Thema:

Abbildung von Prozessen eines Information Security Management System (ISMS) nach BS 7799-2 mit dem ARIS-Tool zur Prozess-Modellierung

Diplomarbeit

Arbeitsgruppe Wirtschaftsinformatik

Themensteller: Prof. Dr. Hans-Knud Arndt

Betreuer: Dr. Stefan Schemmer

Vorgelegt von: Jens Hofmann

Abgabetermin: 23.02.06

Inhaltsverzeichnis

Verzeichnis der Abkürzungen und Akronyme

ARIS	Architektur integrierter Informationssysteme
DIN	Deutsches Institut für Normung
DV	Datenverarbeitung
eEPK	erweiterte Ereignisgesteuerte Prozesskette
EPK	Ereignisgesteuerte Prozesskette
ERM	Entity Relationship Modell
FZD	Funktionszuordnungsdiagramm
GoM	Grundsätze ordnungsmäßiger Modellierung
IS	Informationssicherheit
ISMS	Informationssicherheits-Managementsystem
IT	Informationstechnologie
o. V.	ohne Verfasser
QM	Qualitätsmanagement
SQL	Structured Query Language
UML	Unified Modelling Language
WKD	Wertschöpfungskettendiagramm

Abbildungsverzeichnis

1 Motivation und Zielsetzung

Im Zuge der zunehmenden Zahl an Sicherheitsvorfällen in Organisationen gewinnt die Erkenntnis an Bedeutung, dass Informationen bedeutende Organisationswerte sind deren Sicherheit nicht allein durch Ad-hoc-Sicherheitsmaßnahmen zu gewährleisten ist.
Gesetzliche Vorgaben sorgen dafür, dass Organisationen die Angemessenheit ihrer Maßnahmen bewerten und belegen können müssen. Daraus ergibt sich der Bedarf kontrollierte prozessbasierte Systeme zu etablieren, die zur Aufrechterhaltung der Informationssicherheit in einer Organisation (Informationssicherheits-Mangemementsysteme ISMS) dienen. Hier liegt der Schwerpunkt auf einer hohen Qualität, welche gegenüber Dritten belegt werden kann. Dabei sind die Möglichkeiten der Zertifizierung von Interesse, wobei sich der britische Standard BS7799-2:2002 als international anerkannter Standard etabliert hat. Dieser beschreibt Anforderungen an die Planung, Durchführung, Dokumentation, Bewertung und kontinuierliche Verbesserung, unter zugrunde legen eines prozessorientierten Ansatzes, eines Informationssicherheits-Managementsystems. Dabei wird vor allem die Notwendigkeit, dass alle Prozesse in ihrer Wirksamkeit überwacht werden und durch geeignete Maßnahmen verbesserte werden, vorausgesetzt. Die Grundlage hierfür stellt der Plan-Do-Check-Act-Ansatz, welcher Planung, Durchführen, Kontrolle sowie Verbesserung in einem kontinuierlichen Prozess zusammenfasst. Somit weist der Standard viele Gemeinsamkeiten mit dem DIN EN ISO 9001:2000 Standard auf, mit dem er auch explizit harmonisiert wurde.
Durch die Komplexität der Planung, Einführung, Überwachung, Bewertung und Dokumentation eines Informationssicherheits-Managementsystems, sollten diese durch geeignete Anwendungen unterstützt werden.
Das ARIS-Toolset der Firma IDS Scheer AG wurde speziell zur Modellierung von Prozessen entwickelt und wird beispielsweise bei der Einführung komplexer Applikationen, wie SAP R/3, und der damit verbundenen Prozesse verwendet. Es bietet somit die Möglichkeit die Prozesse eines ISMS geeignet abzubilden.

Zielsetzung

Ziel der Diplomarbeit ist die Abbildung von Prozessen eines ISMS nach BS 7799-2:2002 mit dem ARIS-Toolset unter Verwendung der zugehörigen Modellierungsmethoden. Angestrebt wird hierbei eine möglichst generelle Abbildung, unter weitgehen-

der Abstraktion von Organisationsspezifika, sodass die abgebildeten Prozesse als Muster für spätere Anpassung dienen können. Hierbei kann auf dem bereits bestehenden Referenzmodell der DIN EN ISO 9001:2000 aufgebaut werden. Kernpunkt der Abbildung wird dabei der Bereich der Risikoeinschätzung und –behandlung sein.

Struktur der Arbeit

Nachdem in diesem Abschnitt eine thematische Einleitung gegeben wurde, werden im Kapitel zwei die Grundsätze ordnungsgemäßer Modellierung, welche den Ausgangspunkt einer konsistenten Modellierung bieten, vorgestellt sowie das Vorgehensmodell zur Referenzmodellierung detailliert erläutert. Dabei folgt die Arbeit in den weiteren Kapiteln dem Vorgehensmodell sowohl in der Herangehensweise als auch in der Struktur.

Auf die Grundlagen folgt im Kapitel drei die allgemeine Erläuterung von Managementsystemen sowie die Darstellung deren Ausprägungen, der Qualitätsmanagementsysteme und der Informationssicherheits-Managementsysteme anhand der dieser Arbeit zu Grunde liegenden Standards. Dabei werden die Standards DIN EN ISO 9001 im Bereich der Qualitätsmanagementsysteme sowie BS7799-2:2002 und ISO/IEC 17799:2000 im Bereich der Informationssicherheits-Managementsysteme vorgestellt. Durch die gewählte Thematik dieser Arbeit erfährt hier besonders der Bereich des Informationssicherheits-Managements eine detaillierte Betrachtung und Begründung.

Im Anschluss wird das ARIS-Konzept im ersten Abschnitt des vierten Kapitels vorgestellt. Beginnend bei der Erläuterung des Konzeptes über die Beschreibung des ARIS-Toolsets wird der Bogen zweiten Abschnitt des Kapitels, dem Referenzmodellrahmen mit den Konventionen der Modellierung, gespannt. Diese dienen im Weiteren der Abbildung des ISMS nach BS7799-2:2002.

Der dritte Abschnitt des vierten Kapitels widmet sich dem Referenzmodell. Dazu wird anfangs die detaillierte Struktur des BS7799-2:2002 Standards vorgestellt. Durch die Anlehnung an das zur Verfügung gestellte Referenzmodell der DIN EN ISO 9001:2000 werden darauf folgend, Gemeinsamkeiten, die das Referenzmodell des ISMS unterstützen können, herausgestellt. Unter Einbezug dieser Gemeinsamkeiten und mit der detaillierten Betrachtung der Risikoeinschätzung und –behandlung, wird darauf folgend das Referenzmodell des ISMS nach BS7799-2:2002 vorgestellt.

