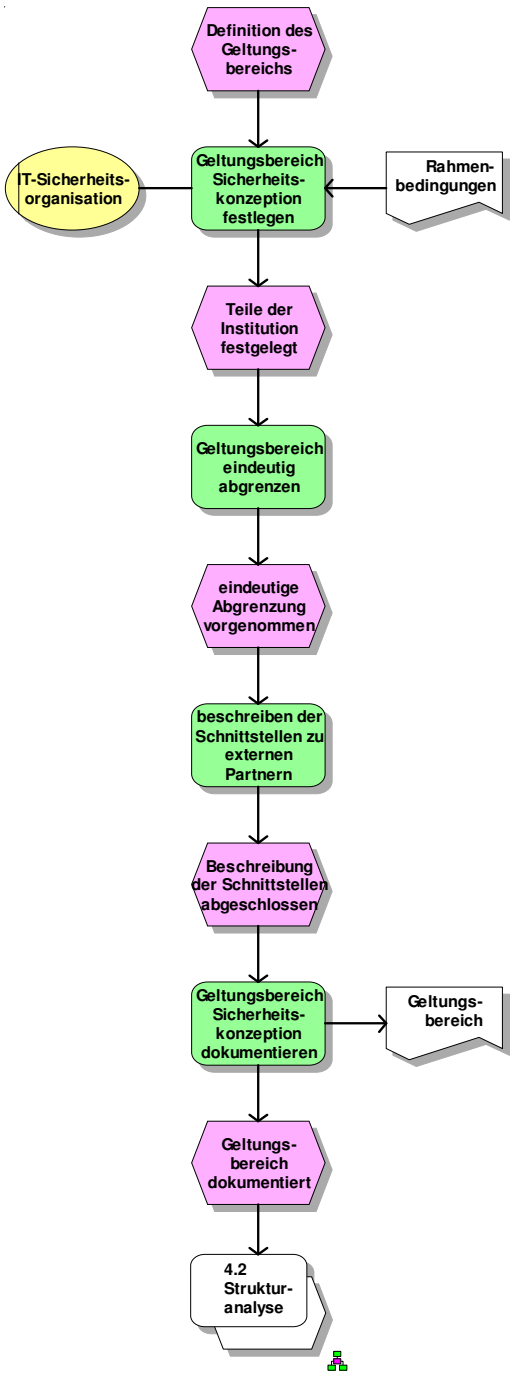
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Funktionsübersicht

Funktionsbaum: 4.6 (FB) Ergänzende Sicherheitsanalyse



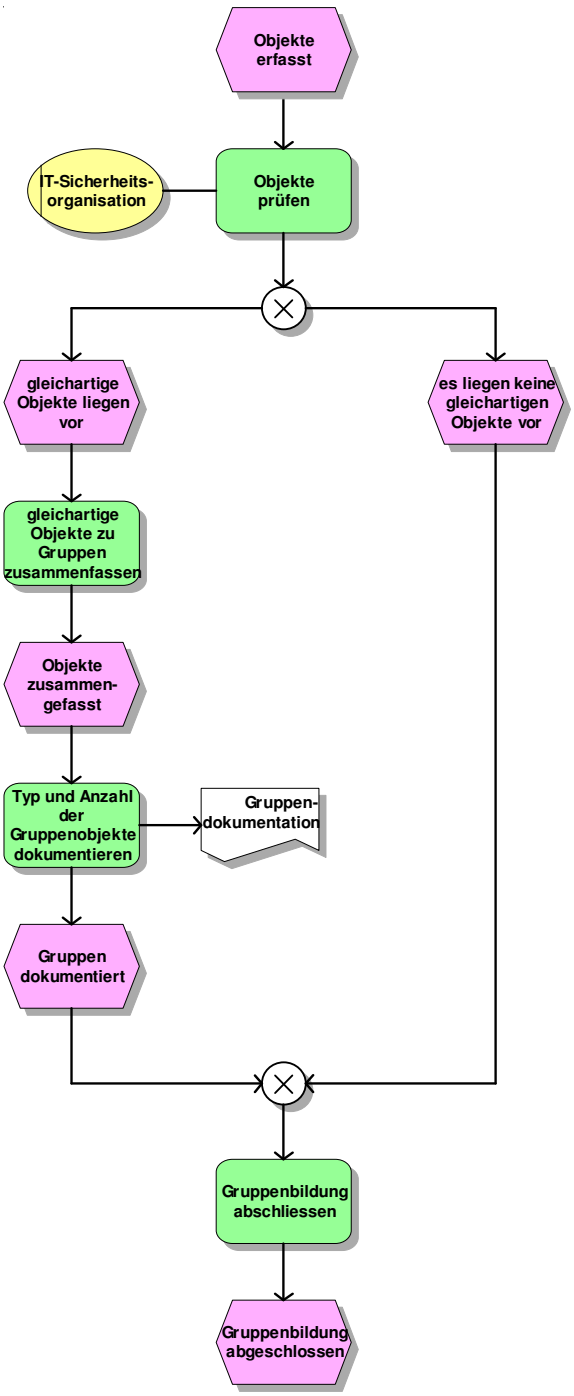
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Funktionsübersicht

eEPK: 4.1 Definition des Geltungsbereichs



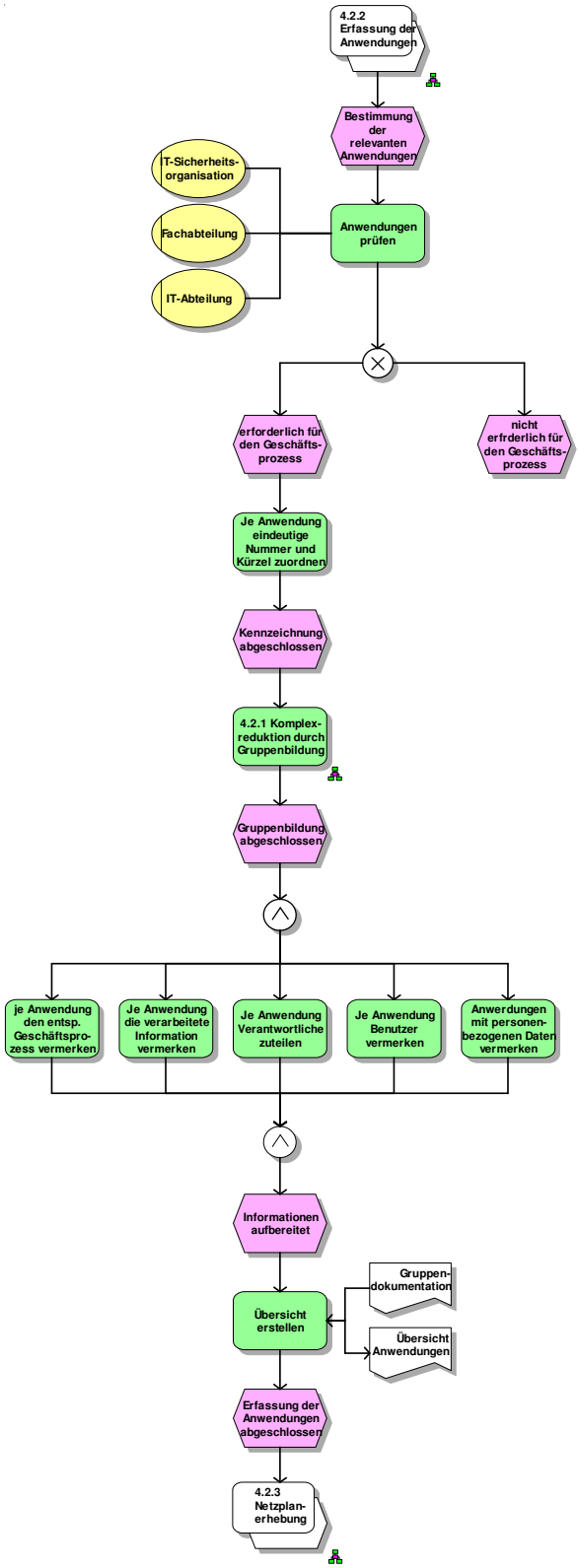
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.2.1 Komplexreduktion durch Gruppenbildung



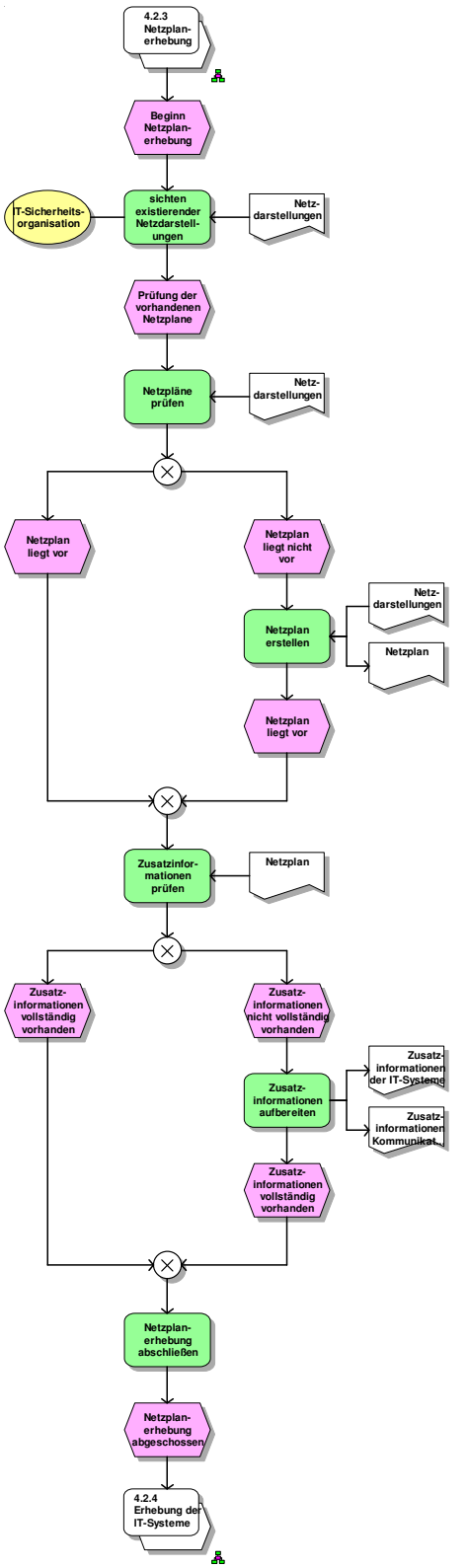
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.2.2 Erfassung der Anwendungen



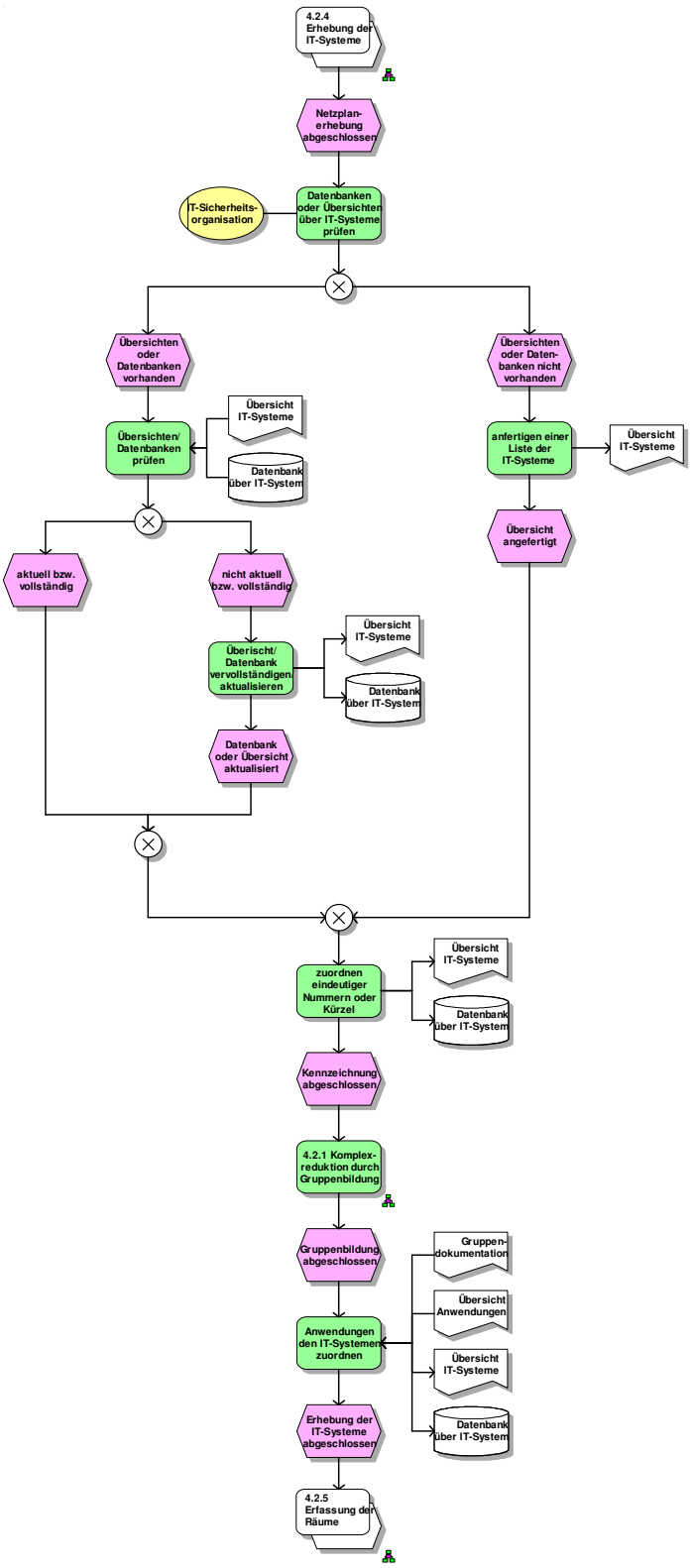
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.2.3 Netzplanerhebung



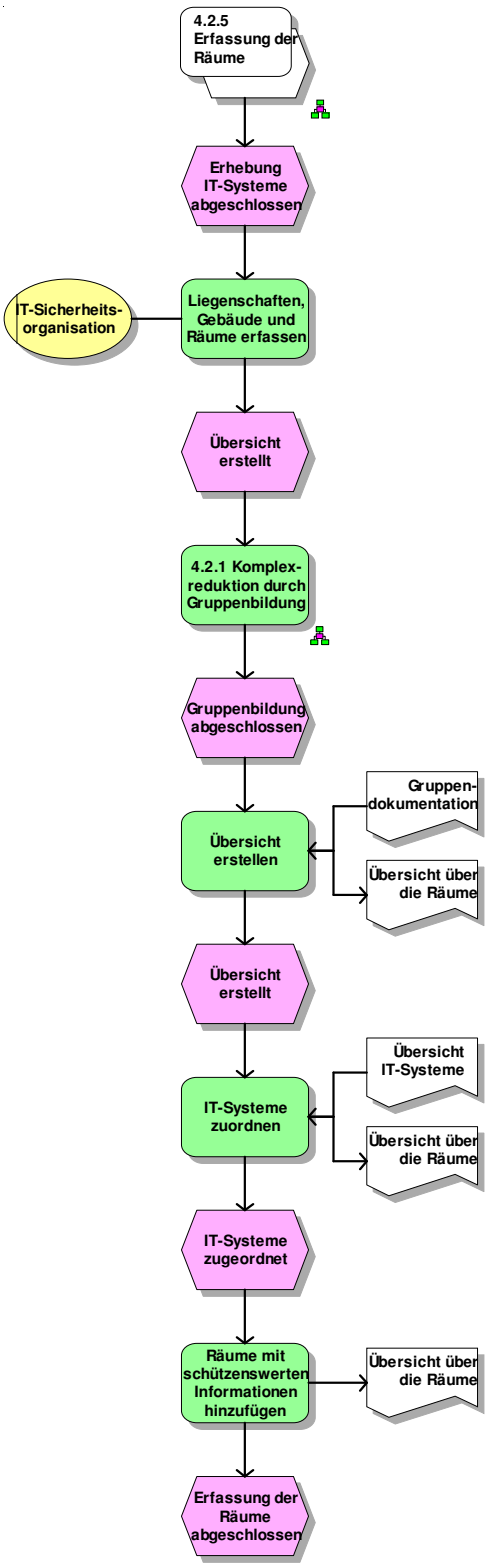
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.2.4 Erhebung der IT-Systeme



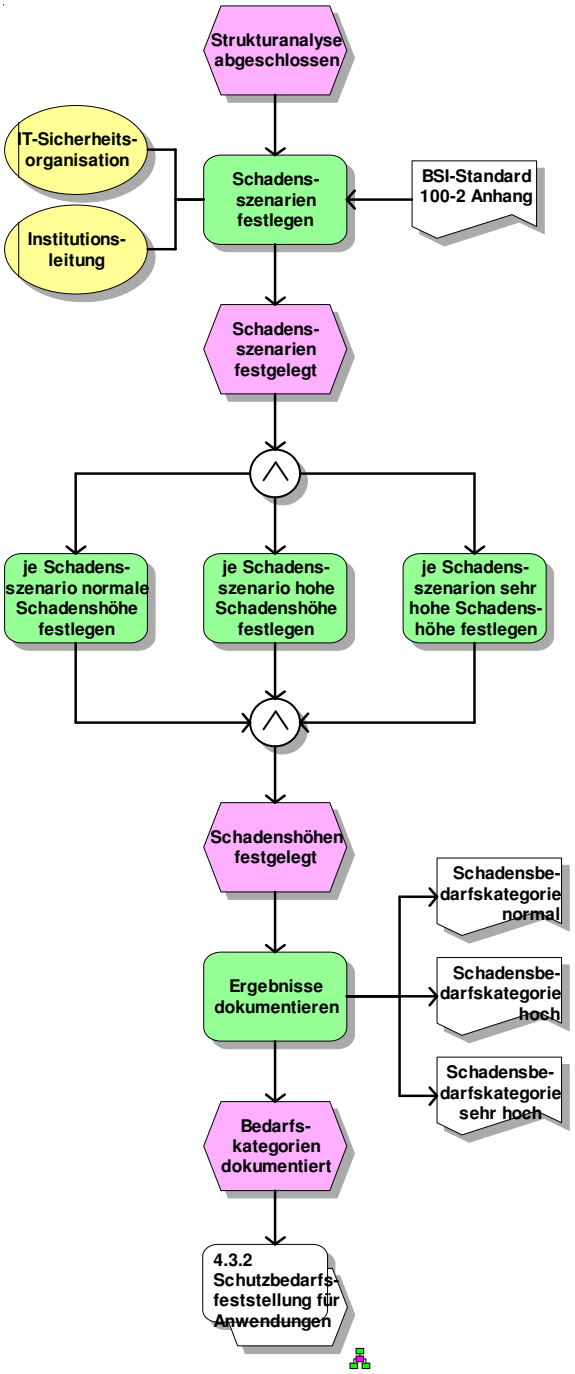
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.2.5 Erfassung der Räume



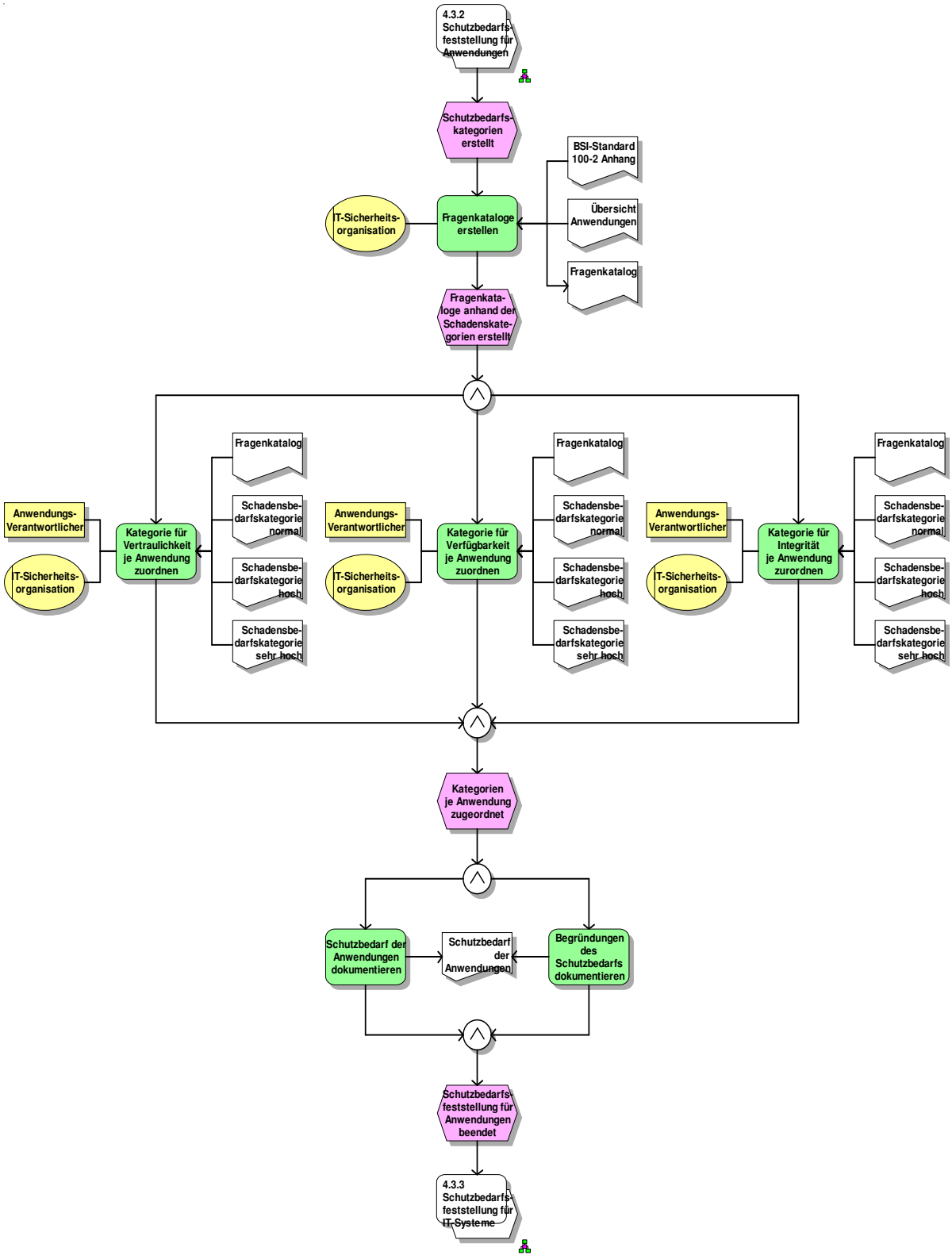
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.3.1 Definition der Schutzbedarfskategorien



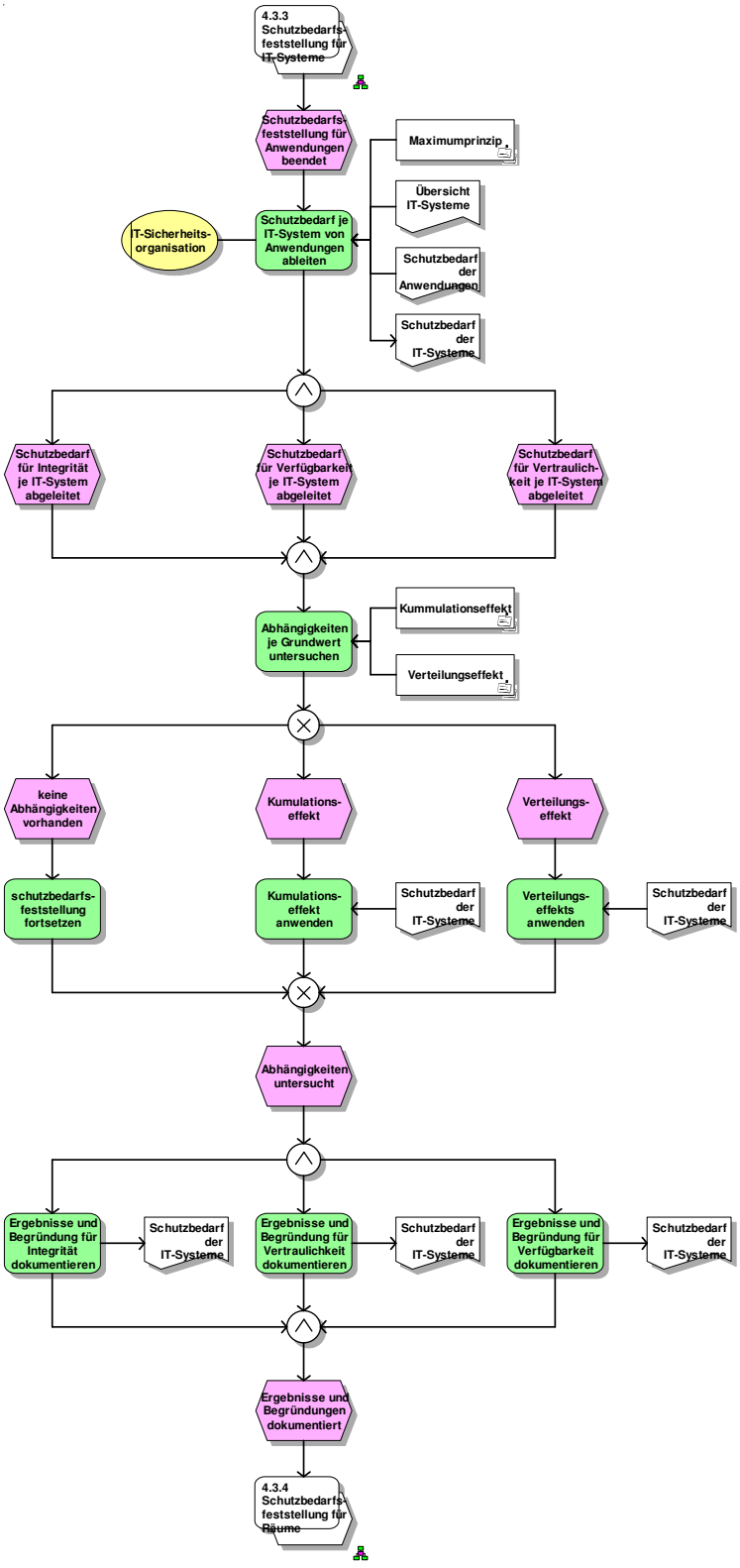
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.3.2 Schutzbedarfsfeststellung für Anwendungen



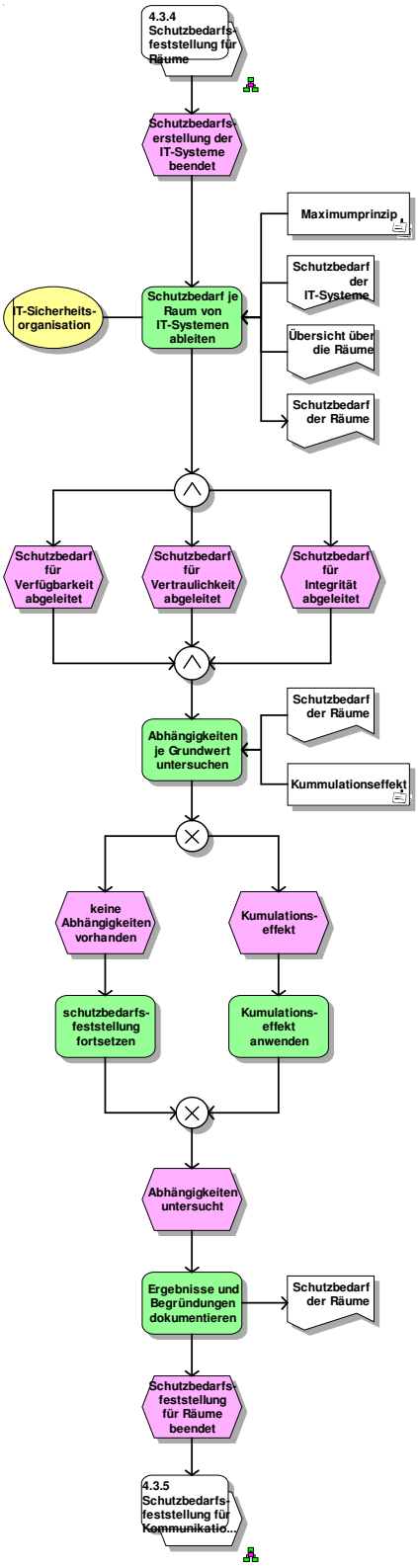
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.3.3 Schutzbedarfsfeststellung für IT-Systeme



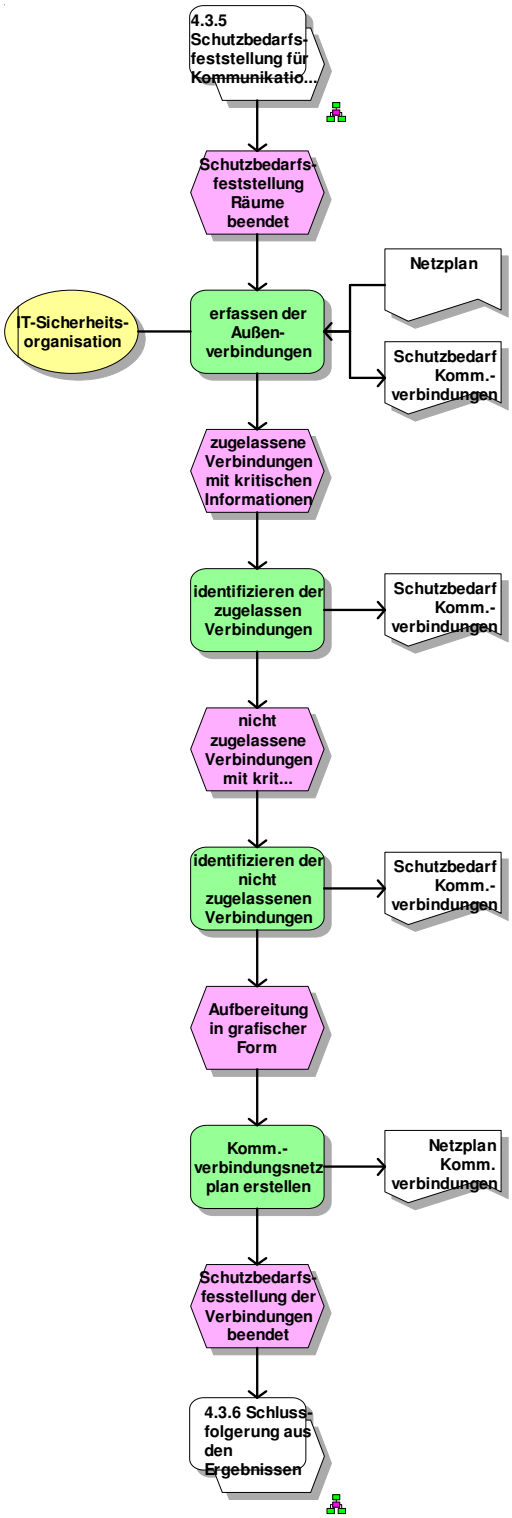
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.3.4 Schutzbedarfsfeststellung für Räume