Im Kapitel fünf wird die Anwendung des Referenzmodells vorgestellt. Einerseits wird das Konzept der IDS Scheer AG erläutert, andererseits ergibt sich im Laufe der Modellierung, durch die detaillierte Betrachtung der Risikoeinschätzung und -behandlung die Möglichkeit diesen Bereich in einer Software abzubilden, welche im zweiten Abschnitt des fünften Kapitels detailliert beschrieben wird.
Den Abschluss der Arbeit bietet die Zusammenfassung der geleisteten Arbeit und den Ausblick auf die weitere Entwicklung.

2 Grundsätze der Modellierung

Einführend werden die Grundsätze der ordnungsgemäßen Modellierung erläutert. Diese bieten einen Ausgangspunkt zur Unterstützung einer konsistenten Modellierung. Darauf aufbauend wird das Vorgehensmodell zur Referenzmodellierung vorgestellt. Dabei orientierten sich die nachfolgenden Kapitel an diesem Vorgehensmodell.
Zuvor werden jedoch zwei im Rahmen dieser Arbeit bedeutenden Begriffe vorgestellt, Diese Begriffe sind der Prozess und das Modell. Dabei stellt ein Prozess einen „Satz von in Wechselbeziehungen oder Wechselwirkung stehenden Tätigkeiten, der Eingaben in Ergebnisse umwandelt“[1] dar, während man unter einem Modell „ein immaterielles und abstraktes Abbild der Realität für die Zwecke eines Subjektes“ [2] versteht. Modelle werden dabei als Hilfsmittel zur Erklärung und Gestaltung realer Systeme eingesetzt.[3] Unter einem System wird ein „Satz von in Wechselbeziehungen oder Wechselwirkung stehenden Elementen“[4] verstanden.

Warum Geschäftsprozessmodellierung?

Zielsetzung der Geschäftsprozessmodellierung ist es, Geschäftsprozesse von der Dokumentation bis hin zur Optimierung zu unterstützen und dabei zu einer möglichst automatischen Umsetzung in IT-Projekten beizutragen.
Dabei versteht man unter einem Geschäftsprozess eine zusammengehörige Abfolge von Organisationsverrichtungen zum Zweck der Leistungserstellung. Der Ausgang und das Ergebnis ist eine Leistung, die von einem internen oder externen Abnehmer angefordert oder abgenommen wird.[5]
Sowohl Organisationen welche im Zuge der zunehmenden Globalisierung unter verstärktem Konkurrenzdruck stehen als auch Behörden, die ihrer Rolle als Dienstleister für den Bürger gerecht werden, schaffen dies nur, wenn sie ihre Geschäftsprozesse optimieren. Eine Organisation wird hierbei als eine „Gruppe von Personen und Einrich-

[1] EN DIN ISO 9000:2000, S.23
[2] Becker/Vossen (1996) S.19
[3] Vgl. Becker/Vossen (1996) S.19
[4] DIN EN ISO 9000:2000, S. 20
[5] Vgl. Scheer (2002), S. 3

tungen mit einem Gefüge von Verantwortungen, Befugnissen und Beziehungen“[6] bezeichnet. Dieses Gefüge ist üblicherweise geordnet. Darüber hinaus kann eine Organisation öffentlich-rechtlich oder privatrechtlich sein. Beispiele für Organisationen sind Gesellschaften, Körperschaften, Firmen, Unternehmen, Institute gemeinnützige Organisationen, Einzelunternehmen, Verbände oder Teile bzw. Mischformen solcher Einrichtungen.

Häufig stellt sich das Problem, dass diese an Aufbau- und Ablaufstruktur orientiert sind. Dabei bildet die Aufbauorganisation das hierarchische Gerüst einer Organisation ab während die Ablauforganisation die Ermittlung und Definition von Arbeitsprozessen unter Berücksichtigung von Raum, Zeit, Sachmitteln und Personen zum Gegenstand haben.

Um das Optimierungspotenzial u. a. für ein Informationssicherheits-Managementsystem, wie es in dieser Arbeit betrachtet wird, erkennen zu können, sollten Geschäftsprozesse über alle Organisationsbereiche hinweg analysiert und transparent gemacht werden. Dies erfordert eine explizite Modellierung der Geschäftsprozesse einer Organisation. Ist diese Modellierung erfolgt liegt somit eine Dokumentation der Prozesse der Organisation u. a. auch der des ISMS vor.

2.1 Grundsätze ordnungsgemäßer Modellierung

Durch die steigende Komplexität sowohl bei Referenzmodellen als auch bei organisationsspezifischen Modellen, ist es notwendig Gestaltungsempfehlungen auszusprechen. Diese Empfehlungen sollen dem Nutzer ein stets konsistentes und aktuelles Abbild der aktuellen Geschäftsprozessstruktur ermöglichen.

Durch die Grundsätze ordnungsgemäßer Modellierung wird dieses Ziel verfolgt, Grundsätze, die die Richtigkeit, Relevanz, Wirtschaftlichkeit, Klarheit und Verständlichkeit, Vergleichbarkeit sowie den systematischen Aufbau des Modells gewährleisten.[7]

Dabei versteht man unter Geschäftsprozessstruktur die Zusammensetzung eines Systems aus Geschäftsprozessen, während ein Referenzmodell im Gegensatz zu organisati-

[6] DIN EN ISO 9000:2000, S. 22

[7] Vgl. Rosemann (1996), S. 85 – 148; Vgl. Scheer (2002), S. 119 - 120

onsspezifischen Modellen nicht nur kontextspezifische Inhalte wiedergibt sondern bewusst versucht einen Kontextbezug zu abstrahieren.[8]