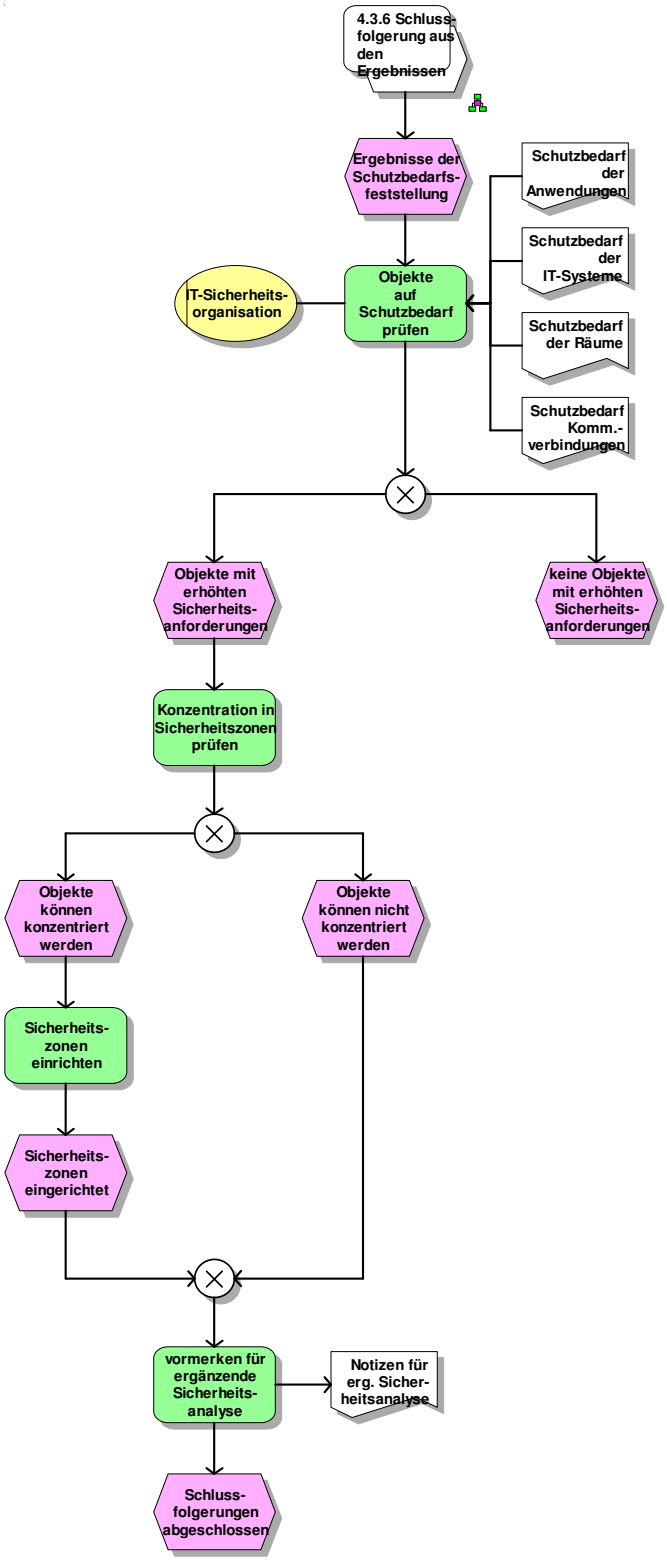
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.3.5 Schutzbedarfsfeststellung für Kommunikationsverbindungen



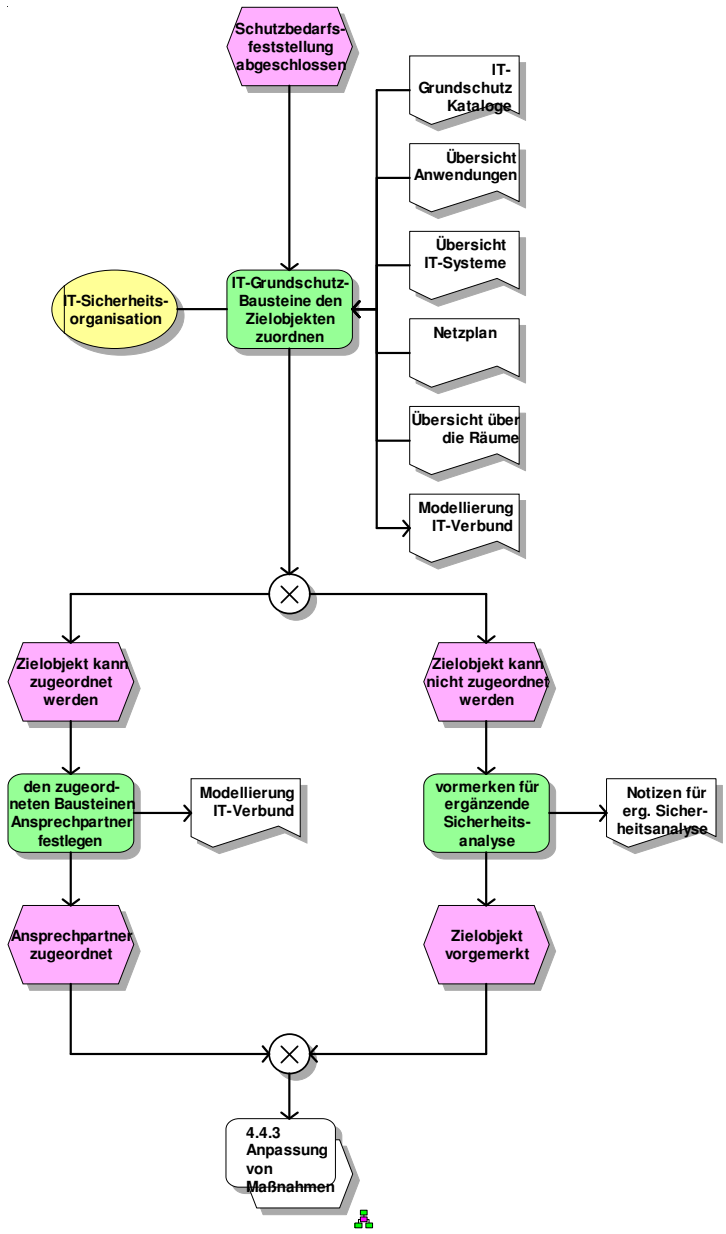
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.3.6 Schlussfolgerung aus den Ergebnissen



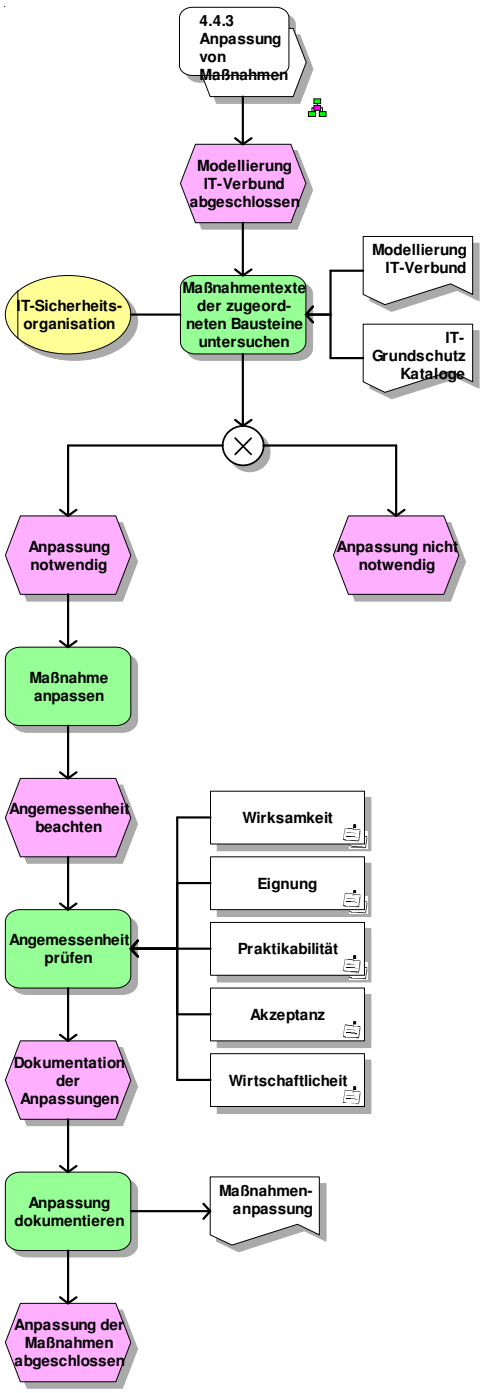
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.4.2 Modellierung eines IT-Verbundes



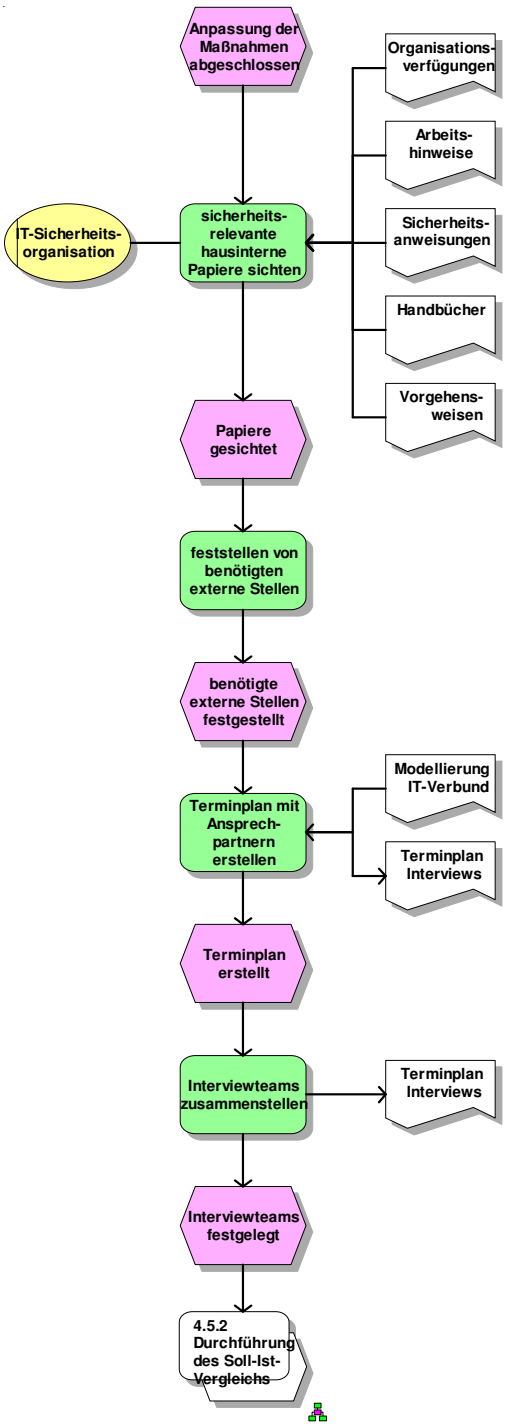
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.4.3 Anpassung von Maßnahmen



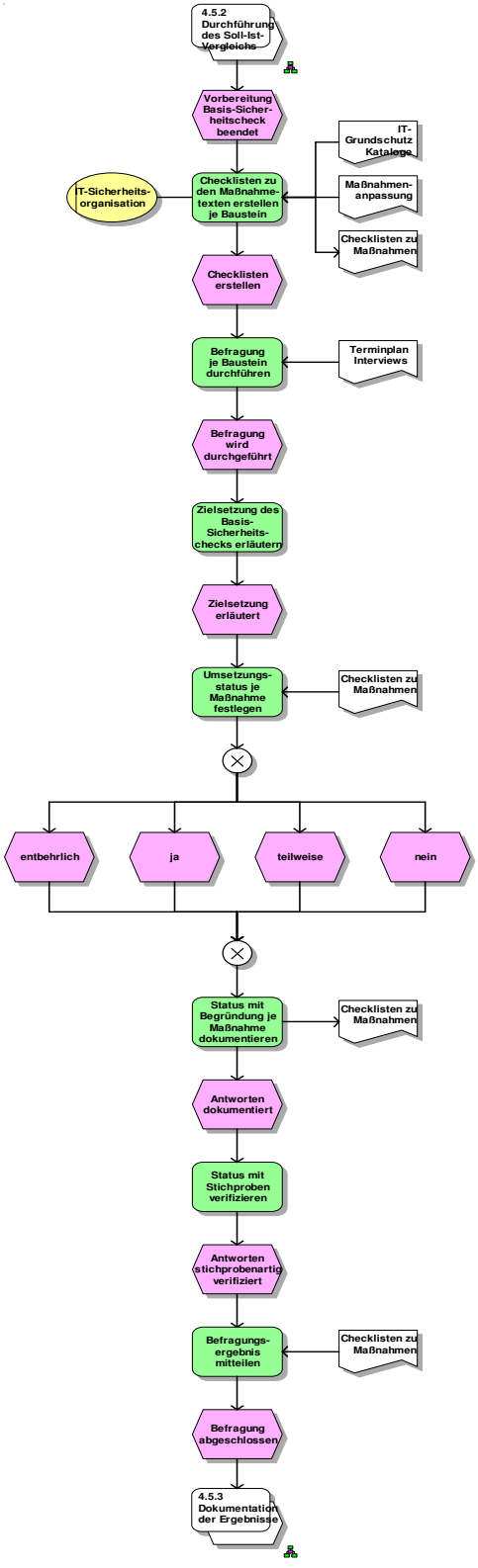
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.5.1 organisatorische Vorarbeiten für den Basis-Sicherheitscheck