1. Grundsatz der Richtigkeit

Der Grundsatz der Richtigkeit lässt sich in syntaktische und semantische Richtigkeit unterteilen. Dabei stellt die syntaktische Richtigkeit die Richtigkeit gegenüber dem Metamodell (beispielsweise gegenüber dem ARIS-Modell welches in Kapitel vier vorgestellt wird) und die semantische Richtigkeit die Richtigkeit gegenüber der Realität dar. Syntaktische Richtigkeit lässt sich durch die Nutzung von rechnergestützten Tools gewährleisten und prüfen. Semantische Richtigkeit hingegen lässt sich nur erschwert prüfen, durch die für Referenzmodelle notwendige Abstrahierung und Verallgemeinerung, die von organisationsindividuellen Modellen abweicht. Konkrete Fehler lassen sich somit nur schwer feststellen.[9]

2. Grundsatz der Relevanz

Ein (Referenz-) Modell entspricht dem Grundsatz der Relevanz gemäß Rosemann wenn[10]:

- das relevante Metamodell gewählt wurde
- alle relevanten Bestandteile des Objektsystems abgebildet worden sind
  (dabei sind Elemente und Beziehungen relevant, wenn der Nutzeffekt der Modellverwendung sinken würde, falls das Modell weniger Informationen enthalten würde) d.h. jene Bestandteile der realen Welt die dem Modellierungszweck entsprechen
- das Modell ausschließlich relevante Konstrukte enthält d.h. das Modell sollte nicht mehr Informationen als nötig enthalten

Wenn beispielsweise sowohl Referenz als auch organisationsinterne Modelle mittels Ereignisgesteuerter Prozessketten[11] erstellt werden und Ereignisgesteuerte Prozessmo-

[8] Vgl. Rosemann/Schütte (1999), S. 23
[9] Vgl. Rosemann (1996) S. 94 -95
[10] Vgl. Rosemann (1996) S. 95 -97
[11] Die Ereignisgesteuerte Prozesskette (EPK) ist eine Methode zur Modellierung von Prozessen.

delle[12] die Basis sowohl für die Geschäftsprozessoptimierung als auch für die betriebswirtschaftliche Standardsoftware darstellen, kann davon ausgegangen werden, dass die relevante Modellierungsmethode zum Einsatz gekommen ist.
Das zweite und dritte Kriterium verlangt wiederum, dass das Modell vollständig in Bezug auf die für den Verwendungszweck relevante Domäne ist. Dabei sollten keine unwesentlichen Elemente enthalten sein.
Im Bezug auf den Grundsatz der Vergleichbarkeit kann dennoch nicht auf die Grundsatz der Relevanz verzichtet werden. Dieser Grundsatz stellt eine wichtige Vorraussetzung für die Vergleichbarkeit von Referenzmodellen dar.[13]

3. Grundsatz der Wirtschaftlichkeit

Der Einsatz eines Referenzmodells vereinfacht die Reorganisations- und bei Software-Einführungsprojekten die schwierige Aufgabe der Strukturierung. Zudem wird die Identifikation der zu betrachtenden Geschäftsprozesse erleichtert und der Modellerstellungsprozess beschleunigt. Sowohl das Risiko einer fehlerhaften Abbildung der bestehenden Zusammenhänge als auch die gewünschten Zusammenhänge fehlerhaft darzustellen wird verringert. Eine Ableitung der organisationsinternen Geschäftsprozesse aus einem Referenzmodell kann die Qualität solcher Modelle steigern. Zudem enthalten Referenzmodelle häufig erprobte Lösungen (best practices).
Eine automatische Übernahme von Referenzmodellen sollte jedoch vermieden werden, da strategische Wettbewerbsvorteile (Erfolgsfaktoren) und Kernkompetenzen verloren gehen.
Dabei beschreibt die Kernkompetenz einer Organisation die Fähigkeit, sich auf eine bestimmte Tätigkeit im Vergleich zu den anderen Organisationstätigkeiten zu konzentrieren und diese besonders gut ausführen zu können.
Für die Nutzen- und Kostenbetrachtung beim Einsatz von Referenzmodellen sind folgende Faktoren zu betrachten
Nutzen gemäß Rosemann[14]:

---

[12] In einem semantischen Prozessmodell wird ein Prozess nach festen Notationsregeln, die von der Modellierungsmethode (z.B. EPK) abhängig, beschrieben. In einem Prozessmodell werden die wechselseitigen Abhängigkeiten zwischen einzelnen Funktionen anhand der zwischen ihnen bestehenden Kontrollflüsse offen gelegt.
[13] Vgl. Rosemann (1996) S. 95 - 97
[14] Vgl. Rosemann (1996), S. 99

- Strukturierung von Reorganisationsobjekten
- vereinfachte Prozessidentifikation
- schnelle Modellerstellung
- Minimierung organisatorischer Schnittstellen
- verstärkte Kundenorientierung
- Effizienzsteigerung im Software-Anpassungs-Prozess
- einfache Einarbeitung
- Abbildung von Interdependenzen
- verbesserte innerbetriebliche Kommunikation
- Erhöhung der Qualität der Organisationsmodelle
- Modellierung- und Brachenkompetenz der Ersteller (impliziert Best Practices)

Kosten gemäß Rosemann[15]:

- Anschaffungsauszahlungen, Kosten der Methodenschulung
- Kosten der Erstellung des organisationsindividuellen Modells
- Kosten der Anpassung der Modelle
- Kosten des Modellvergleichs

Neben Kosten und Nutzen muss auch das Risiko gemäß Rosemann betrachtet werden[16]:

- Das Risiko der fehlerhaften Abbildung, welches durch den Einsatz von Referenzmodellen verringert wird.
- Das Risiko des Verlustes von Kernkompetenzen durch den Einsatz von Referenzmodellen.

4. Grundsatz der Klarheit und Verständlichkeit

Durch die verstärkte Nutzung von Referenzmodellen durch Mitarbeiter entsprechender Fachabteilungen stellt der Grundsatz der Klarheit und Verständlichkeit ein wichtiges Kriterium zur Beurteilung dar. Nachdem die Nutzer im Umgang mit Ereignisgesteuerten Prozessketten geschult sind, ist das Referenzmodell für die Modelladressaten ver-

[15] Vgl. Rosemann (1996), S. 99 - 102
[16] Vgl. Rosemann (1996), S. 99 - 102

ständlich und von diesen für ihre Zielsetzung verwendbar. Die Verständlichkeit wird durch den Rahmen des Referenzmodells erhöht.
Geschäftsprozessmodelle werden zudem mit einem erläuternden textlichen Anhang versehen. Dadurch erhöht sich die Klarheit und der Modellnutzer erlangt leichter Verständnis. Nachteil dieser textlichen Erläuterung ist der erhöhte Aufwand zur Vergleichbarkeit.[17]