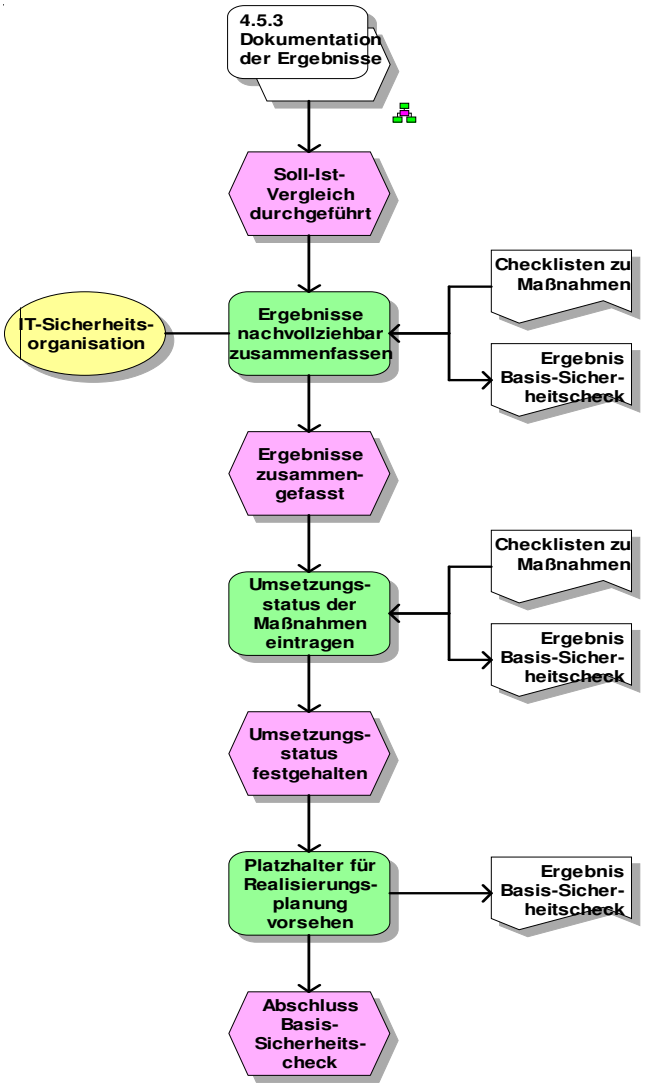
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.5.2 Durchführung des Soll-Ist-Vergleichs



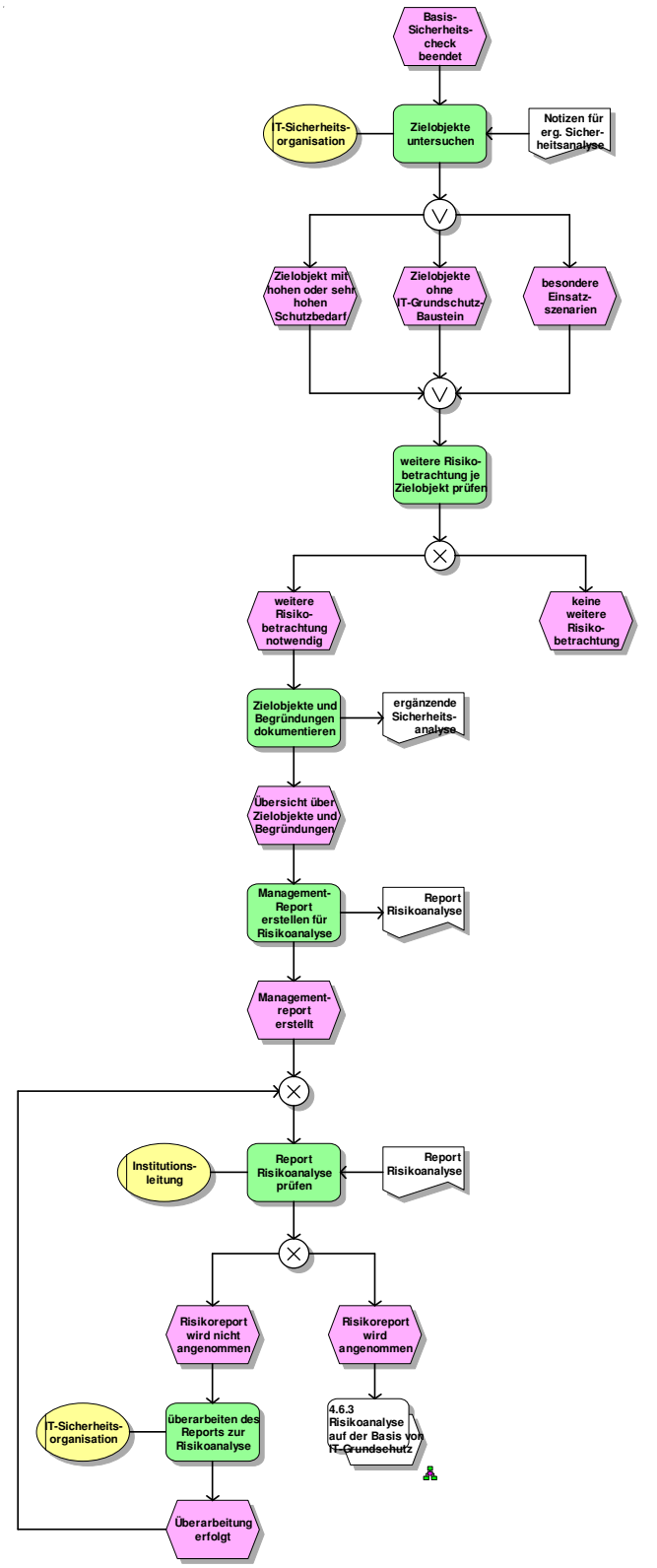
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.5.3 Dokumentation der Ergebnisse



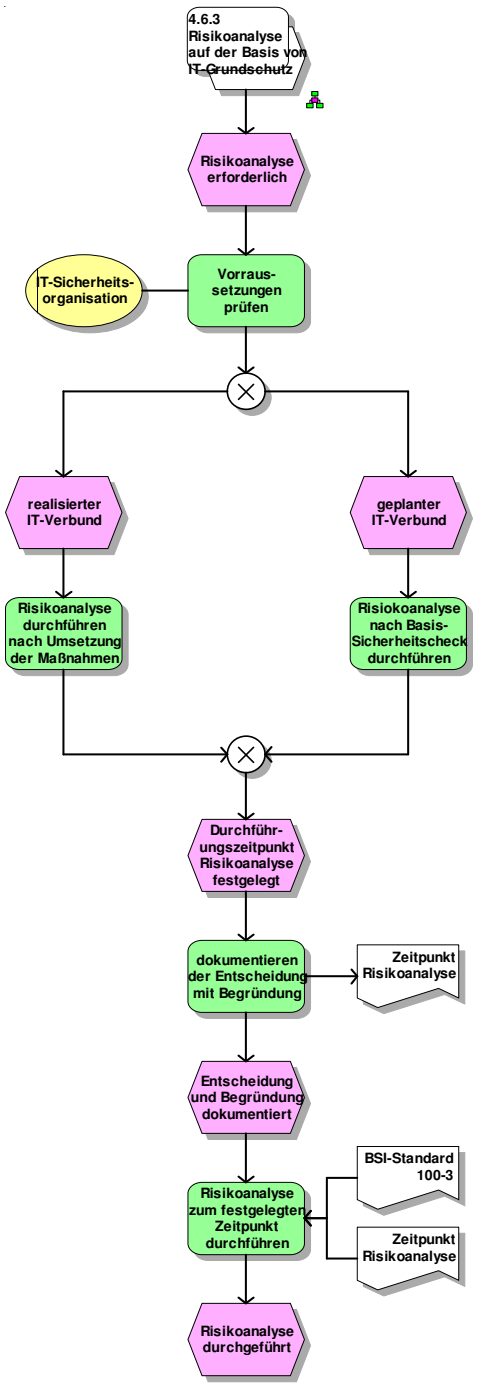
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

eEPK: 4.6.2 Vorgehensweise zur ergänzenden Sicherheitsanalyse



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

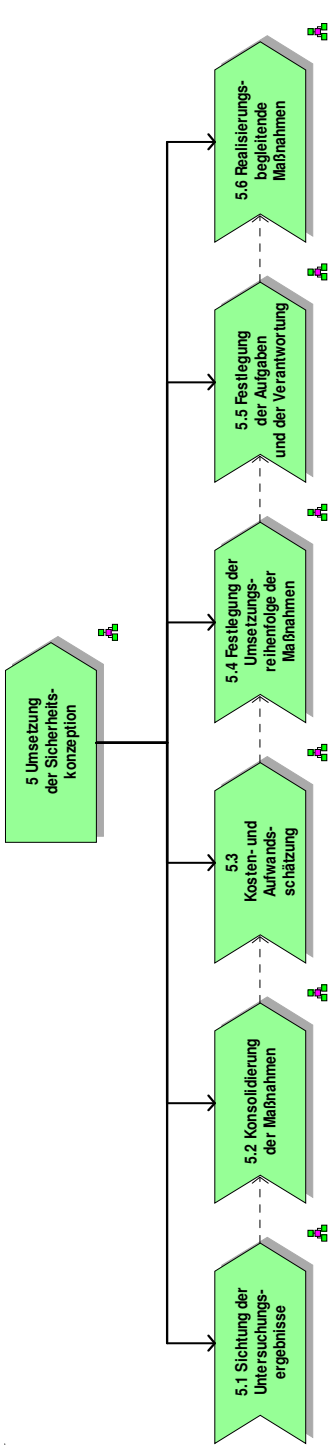
eEPK: 4.6.3 Risikoanalyse auf Basis IT-Grundschutz



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz\Arbeitsschritte

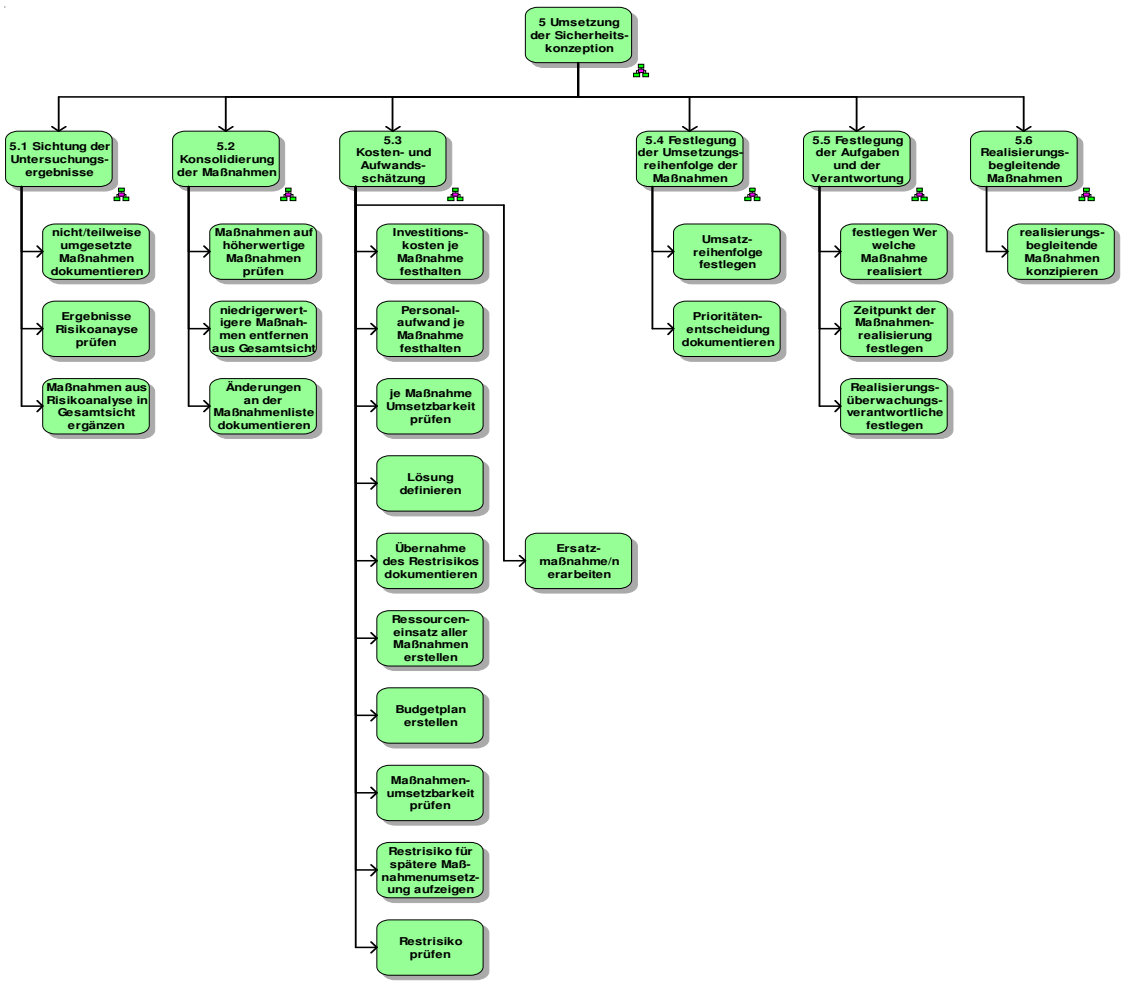
5 Umsetzung der Sicherheitskonzeption

WKD: 5 Umsetzung der Sicherheitskonzeption



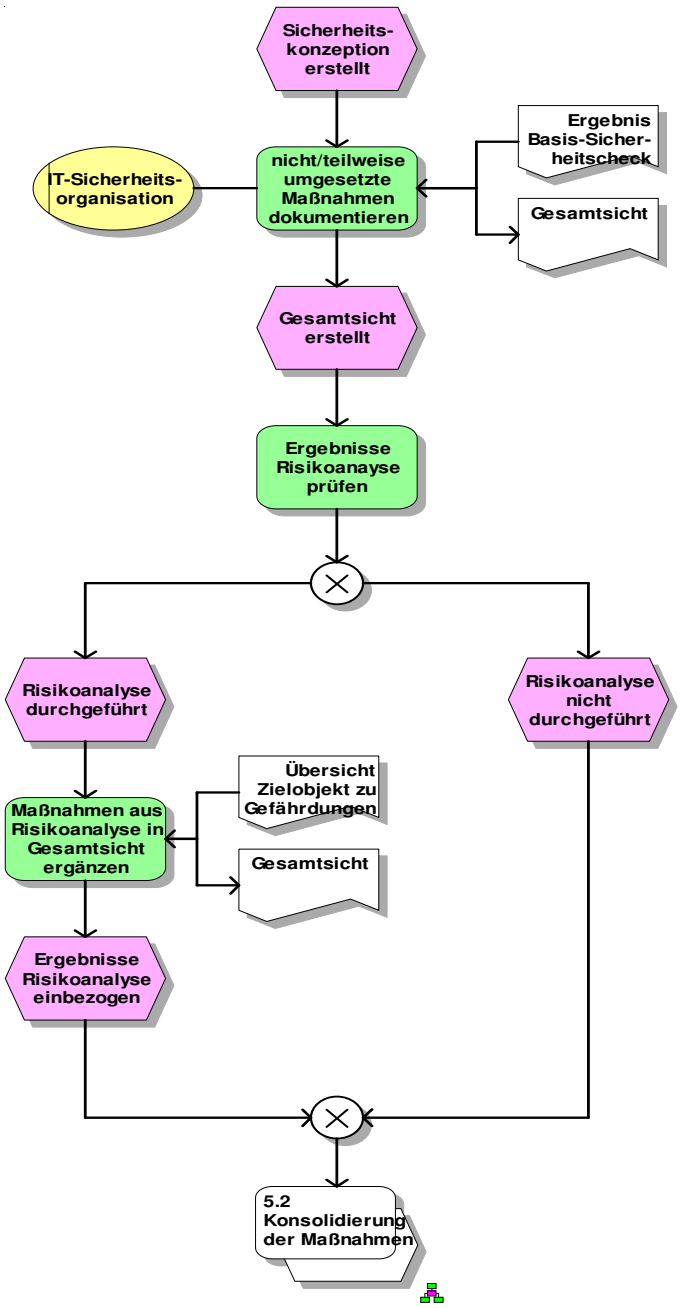
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\5 Umsetzung der Sicherheitskonzeption