5. Grundsatz der Vergleichbarkeit

Dieser Grundsatz hat bei der Verwendung von Referenzmodellen eine erhebliche Bedeutung, da ein Referenzmodell den Bezugspunkt zum organisationsindividuellen Modell bildet. Der mit dem Vergleich verbundene Aufwand ist eine wesentliche Zielgröße für die Beurteilung von Referenzmodellen. Durch das Befolgen vorgegebener Konventionen ist die perspektiveninterne Vergleichbarkeit sicherzustellen.
Der Vergleich des organisationsspezifischen Modells mit dem Referenzmodell, kann dadurch erschwert werden, dass Ausschnitte der Realwelt von verschiedenen Betrachtern in unterschiedlichen Prozessketten unterschiedlich abgebildet werden, insbesondere gemäß Rosemann durch[18]:

- Nutzung von Generalisierung/Spezialisierung: Eine unterschiedliche Definition von Objekten kann zu parallelen Teilsträngen oder einer häufigen Nutzung von XOR-Verzweigungen führen
- Konkretisierung (Detaillierungsgrade) der gesamten oder einzelner Vorgänge
- Benennung der Informationsobjekte (innerhalb und zwischen den Modellsichten) und
- Anordnung der Informationsobjekte[19]

Wesentlicher Punkt ist hierbei der Detaillierungsgrad, aus dem sich folgende Probleme gemäß Rosemann ergeben[20]:

- Der Detaillierungsgrad sollte nicht geringer oder größer als dies zum Erkennen der organisationsindividuellen Stärken und Schwächen erforderlich ist, sein.

[17] Vgl. Rosemann (1996) S. 99 - 102
[18] Vgl. Rosemann (1996), S. 102
[19] Einheit von verschiedenen Informationen zur Repräsentation eines realen oder künstlichen Objektes der realen Welt.

- Im organisationsindividuellen Modell werden ggf. Abhängigkeiten von Personen, die Geschäftsprozess ausführen, berücksichtigt. Diese lassen sich in einem Referenzmodell per Definition nicht abbilden.
- Eine notwendige Detaillierung wird u. a. auch vom Anlass beeinflusst. Dies kann beispielsweise die Prozesskostenrechnung sein. „Die Prozesskostenrechnung basiert auf dem Prinzip, Geschäftsprozesse in elementare Teilprozesse zu segmentieren. Für die resultierenden Teilprozesse werden durchschnittliche Kosten [...] ermittelt“[21]
- In Referenzmodelle werden Strukturen und Abläufe so abgebildet, dass sie für eine Vielzahl von Organisationen verwendbar sind. Daraus ergibt sich ein unterschiedlicher Detaillierungsgrad.

Ein automatischer Vergleich zwischen organisationsindividuellen und Referenzmodell kann aus verschieden Gründen nicht durchführbar sein.

- Unterschiedliches Layout
- Verwendung unterschiedlicher Bezeichnungen
- Verwendung unterschiedlicher Informationsobjekte und Objekttypen

Ein manueller Abgleich ist meist auf Grund des hohen Umfangs sehr aufwendig und ist deshalb nur an verschiedenen Kernmodellen sinnvoll.[22]

6. Grundsatz des systematischen Aufbaus

Dieser Grundsatz verlangt die Integrationsfähigkeit von Modellen, welche in organisationsindividuellen Sichten entwickelt wurden. Dazu wird ein sichtenübergreifendes Metamodell erforderlich, wie es beispielsweise das ARIS-Modell bereitstellt, welches im Weiteren erläutert wird.[23]

---

[20] Vgl. Rosemann (1996), S. 102
[21] Scheer (2002), S. 66
[22] Vgl. Rosemann (1996), S. 102 - 103
[23] Vgl. Rosemann (1996), S. 103 -104; Vgl. Scheer (2002), S.119 - 120

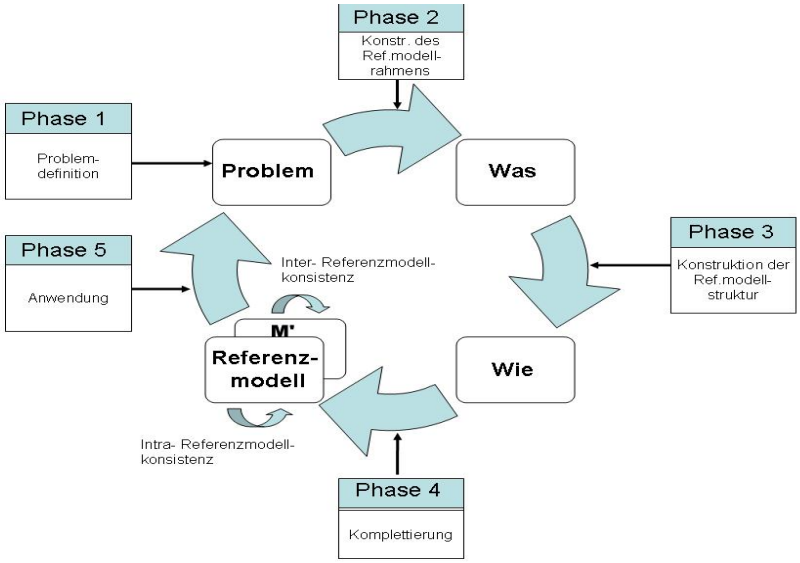
Allgemein lassen sich die Inhalte von Modellen in verschiedene Sichten untergliedern. Ziel der Sichtenbildung ist die Komplexitätsreduktion. Sichten sind dabei dynamische Fenster auf die zugrunde liegenden Beziehungen.[24]

2.2 Vorgehensmodell zur Referenzmodellierung

Um eine gemäß der Grundsätze ordnungsgemäßer Modellierung in der Abbildung des BS7799-2:2002 Standards vorgehen zu können, wird in diesem Abschnitt ein allgemeines Vorgehen zur Referenzmodellierung vorgestellt, welches in dieser Diplomarbeit Anwendung findet.

Phasen der Referenzmodellierung

Die Grundsätze ordnungsgemäßer Modellierung (GoM) zielen auf die Ergebnisqualität von Modellen ab. Es werden aber keine Gestaltungshilfen für den Konstruktionsprozess gegeben. Aus diesem Grund wurde das Vorgehensmodell zur Referenzmodellkonstruktion und –anwendung (siehe Abbildung 2.1) entwickelt.