Funktionsbaum: 5 Umsetzung der Sicherheitskonzeption



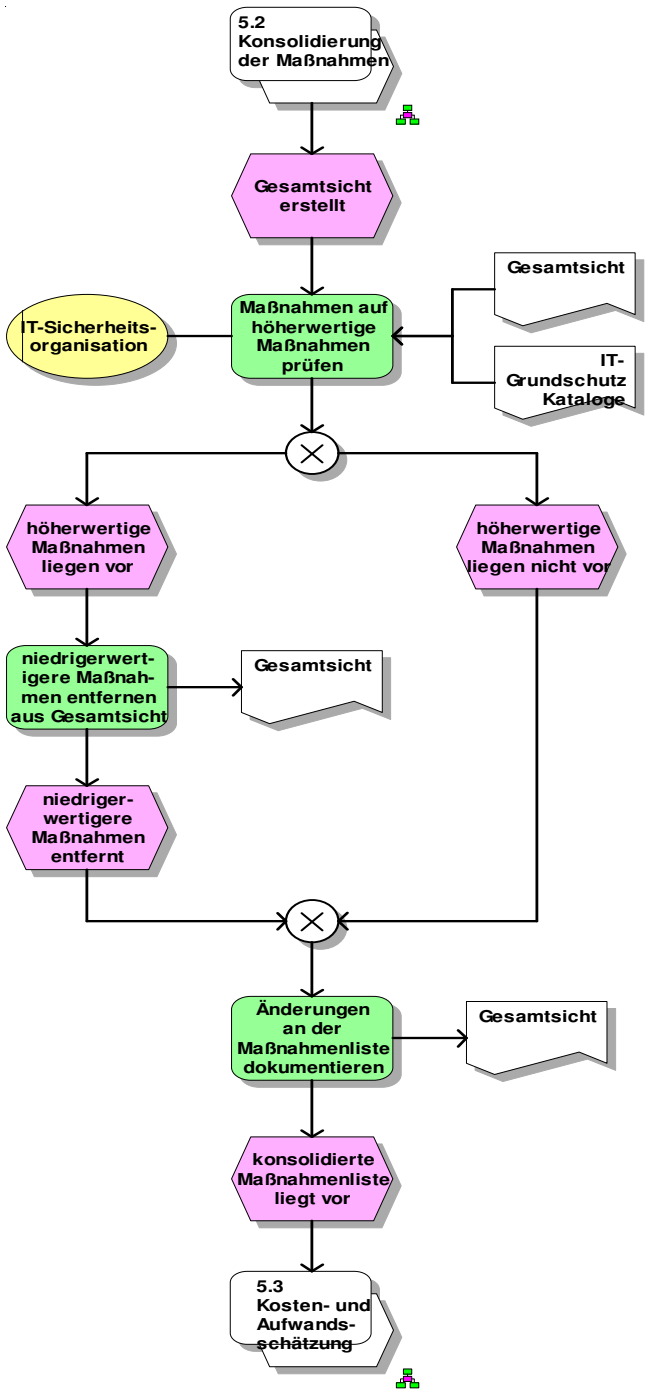
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\5 Umsetzung der Sicherheitskonzeption\Funktionsübersicht

eEPK: 5.1 Sichtung der Untersuchungsergebnisse



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\5 Umsetzung der Sicherheitskonzeption\Arbeitsschritte

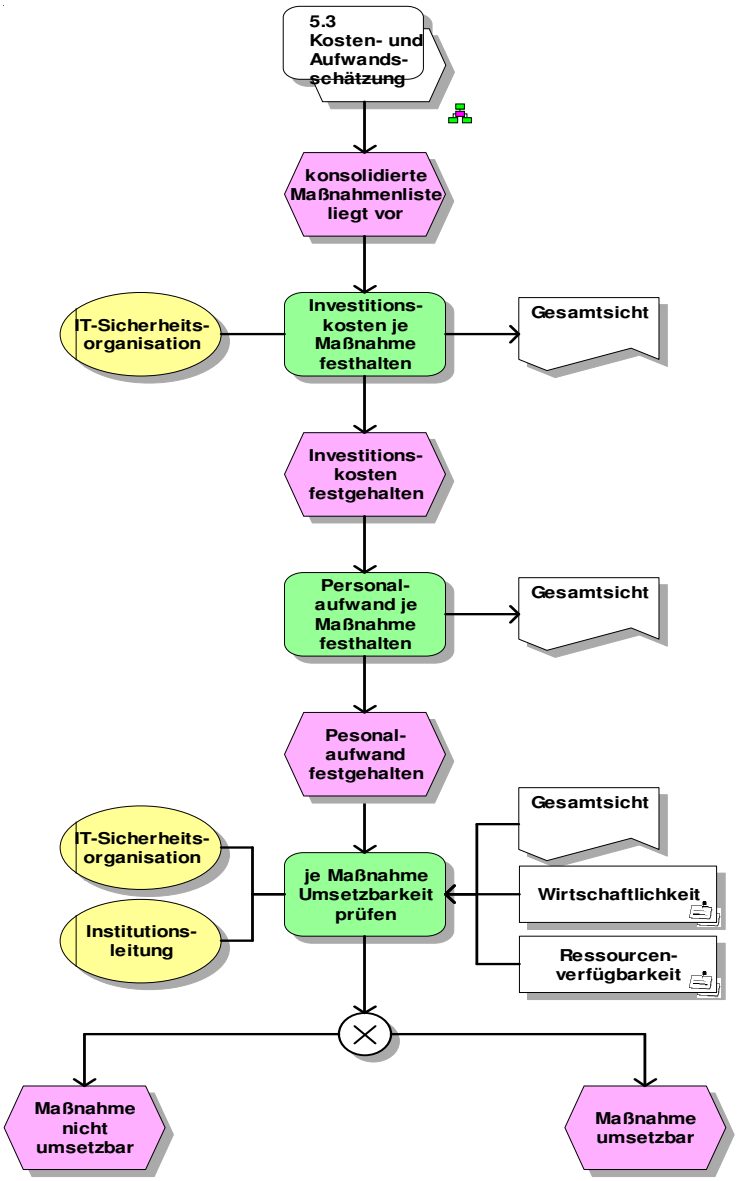
eEPK: 5.2 Konsolidierung der Maßnahmen



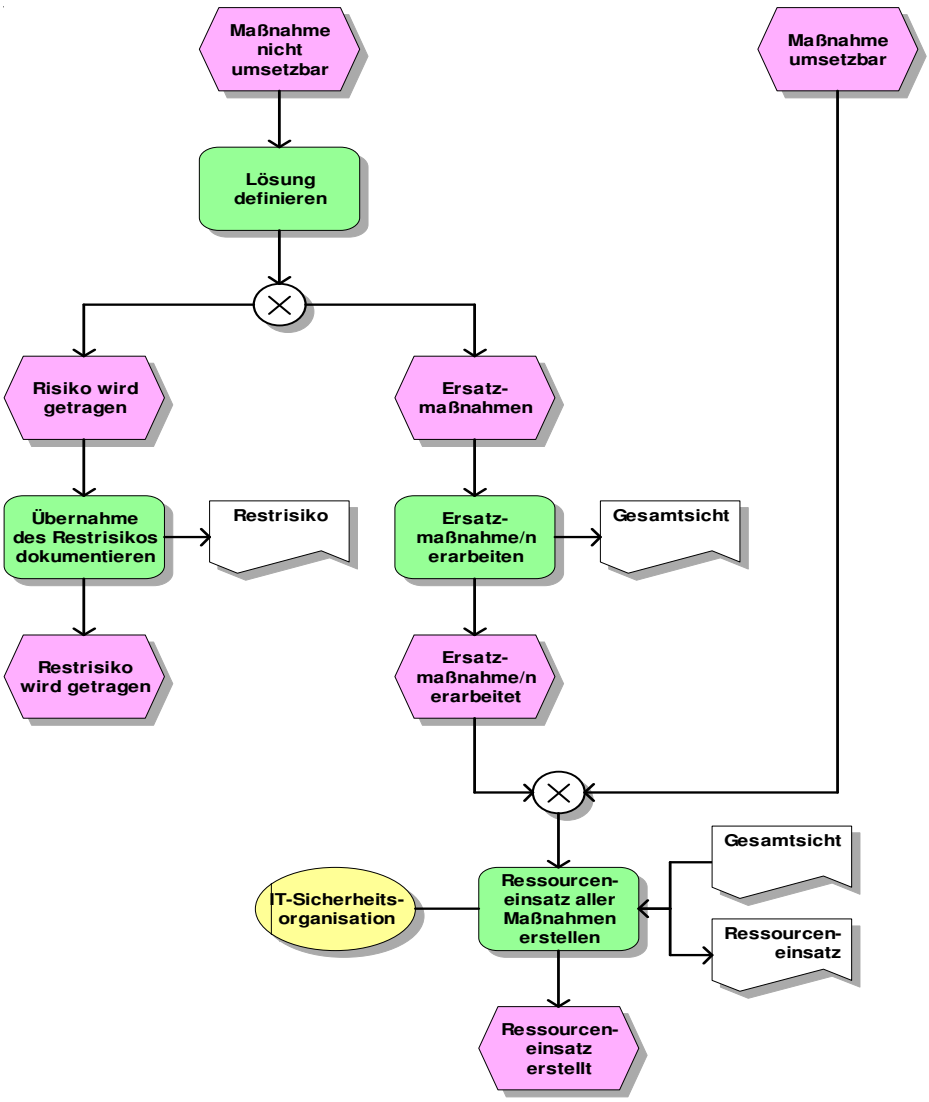
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\5 Umsetzung der Sicherheitskonzeption\Arbeitsschritte

eEPK: 5.3 Kosten- und Aufwandsschätzung

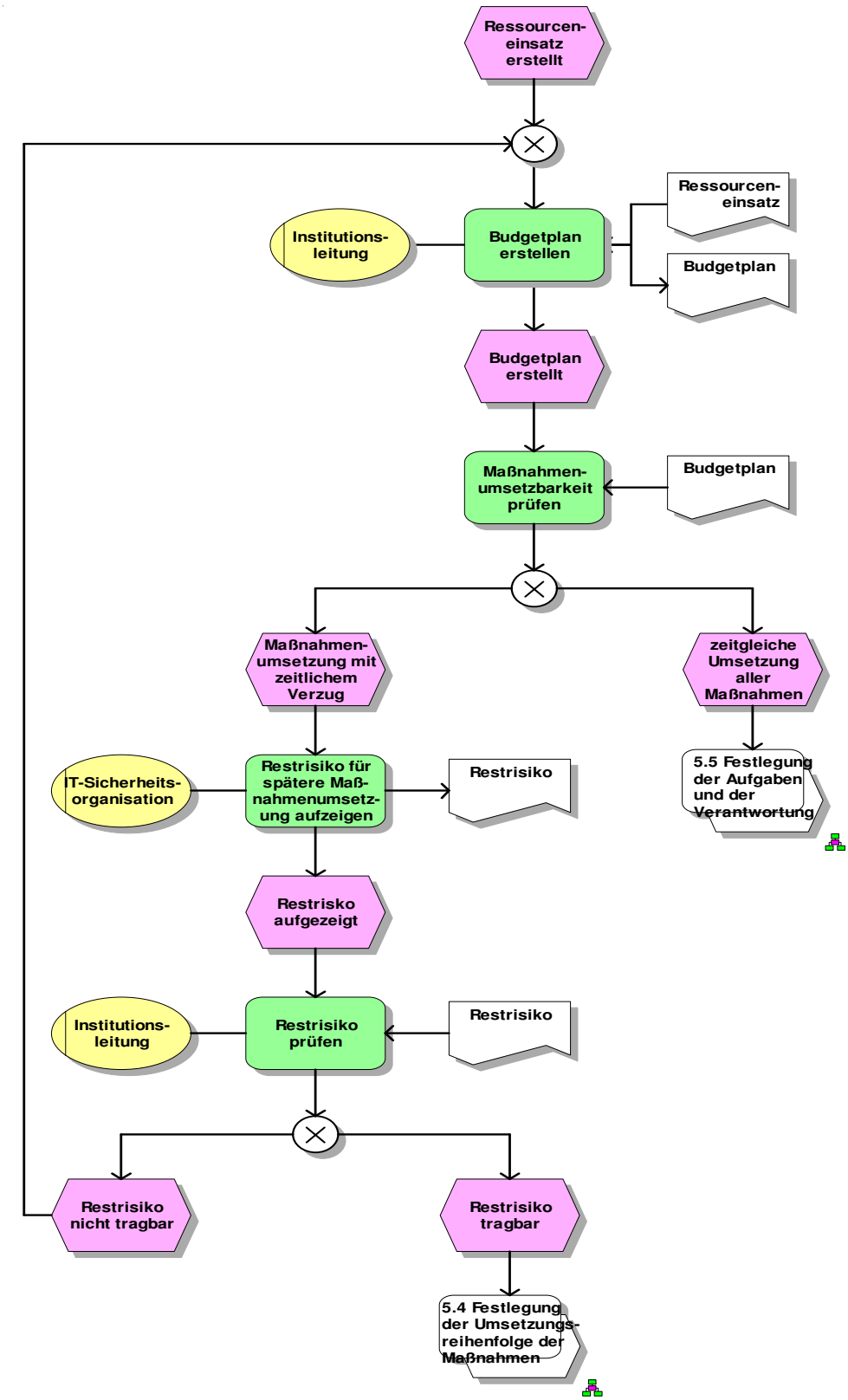
(Teil 1 von 3)



(Teil 2 von 3)