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

Abb. 2.1 Vorgehensmodell zur Referenzmodellierung

[24] Vgl. Schreier (1991), S. 125

Ein Referenzmodell ist dabei ein für eine Branche oder einen ganzen Wirtschaftszweig erstelltes Modell, welches allgemeingültigen Charakter haben soll. Es kann somit als Ausgangslösung zur Entwicklung organisationsspezifischer Modelle dienen.[25]

Phase 1 Problemdefinition

Zu Beginn der Referenzmodellierung gilt es die Problemdefinition zu erarbeiten. Auf Grund der besonderen Gefahr, dass eine Lösung für ein Problem konstruiert wird, welches aus Sicht des Anwenders nicht existiert, wird dieser Phase besondere Bedeutung bei der Referenzmodellierung zugeschrieben. Dieses Problem entsteht als Ergebnis eines Einigungsprozesses, an welchem mehrere Personen beteiligt sind. Dabei ist die Bedeutung eines Modellkonstruktionsprozess, an welchem mehrere Personen beteiligt sind, nicht zu unterschätzen. Durch das Vorhandensein mehrerer Sichten (Personen), kann Gewähr für einen Modellkonstruktionsprozess, welcher seinen Zweck erfüllt in der Regel gegeben werden.
Eine Problemdefinition eines Modellierers bezieht sich auf Annahmen über Probleme, die ihm für eine Klasse von Organisationen als besonders relevant erscheinen. Auf diese folgt die Erstellung eines Prototypen, welcher in mehreren Iterationsstufen geprüft und verbessert wird.[26]

Phase 2 Konstruktion des Referenzmodellrahmens

Die spezifischen Modelle von Organisationen lassen sich als Varianten des Referenzmodells auffassen, so dass Ähnlichkeiten zum Variantenmanagement in der Industrie genutzt werden können. Dazu zählen u. a. auch Überlegungen zur Klassifikation von Modellbestandteilen. Diese sind notwendig um dem Modellierer die Möglichkeit zu geben, Attribute und Attributsausprägungen zu definieren. Mit diesen kann eine spätere Konfiguration des Modells und Auswertung des konfigurierten Modells erfolgen. Unterstützt wird die Modellierung hierbei durch die Konvention der Modellierung, welche

[25] Vgl. Rosemann/Schütte (1999) S. 27
[26] Vgl. Rosemann/Schütte (1999), S. 27 - 30

Begriffe und Modellbausteine vorgeben. Die Ergebnisse der Konstruktion des Referenzmodellrahmens werden in den Konventionen der Modellierung festgehalten.[27]

Phase 3 Konstruktion der Referenzmodellstruktur

Nachdem in der 2. Phase das „WAS“ spezifiziert wurde, wird nun das „WIE“ definiert. Dazu wird in dieser Phase die detaillierte Struktur des in Phase 2 vorgezeichneten Modells beschrieben. Ergebnis sind Referenzprozessmodelle und Referenzdatenmodelle sowie deren Verbindung. Diese Verfeinerung des Referenzmodellrahmens durch Prozess- und Datenmodelle repräsentiert die mit dem konstruierten Referenzmodell verbundene Problemdefinition. Zur Prüfung der Vollständigkeit und Qualitätskontrolle der detaillierten Modelle wird in dieser Phase eine Verifikation durch den Anwender durchgeführt.[28]

Phase 4 Komplettierung

Vor der Anwendung eines Referenzmodells sind Querverbindungen innerhalb des Modells notwendig. Diese spielen in Form interner Verbindungen eine Rolle und entsprechen dabei den Forderungen nach Konsistenz des Referenzmodells. Die durch Modelle und Restriktionen ermittelten zulässigen Anwendungen führen zur Verwendung des Referenzmodells. Des Weiteren sollten Referenzmodelle um quantitative Aussagen, wie u. a. Prozesslaufzeiten und Kosten, angereichert werden um die Modelle prüfen zu können und Anhaltspunkte für ein referenzmodellgestütztes Bewertung und den Vergleich geben zu können.[29]

Phase 5 Anwendung

In theoretischen Arbeiten wird meist das Augenmerk auf die Erstellung nicht aber auf die Anwendung von Modellen gelegt. Der Grund hierfür könnte die schwierige Verallgemeinerung von Faktoren einer Anwendung sein. Bei allgemeingültigen Referenzmodellen ist insbesondere die Phase der Anwendung zu berücksichtigen, da diese erst in

[27] Vgl. Rosemann/Schütte (1999), S. 31 - 32
[28] Vgl. Rosemann/Schütte (1999), S. 33 - 38
[29] Vgl. Rosemann/Schütte (1999). S. 38 - 39

einem bestimmten Anwendungsfall ihren Nutzen zeigen können. Daraus ist eine Gesamtbetrachtung von der Erstellung bis zur Anwendung erforderlich. Konstruktion und Anwendung bilden somit eine Einheit.

Mit diesem Vorgehensmodell und den Grundsätzen ordnungsgemäßer Modellierung steht ein Rahmen zur Verfügung, mit dessen Hilfe sich systematisch die Konstruktion eines Referenzmodells bis hin zur Anwendung durchführen lässt. [30]
Um die konsistente Modellierung zu unterstützen wird das in Kapitel 4 vorgestellte ARIS-Toolset zur Prozessmodellierung eingesetzt.

Weiteres Vorgehen

Die bereits vorgestellten Phasen der Referenzmodellierung werden in dieser Diplomarbeit umgesetzt. Dabei wird im Kapitel drei die Phase eins „Problemdefinition“ durchgeführt. Hierbei werden die Grundlagen der Managementsysteme bis hin zu dem ISMS und dessen Standard BS7799-2:2002 vorgestellt. Dem schließt sich in Kapitel vier die Betrachtung der Phasen zwei bis vier an. Dabei werden im ersten Abschnitt des Kapitels die Grundlagen der Architektur integrierter Informartionssysteme (ARIS), das ARIS-Toolset und im zweiten Abschnitt die Konventionen der Modellierung erläutert. Im dritten Abschnitt des vierten Kapitels schließt sich die Umsetzung der Modellierung an. Im fünften Kapitel wird die Phase fünf „Anwendung“ betrachtet.