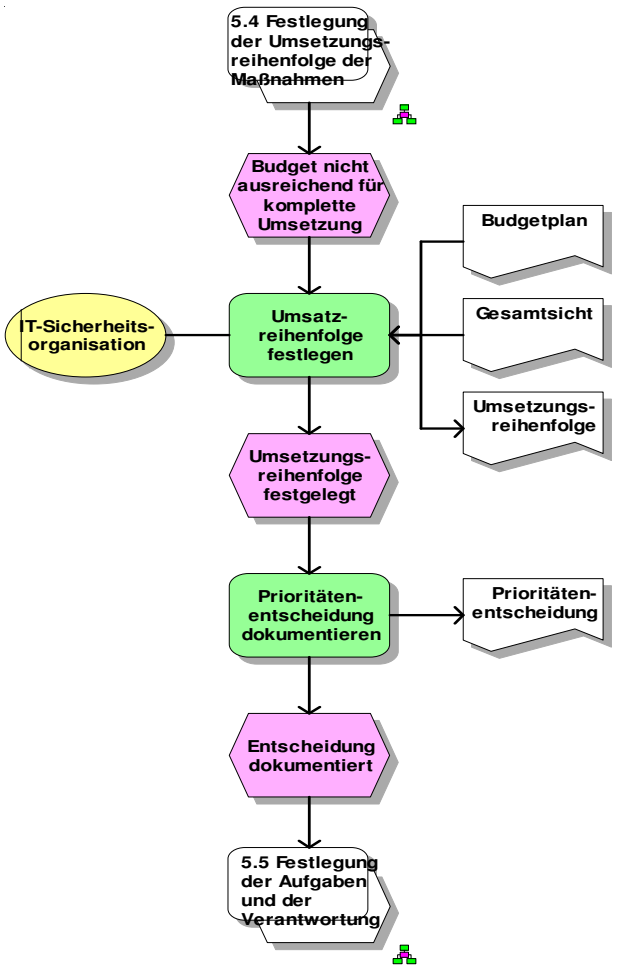

Maßnahme nicht umsetzbar
Maßnahme umsetzbar
Lösung definieren
Risiko wird getragen
Ersatz-maßnahmen
Übernahme des Restrisikos dokumentieren
Restrisiko
Ersatz-maßnahme/n erarbeiten
Gesamtsicht
Restrisiko wird getragen
Ersatz-maßnahme/n erarbeitet
Gesamtsicht
IT-Sicherheits-organisation
Ressourcen-einsatz aller Maßnahmen erstellen
Ressourcen-einsatz
Ressourcen-einsatz erstellt

(Teil 3 von 3)



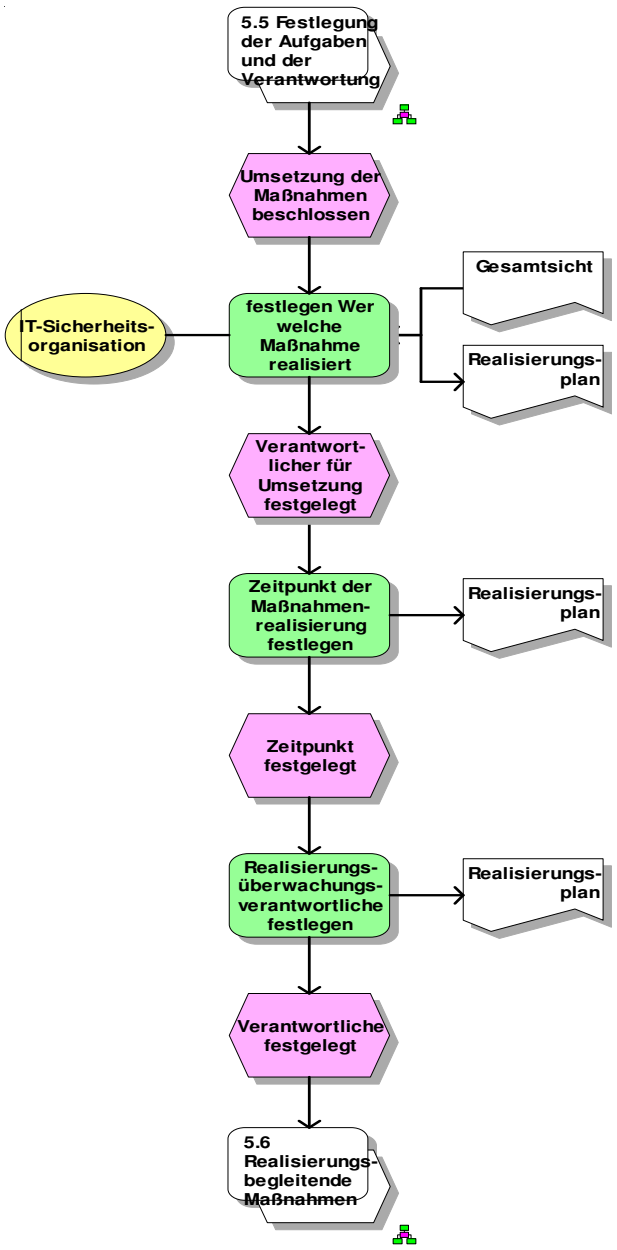
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\5 Umsetzung der Sicherheitskonzeption\Arbeitsschritte

eEPK: 5.4 Festlegung der Umsetzungsreihenfolge der Maßnahmen



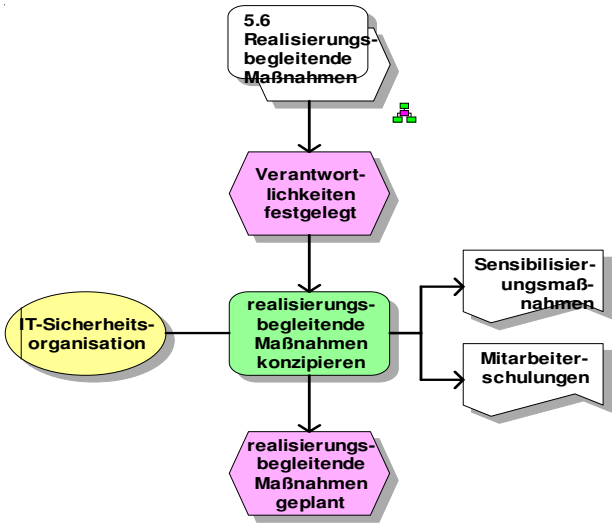
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\5 Umsetzung der Sicherheitskonzeption\Arbeitsschritte

eEPK: 5.5 Festlegung der Aufgaben und der Verantwortung



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\5 Umsetzung der Sicherheitskonzeption\Arbeitsschritte

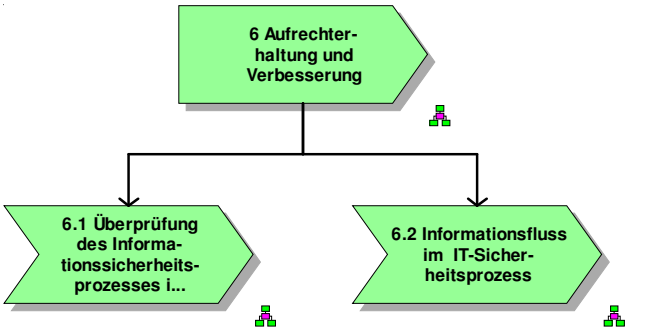
eEPK: 5.6 Realisierungsbegleitende Maßnahmen



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\5 Umsetzung der Sicherheitskonzeption\Arbeitsschritte

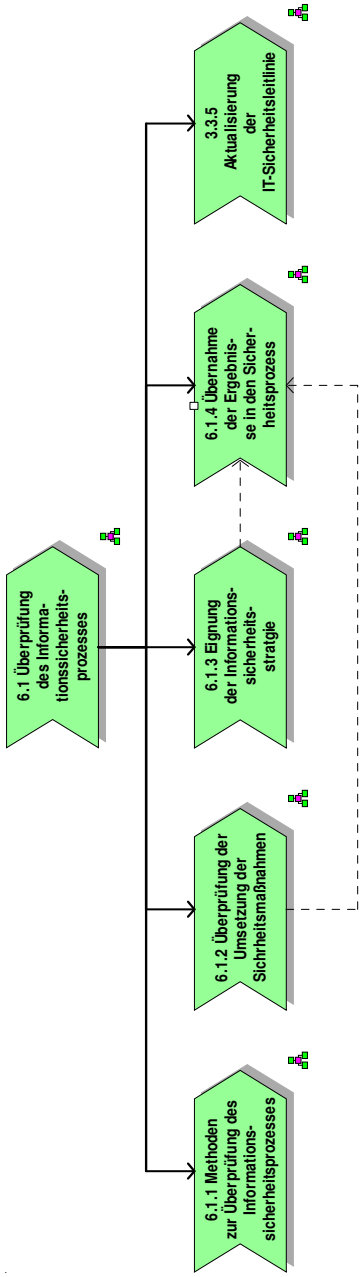
6 Aufrechterhaltung und Verbesserung

WKD: 6 Aufrechterhaltung und Verbesserung



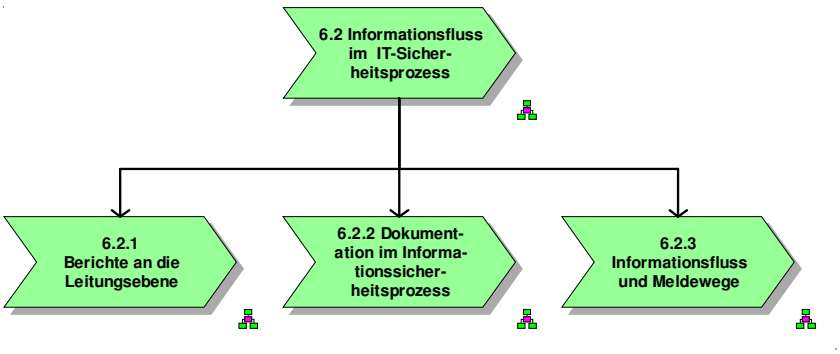
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung

WKD: 6.1 Überprüfung des Informationssicherheitsprozesses in allen Ebenen



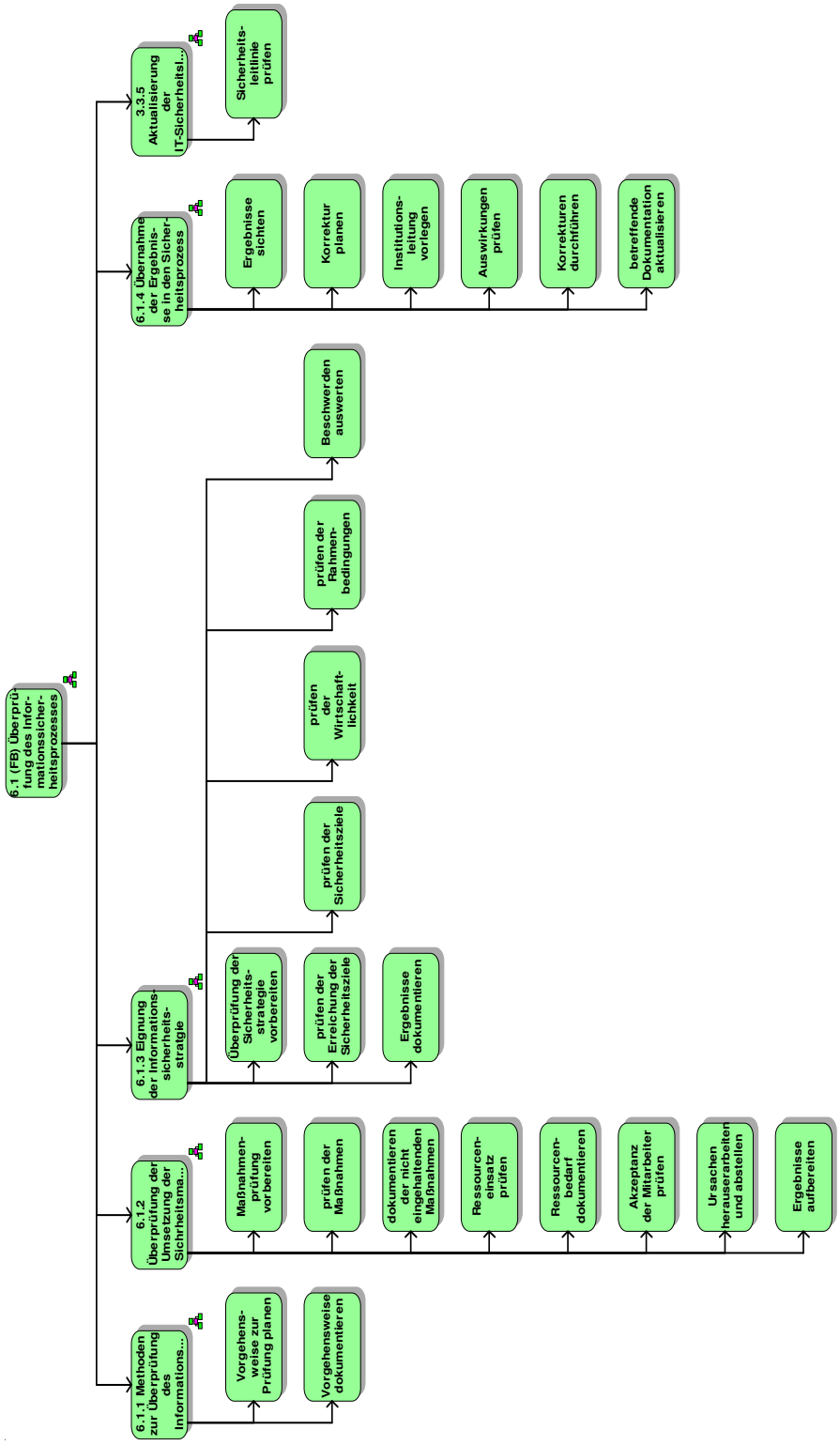
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Managementbetrachtung

WKD: 6.2 Informationsfluss im IT-Sicherheitsprozess



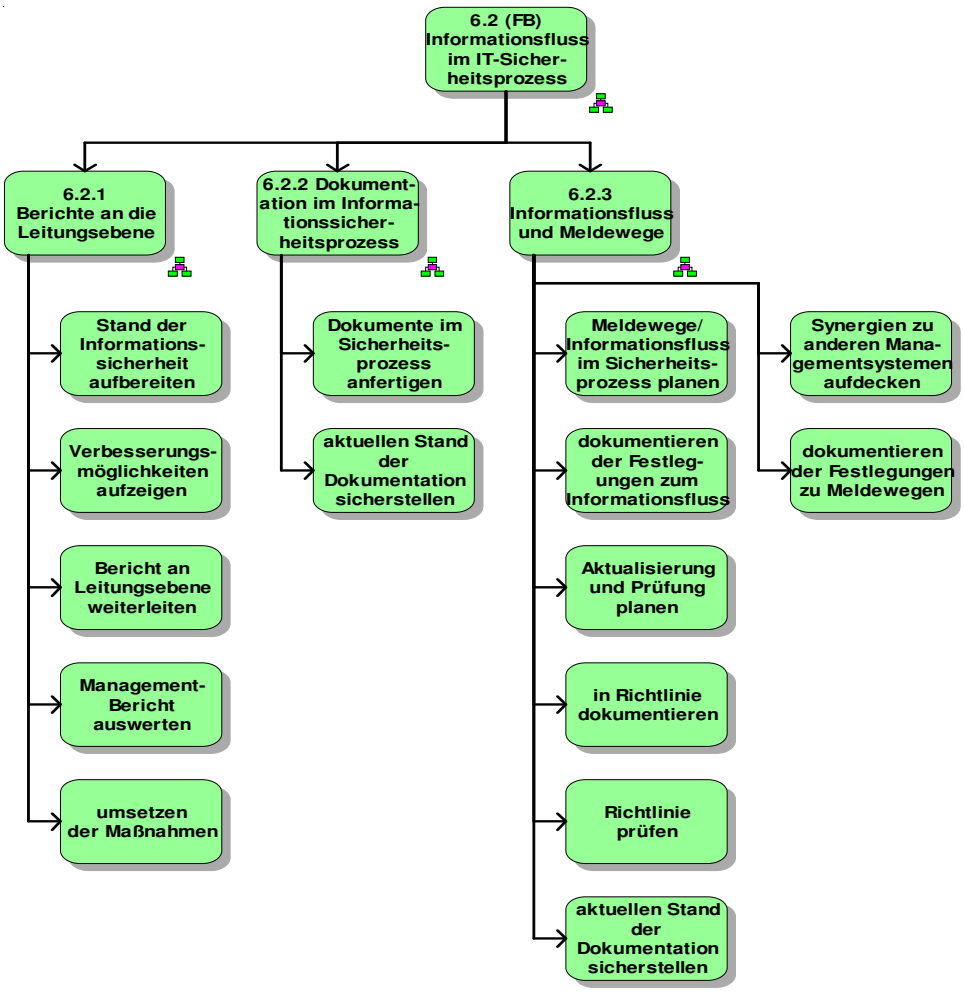
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Managementbetrachtung

Funktionsbaum: 6.1 (FB) Überprüfung des Informationssicherheitsprozesses



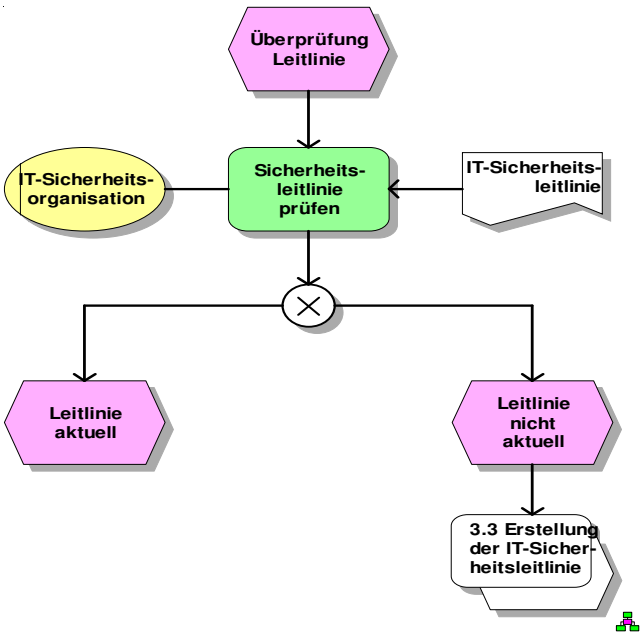
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Funktionsübersicht

Funktionsbaum: 6.2 (FB) Informationsfluss im IT-Sicherheitsprozess



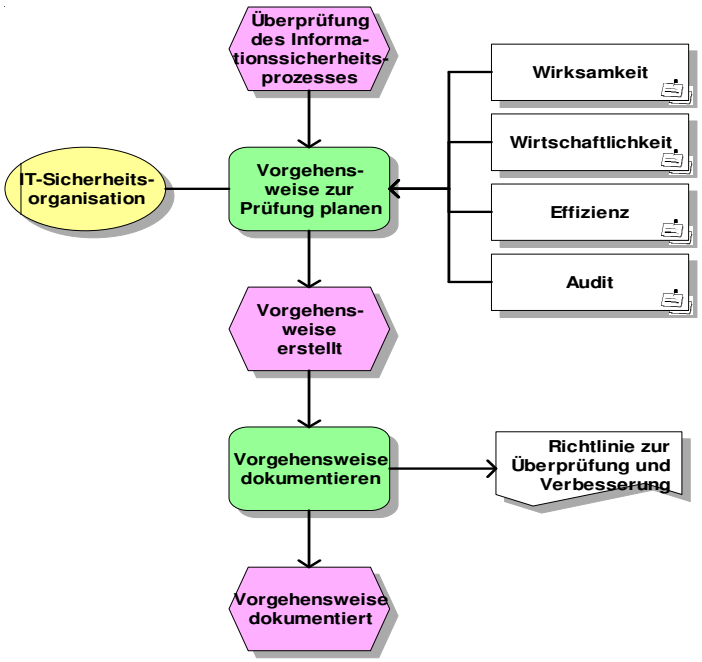
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Funktionsübersicht

eEPK: 3.3.5 Aktualisierung der IT-Sicherheitsleitlinie



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Arbeitsschritte

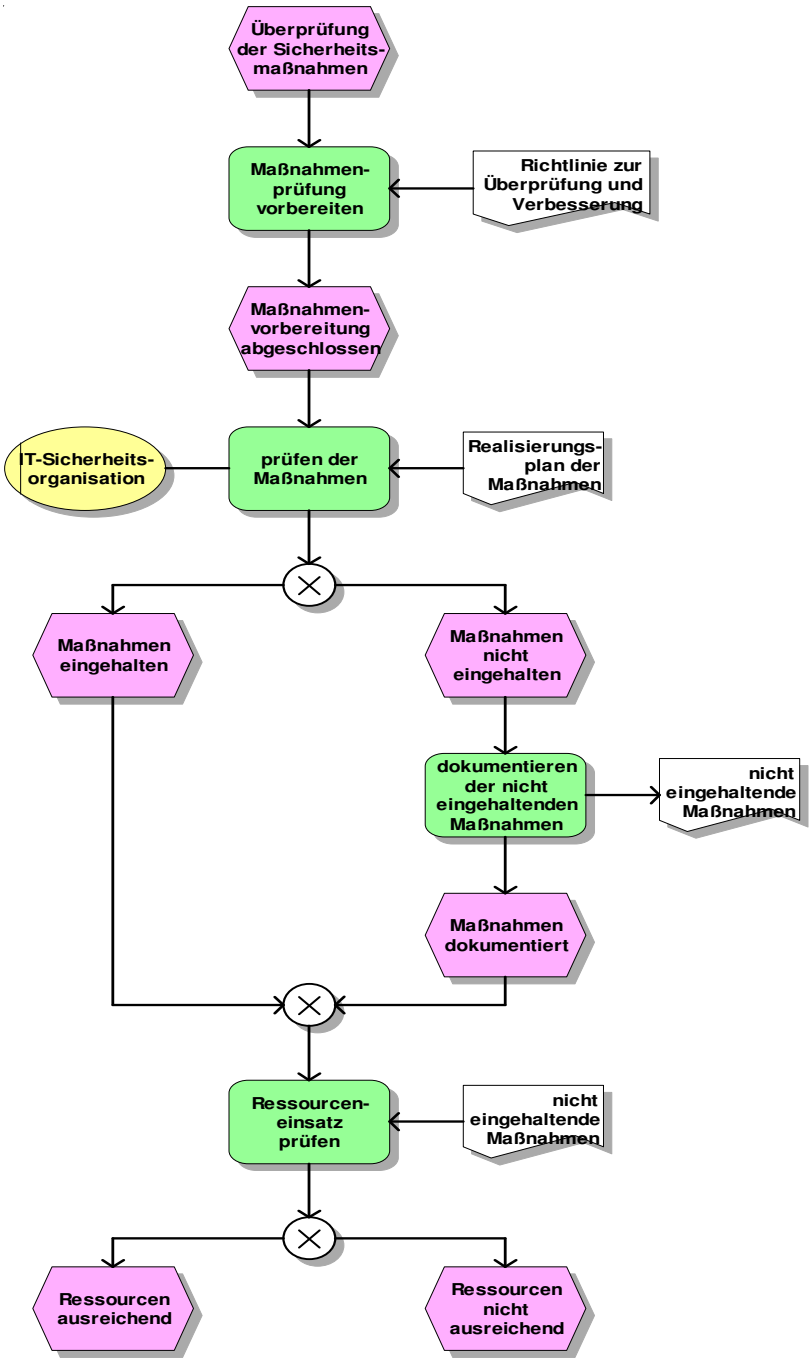
eEPK: 6.1.1 Methoden zur Überprüfung des Informationssicherheitsprozesses



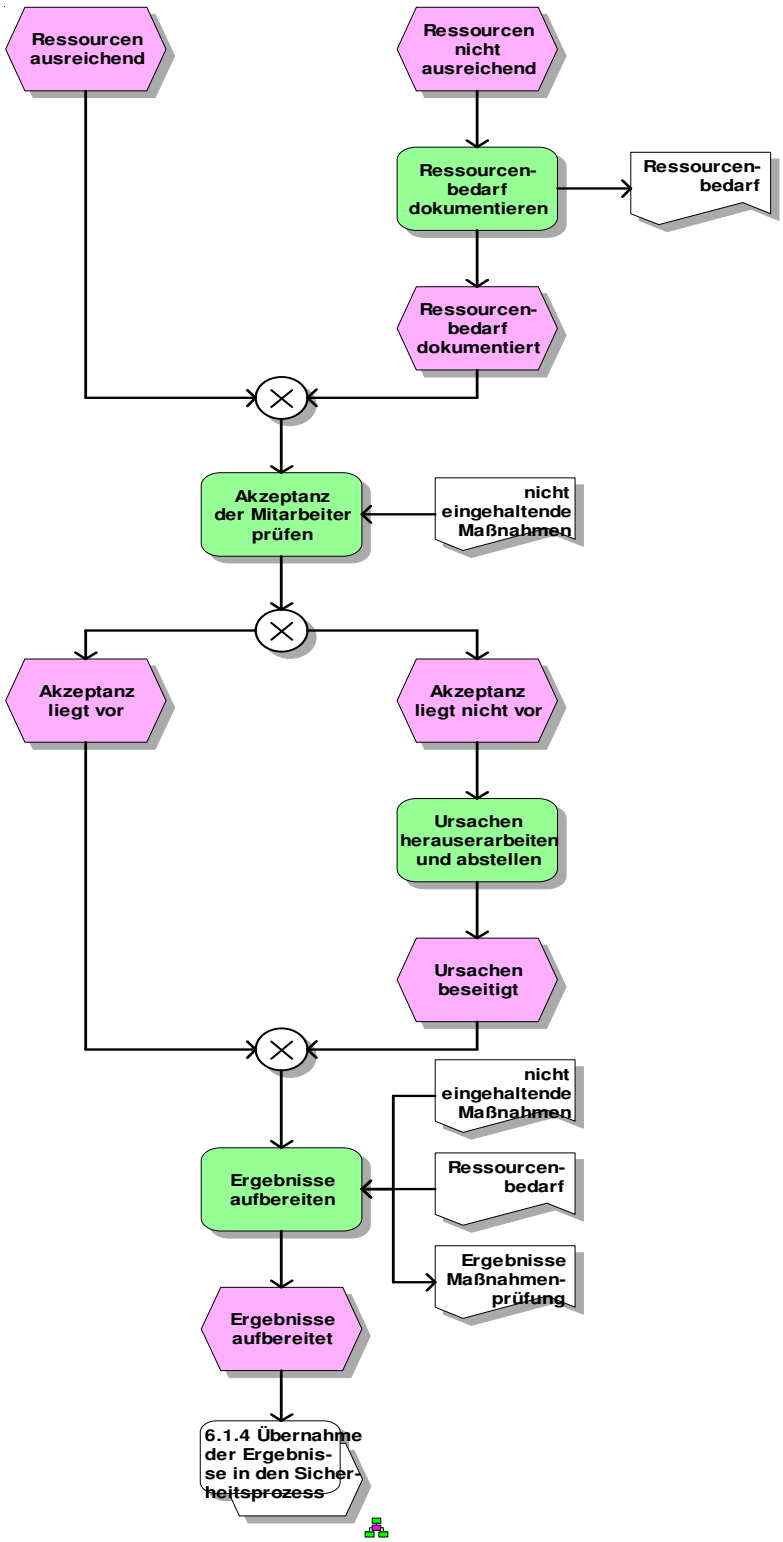
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Arbeitsschritte

eEPK: 6.1.2 Überprüfung der Umsetzung der Sichrheitsmaßnahmen

(Teil 1 von 2)

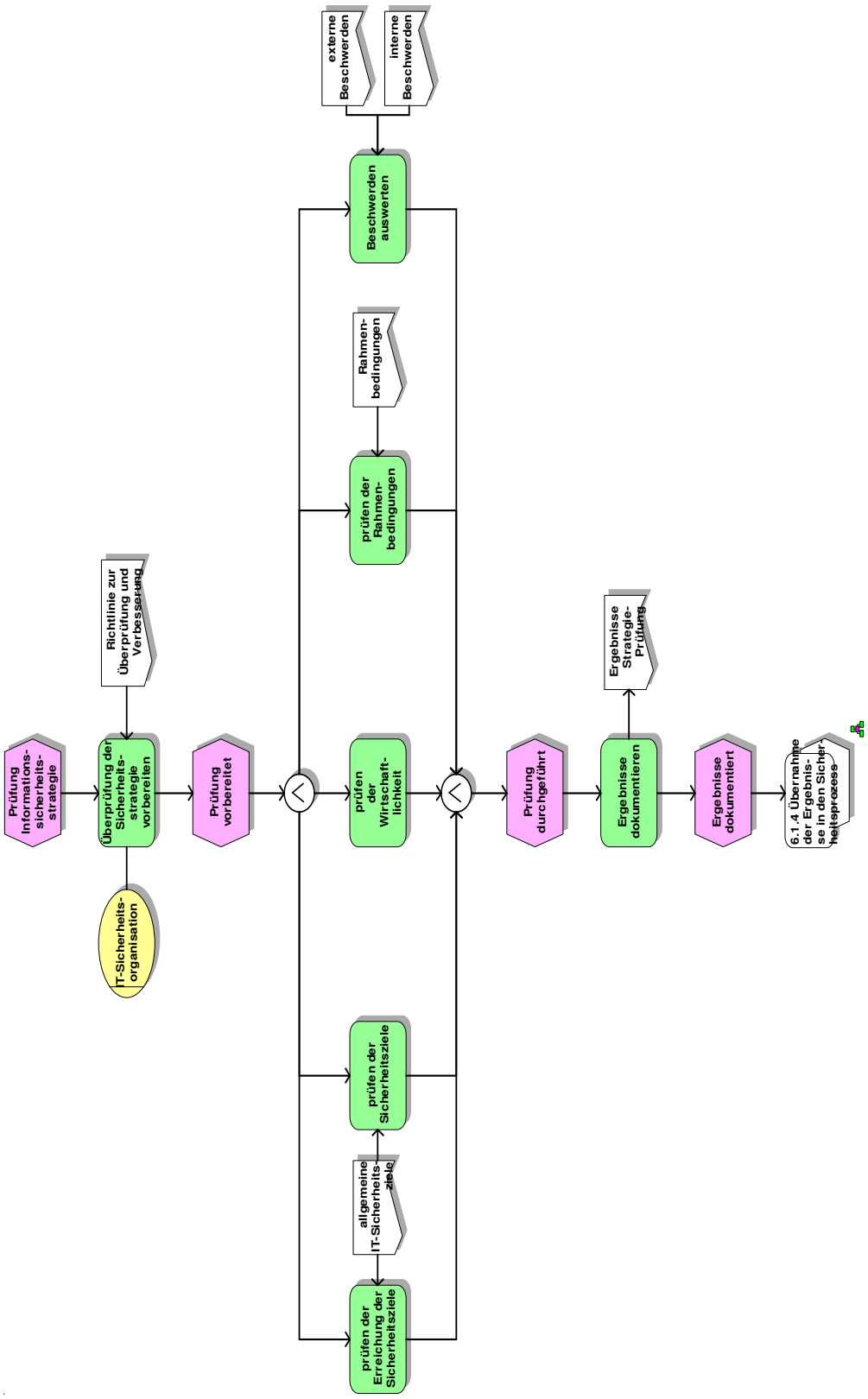


(Teil 2 von 2)