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

3 Problemdefinition

Die in der ersten Phase geforderte Problemdefinition für diese Arbeit, findet sich in diesem Kapitel wieder. Dabei wird eine Einleitung in das Thema Managementsysteme geben sowie die Standards DIN EN ISO 9001:2000 für Qualitätsmanagementsysteme, BS7799-2:2002 sowie ISO/IEC17799:2000 für Informationssicherheits-Managementsysteme vorgestellt. Deren Bedeutung findet eine detaillierte Begründung.

3.1 Managementsysteme

Grundlage der Betrachtung der Managementsysteme ist die Definition des Begriffs.
Der Begriff Management wird als „Aufeinander abgestimmte Tätigkeiten zum Leiten und Lenken einer Organisation“[31] beschrieben. Ein Managementsystem wird als „System zum Festlegen von Politik und Zielen sowie zum Erreichen dieser Ziele„[32] definiert. Dabei wird die Politik als Gesamtabsichten und Ausrichtung einer Organisation in Bezug auf einen bestimmten Aspekt, wie von der obersten Führungsebene förmlich ausgedrückt, definiert.[33] Aspekte sind u. a. Qualitätsleistungen oder Informationssicherheitsleistungen.

Begründung von Managementsystemen

Ursprung der Managementsysteme liegt vor allem den USA.[34] Begründet liegen diese u. a. in den hohen Haftungsrisiken bei Produkten und in der Produktion. Dabei erreichen die Schadensansprüche nicht selten Höhen die den Kapitalwert einer Organisation übersteigen. Somit können diese Ansprüche deren Existenz bedrohen.
Dieses Risiko lässt sich vor allem durch Nachweis der Sorgfaltspflicht minimieren. Indem alle nach menschlichem Ermessen voraussehbaren Schadensfälle im Voraus berücksichtigt werden und Vorkehrungen getroffen werden, werden diese vermieden.
Um dieses Ziel zu erreichen muss deutlich gemacht werden, dass die Organisation von der Entwicklung bis zum Einsatz der Produkte oder Dienstleistungen diese wirksam mit

[31] DIN EN ISO 9000:2000, S.20
[32] DIN EN ISO 9000:2000, S.20
[33] Vgl. DIN EN ISO 9000:2000, S.20; Vgl. DIN EN ISO 14001:2004, S.11

Instruktionen und Produktbeobachtungen verfolgt und Verantwortlichkeiten regelt. Dies lässt sich vor allem durch schriftlichen Beweis der Durchführung und Dokumentation der Durchführungskontrolle bewirken. Ein Beispiel hierfür sind Qualitätsmanagementsysteme. „Qualitätsmanagementsysteme sorgen dafür: sie beschreiben die Tätigkeiten in der Organisation, legen Umfang und Form der Aufzeichnungen über getroffene Maßnahmen fest und beinhalten Verfahren zu dokumentierten Kontrolle der Durchführung.“[35] Somit lässt sich stets die Einhaltung der Sorgfaltspflicht nachprüfen.

Ein weiterer Grund der Einführung von Managementsystemen ist die Ausweitung von Kunden-Lieferanten-Beziehungen. Durch die breite Einführung von Qualitätsmanagementsystemen und dem nahezu parallel laufenden Trend des Outsourcings haben sich die Organisationen auf ihre Kernkompetenzen wie beispielsweise Entwicklung, Montage, Vertrieb zurückgezogen. Dies führte einerseits zu einer Ausgliederung, dem Outsourcing, und andererseits zu einer stärkeren Bindung und Verantwortung der Lieferanten. Dabei spielen aber auch die Minimierung der Transaktionskosten zwischen allen beteiligten Akteuren sowie Probleme bei der Delegation eine wesentliche Rolle. Wobei eines der Hauptprobleme der Delegation darin liegt, dass der Ausführende nicht im Sinne des Auftraggebers handelt. Dabei nimmt diese Gefahr mit abnehmender Kontrolle durch den Auftraggeber zu. In diesem Zusammenhang sind auch notwendige moralische Standards, wie beispielsweise die Vertrauenswürdigkeit, Aspekte die nicht außer Acht gelassen werden können. Angesichts der Unvollständigkeit von Verträgen, lassen sich in diesen, durch die Vertragspartner mit einem mehr oder weniger großen Aufwand Vertragslücken ausnutzen. Durch Vertrauenswürdigkeit der Partner ist die Ausgestaltung von Verträgen wesentlich unkomplizierter.

Ein weiterer Aspekt ist die gesellschaftliche Differenzierung welche neue Anspruchsgruppen schafft. Dabei werden vier Handlungssphären in modernen sozialen Systemen wie Organisationen unterschieden. Diese sind nach Parson die Kommunikation, Gemeinschaft, Ökonomie und Politik.[36] Dabei hat das ökonomische Teilsystem die Aufgabe sich schnell an Veränderungen anzupassen. Das politische Teilsystem sorgt dafür, dass sich das Gesamtsystem nicht beliebig verhält. Das gemeinschaftliche Teilsystem ist für die Integration aller Akteure auf den verschieden Handlungsfeldern in das Gesamtsystem da sowie das kommunikative Teilsystem, welches den Sinn des gesamten Sys-

[34] Vgl. Michael/Morawietz (1995), S. 1
[35] Ahrens (2001), S. 3
[36] Parson (2001), S. 3 - 24

tems reflektiert. Diese Differenzierung bringt den Vorteil der Spezialisierung für bestimmte Aufgabenbereiche innerhalb der sozialen Systeme. Die vier genannten Handlungssphären interagieren dabei untereinander. „In gut funktionierenden Gesellschaften werden Unternehmen also trotz ihrer wirtschaftlichen Autonomie mit Forderungen konfrontiert, die Ursprung in anderen Handlungssphären haben.“[37] Dabei werden u. a. Informationssicherheit und Qualität gefordert.

Durch den Einfluss unterschiedlicher Handlungssphären lassen Managementsysteme als Indikator für Eigen- und Fremdsteuerung nutzen. Dabei liegt der Grund für das Vorhanden sein der geregelten Managementsystemen in der Fremdsteuerung[38], welche beispielsweise durch gesetzliche Regeln eingreift. Durch Forderungen, wie beispielsweise die bereits genannte Informationssicherheit oder Qualität, führt diese zu mehreren geregelten Managementsystemen in einer Organisation.