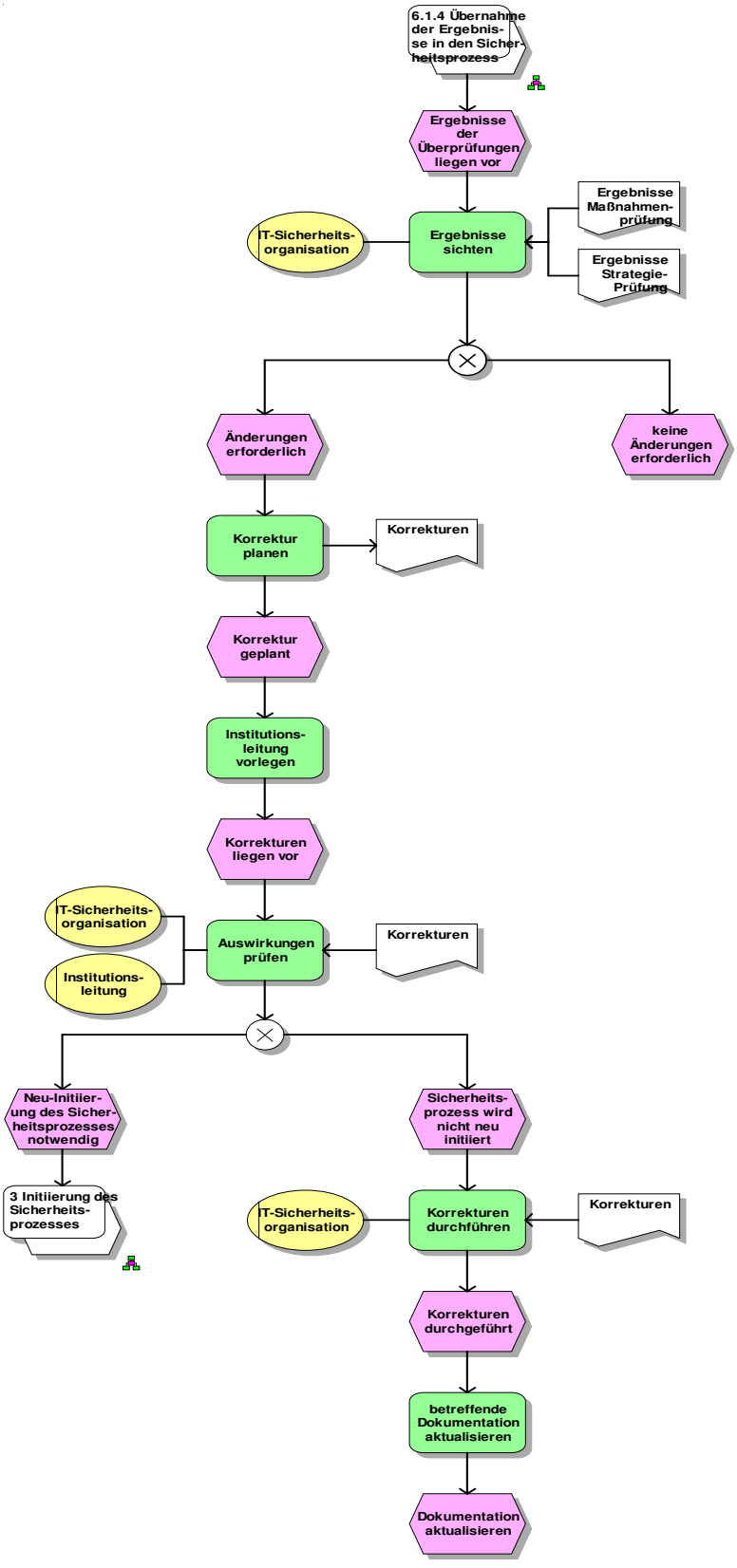
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Arbeitsschritte

eEPK: 6.1.3 Eignung der Informationssicherheitsstrategie



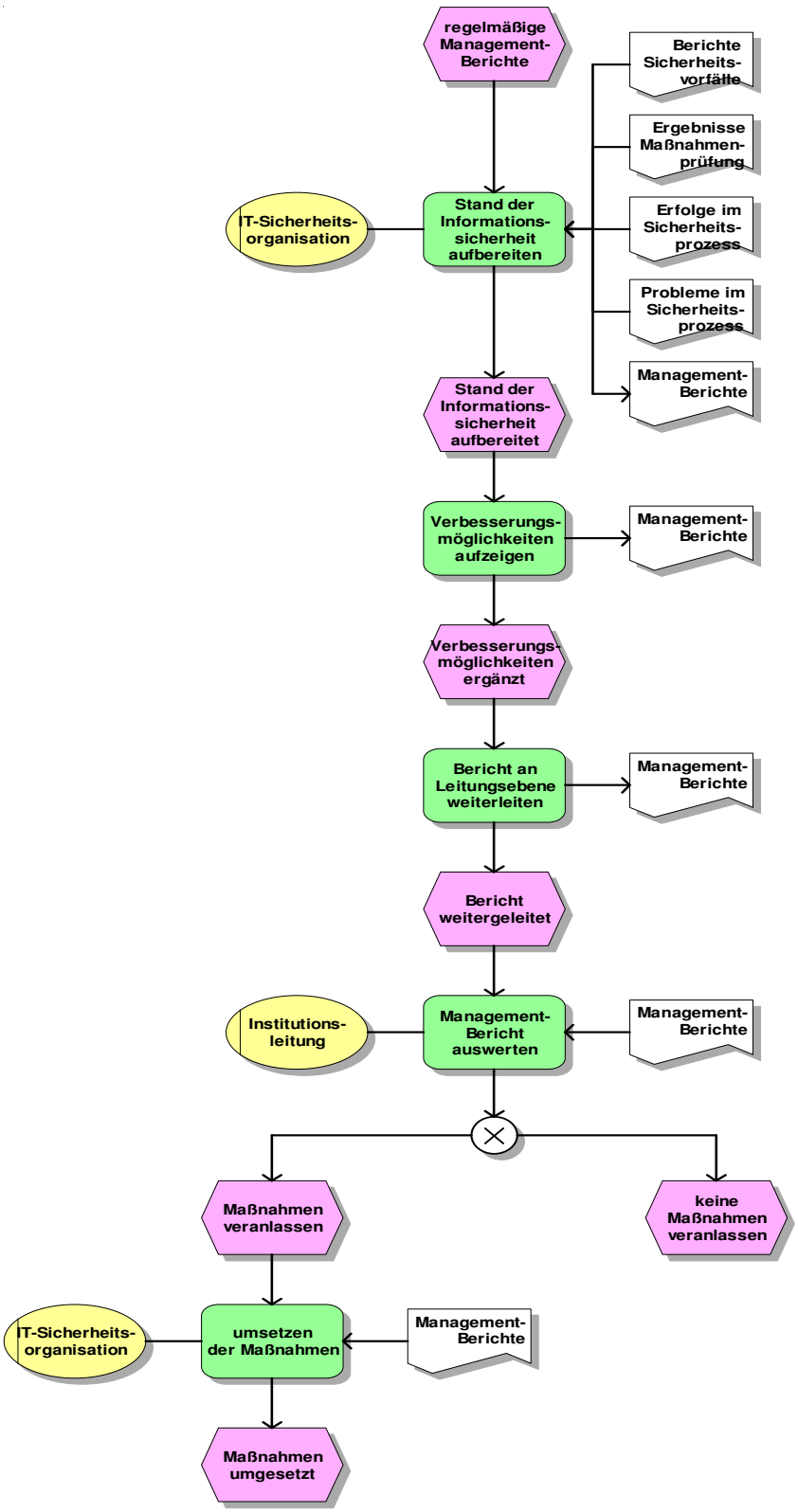
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Arbeitsschritte

eEPK: 6.1.4 Übernahme der Ergebnisse in den Informationssicherheitsprozess



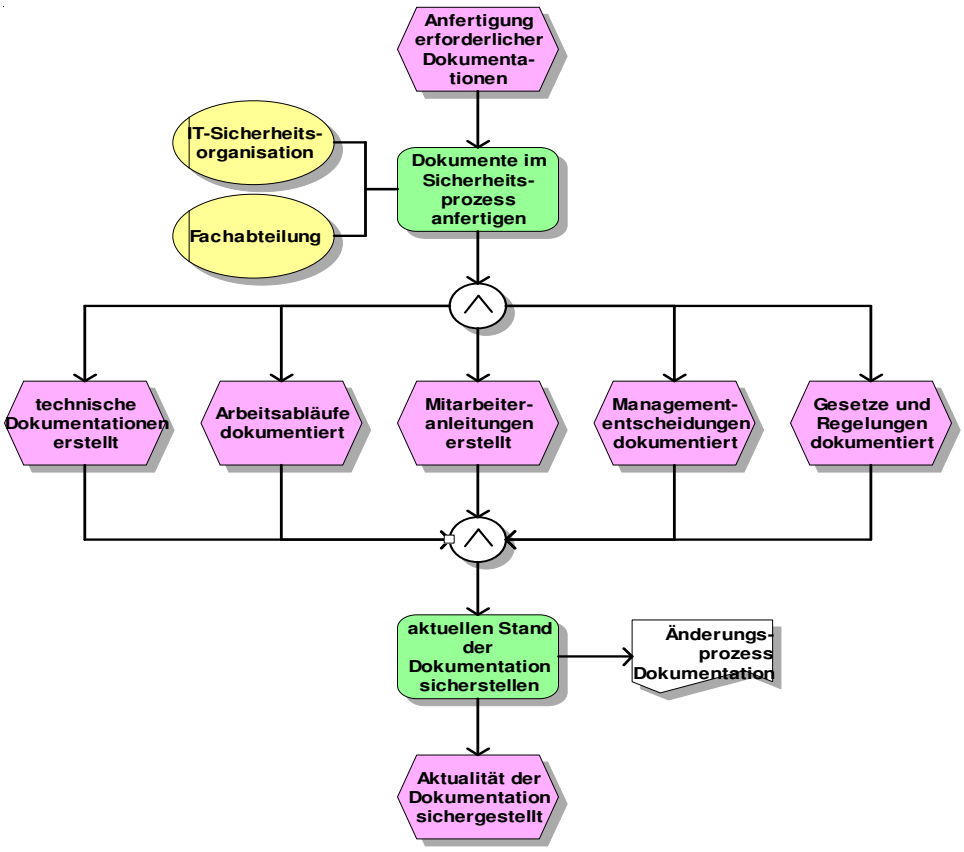
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Arbeitsschritte

eEPK: 6.2.1 Berichte an Leitungsebene



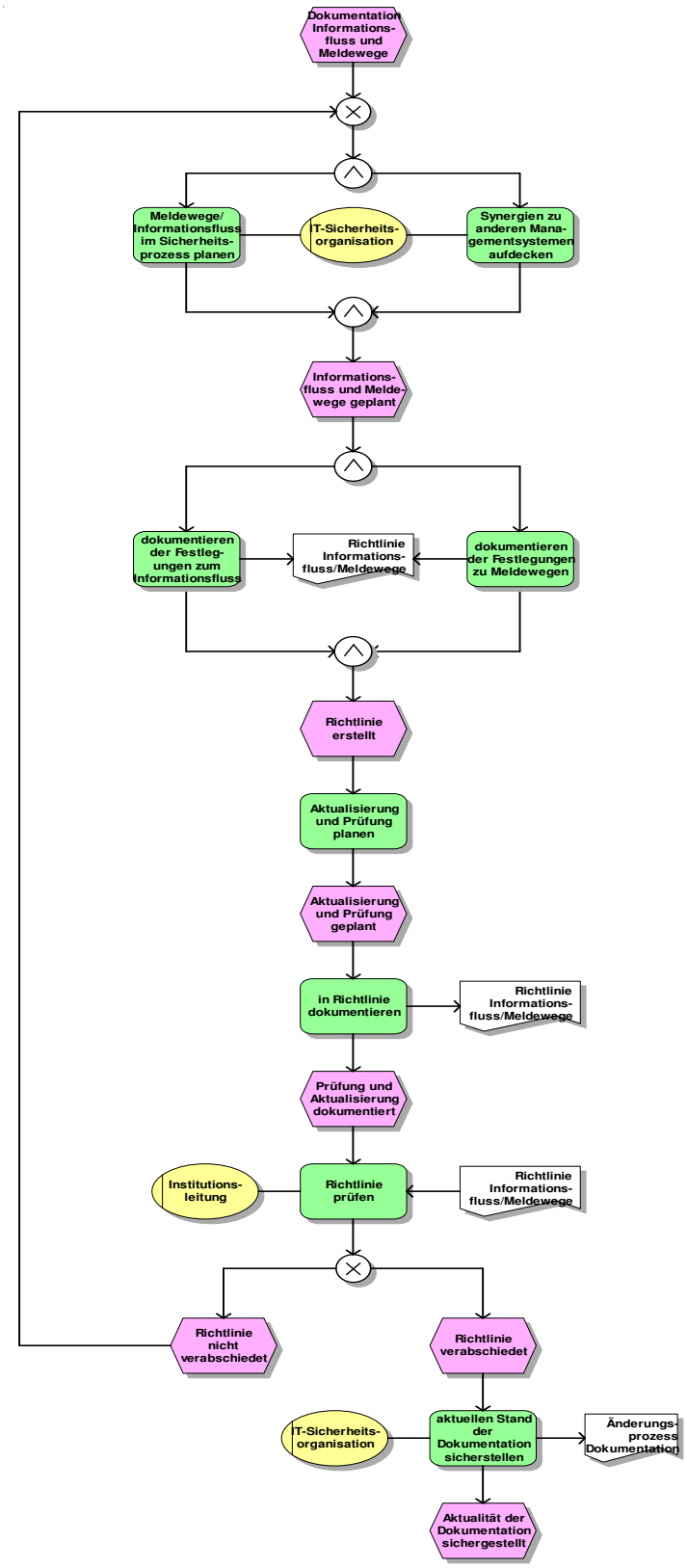
Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Arbeitsschritte

eEPK: 6.2.2 Dokumentation im Informationssicherheitsprozess



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Arbeitsschritte

eEPK: 6.2.3 Informationsfluss und Meldewege



Gruppenstruktur: \Referenzmodell ISO27001 auf Basis IT-Grundschutz\6 Aufrechterhaltung und Verbesserung\Arbeitsschritte

Abschließende Erklärung

Ich versichere hiermit, dass ich meine Diplomarbeit, Erarbeitung eines Referenzmodells zur Einführung eines Informationssicherheits-Managementsystems nach ISO 27001 auf Basis IT-Grundschutz, selbständig und ohne fremde Hilfe angefertigt habe, und dass ich alle von anderen Autoren wörtlich übernommenen Stellen wie auch die sich an die Gedankengänge anderer Autoren eng anlegenden Ausführungen meiner Arbeit besonders gekennzeichnet und die Quellen zitiert habe.

Magdeburg, den 25. August 2008