Ein weiterer Grund für die Einführung von Managementsystemen ist die zunehmende Komplexität in Organisationen und Technik. Dabei könnte die Reduktion von Komplexität u. a. Vereinfachung interner Prozess und Strukturen, dazu führen, die Umgebung nicht mehr adäquat abbilden zu können und dadurch falsch zu handeln. Eine Empfehlung ist es deshalb die Komplexität innerhalb der Organisationen zu steigern. Um diese zu beherrschen wird Unterstützung benötigt. „Im Unternehmen geschieht dies u. a. mit Hilfe von Managementsystemen.“[39] Des Weiteren kommt die stetige Zunahme der Technikkomplexität hinzu. Diese können zu Größenordnungen führen die nur noch schwer beherrschbar sein können. In diesem Hintergrund können Managementsysteme einen Beitrag zur Beherrschung der Komplexität leisten in dem sie es ermöglichen in einer komplexen Organisation mit komplexen technischen Systemen Verantwortung zurechnen zu können.

Dabei ist die Gemeinsamkeit aller Managementsysteme die Komplexitätsbeherrschung durch Dokumentation, explizite Verantwortungszurechnung und dokumentierte Kontrolle und nachzuweisende Verbesserung nachdem Mängel bekannt werden. [40]

---

[37] Ahrens (2001), S. 11

[38] Forderungen, u. a. gesetzliche Vorschriften, werden an die Organisation gerichtet und müssen von dieser erfüllt werden.

[39] Ahrens (2001), S. 14

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

Grundelemente, Gestaltungsregeln und Nutzen von Managementsystemen

Was sind Managementsysteme

„In der Praxis findet man zwei grundsätzlich verschieden Formen von Managementsystemen.“[41] Die quasi natürliche, nicht genormte Managementsysteme und durch Gesetze, Vorgaben und Normen geregelt Managementsysteme. Natürliche Managementsysteme beziehen sich dabei auf die Kernaufgabe, die Wertschöpfung, der Organisation. Sie umfassen im Wesentlichen die Zieldefinition, die Durchsetzung der Maßnahmen zur Zielerreichung sowie die Erfolgskontrolle. Aspekte der Wertsicherung oder Zukunftsrichtung werden bei diesen jedoch vernachlässigt.
Die durch Gesetze, Vorgaben und Normen geregelten Managementsysteme resultieren aus deren Anforderungen und der Erfüllung dieser Anforderungen. Sie bleiben dabei thematisch in der Regel vom Management der Wertschöpfungsprozesse getrennt und spezialisieren sich auf die Forderungen wie beispielsweise Qualitätsanforderungen oder Informationssicherheitsanforderungen.
Allgemein entstehen Managementsysteme immer dann, wenn die Komplexität der Aufgaben ein geplantes Vorgehen einer Organisation erfordert. Dabei bedeutet Komplexität in diesem Zusammenhang, dass sich die Entwicklung eines Systems nicht mit Hilfe einfacher Ursache-Wirkungsbeziehungen vorhersagen oder beeinflussen lässt. Der Begriff des Systems wird definiert als selbständige Teile, die reguliert zusammenarbeiten und damit ein Gefüge bilden.[42]

Nutzen von Managementsystem

Nachdem der Grund für das Vorhandensein von Managementsystemen herausgestellt wurde und geklärt werden konnte was Managementsysteme sind, lässt sich deren Nutzen in fünf Punkten gemäß Hofmann-Kamensky zusammenfassen[43].

- Regeln und Prinzipien, welche das Verhalten einer Organisation vorausschauend lenken, sowie die Vermittlung der Sinnfälligkeit dieser Regeln

[41] Hofmann-Kamensky (2001), S. 19
[42] Vgl. DIN EN ISO9000:2000, S. 20
[43] Vgl. Hofmann-Kamensky (2001), S. 27

- Verbindung der Organisation zu Markt und Gesellschaft um die Existenz- und Entwicklungsfähigkeit zu erhalten
- Abbildung von Markt- und Rahmenbedingung welche Anforderung darstellen und die Übertragung dieser Anforderungen in Aufgaben
- Tätigkeitsbegleitendes Lernen und eine Speicherung des erworbenen Wissens
- Vorsorge und Wertsicherung zur Erhaltung

Gestaltungsregeln

Wesentlicher Punkt bei Managementsystemen ist es, die Logik und den Zusammenhang erkennen zu können. Dazu werden im Folgenden grundlegende Gestaltungsregeln für Managementsysteme erklärt. Diese geben ein Konstruktionsprinzip an, wie ein solches Managementsystem gemäß Hofmann-Kamensky geschaffen werden kann[44].

- Informationen über den Sinn und die Grundregeln
  Diese halten den Sinn und die Gestaltungsregeln einer Organisation fest. Die Grundregeln müssen dabei aktiv in der Organisation kommuniziert werden.
- Information über den Bauplan der Organisation
  „Das Managementsysteme ist eine Blaupause der planenden, sinn- und wertschöpfenden sowie wertsichernden Tätigkeiten“[45]
- Verhaltensspielräume und sichere Einhaltung von Vorgaben schaffen
  Hierbei sollten das Sollverhalten allgemein zu beschreiben und die dabei erwarteten Ergebnisse, keine Regeln ohne Begründung und Risikoangabe, die Anzahl der Verhaltensoptionen bei hohem Risiko minimiert und die Komplexität bei Verhaltensoptionen bei Prozessen ohne konkretes Ergebnis festgelegt werden
- Dauernde, schrittweise Verbesserung durch Regelkreise (kontinuierliche Verbesserung)
  „Die ständige Suche und Umsetzung von Verbesserungen in der Effizienz der Gesamtorganisaton und in der Effektivität gegenüber externen und internen Kunden ist ein Dauerprozess der in Form von Regelkreisen zu organisieren ist.“[46] Einen solchen Regelkreis beschreibt das PDCA-Konzept, welches im folgenden Abschnitt erläutert wird.

[44] Vgl. Hofmann-Kamensky (2001), S. 26 - 37
[45] Hofmann-Kamensky (2001), S. 29
[46] Hofmann- Kamensky (2001), S. 31

- Selbstorganisation zulassen
  Diese Gestaltungsregel empfiehlt möglichst weitgehende Eigenregelung der Organisationsbereiche durch Sollwerte oder Regeln, welche in einem Gesamtplan in Beziehung stehen. Ausschließlich Abweichungen werden berichtet.
- Schnittstellen für Aufnahme und Abgabe von Informationen schaffen
  Für die Organisation ist die Vernetzung mit dem Umfeld eine Möglichkeit Informationen aufzunehmen bzw. abzugeben. Dabei spielt nicht nur externe sondern auch die interne Vernetzung eine Rolle. Die interne ermöglicht es mit den Mitarbeitern zu kommunizieren, während die externe eine Kommunikation mit übergeordneten Systemen erlaubt.
- Weiterentwicklung und Lernen organisieren
  Weiterentwicklung kann zur Verbesserung des Erfolgs führen und dadurch die Organisation stärken. Somit sollte das Managementsystem das Wissen und Lernen organisieren, die kontinuierliche Verbesserung suchen und häufige interne sowie externe Bewertung ermöglichen. Darüber hinaus das Speichern von Wissen unterstützen, die Möglichkeiten zu dessen Transfer schaffen sowie ausreichend Informationen für Planung, Strategie, Informationsgewinnung und notwenigen Ressourcen organisieren.

3.1.1 Der PDCA-Kreislauf

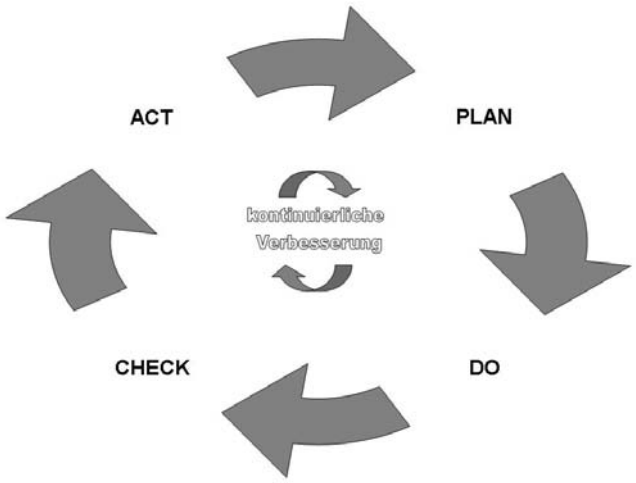
Das Konzept des PDCA-Kreislaufs wurde erstmals in den 1930er Jahren von Walter A. Shewhart bei den Bell Laboratories entwickelt. In den 1950er Jahren wurde das Konzept von seinem Schüler W. Edwards Deming, einer führenden Autorität auf dem Gebiet des Qualitätsmanagements, weiterentwickelt. Es ist heute als Deming- oder PDCA-Kreislauf bekannt.
Mit PDCA werden die nachstehenden Stufen (siehe Abbildung 3.1) im Rahmen eines kontinuierlichen Verbesserungsprozesses bezeichnet. Jede Aktivität ist ein Prozess. Das Ergebnis jedes Prozesses muss durch geeignete Kennzahlen messbar sein und muss auch gemessen werden. Dabei dienen Kennzahlen der Objektivierung und Visualisierung von Organisationszielen und Verbesserungsbemühungen.

Plan: Identifikation der im Prozessablauf auftretenden Schwächen und Fehler; Entwicklung von Ideen zur Verbesserung und Planung

Do: Ausführung der geplanten Verbesserungen zunächst auf einer Test-Ebene. Der Prozess selbst wird auf diese Weise nicht beeinträchtigt.

Check: Überprüfung, ob die durchgeführten Maßnahmen zur Verbesserung des Prozesses führen.

Act: Auf dieser Stufe des PDCA-Kreislaufs werden die Ergebnisse analysiert, Verbesserungspotentiale identifiziert und weitere Maßnahmen beschlossen. [47]



In Anlehnung an Kaminske/Brauer (2003), S. 296

Abb. 3.1: PDCA-Kreislauf

Die vier benannten Stufen fügen sich zu einem Kreislauf, wie in Abbildung 3.1 dargestellt, zusammen und unterstützten somit den Prozess der kontinuierlichen Verbesserung. Dieser Prozess wurde dabei in den Standards BS7799-2:2002 und ISO9001:2000 umgesetzt.

3.2 Qualitätsmanagementsysteme

In der Begründung der Managementsysteme wurde bereits auf die Qualitätsmanagementsysteme eingegangen. Im folgenden Abschnitt soll dazu der DIN EN ISO

[47] Vgl. DIN EN ISO140001:2004, S. 7

9001:2000 Standard betrachtet werden, welcher Anforderungen an Qualitätsmanagementsysteme beschreibt. Der Begriff Qualität wird dabei als „Vermögen einer Gesamtheit inhärenter Merkmal eines Produktes, Systems oder Prozesses, zur Erfüllung von Forderungen von Kunden und anderen interessierten Parteien“[48] definiert. Ein Kunde stellt eine „Organisation oder Person, die ein Produkt empfängt“[49], während interessierte Parteien Personen oder Gruppen mit einem Interesse an der Leistung oder dem Erfolg einer Organisation sind.[50] Somit stellt ein Qualitätsmanagementsystem ein „Managementsystem zum Leiten und Lenker einer Organisation bezüglich der Qualität“[51] dar.

3.2.1 DIN EN ISO 9001:2000 Qualitätsmanagementsysteme

Mit der Standardreihe der DIN EN ISO 9000 sind Standards geschaffen worden, welche die Grundsätze für Maßnahmen zum Qualitätsmanagement dokumentieren. Gemeinsam bilden sie einen zusammenhängenden Satz von Normen für Qualitätsmanagementsysteme, welche das gegenseitige Verständnis auf nationaler und internationaler Ebene erleichtern sollen.

Jedes Produkt unterliegt anderen spezifischen Anforderungen und ist demnach nur unter individuellen Qualitätssicherungsmaßnahmen zu erzeugen. Qualitätsmanagementsysteme hingegen sind nicht produktorientiert und können daher unabhängig von der Branche und den spezifischen Produkten einen ähnlichen Aufbau festlegen.

Das erfolgreiche Führen und Betreiben einer Organisation erfordert, dass sie in systematischer und klarer Weise geleitet und gelenkt wird. Ein Weg zum Erfolg kann die Einführung und Aufrechterhaltung eines Managementsystems sein, das auf ständige Leistungsverbesserung ausgerichtet ist, indem es die Erfordernisse aller interessierten Parteien berücksichtigt. Eine Organisation zu leiten und zu lenken umfasst neben anderen Managementdisziplinen auch das Qualitätsmanagement.

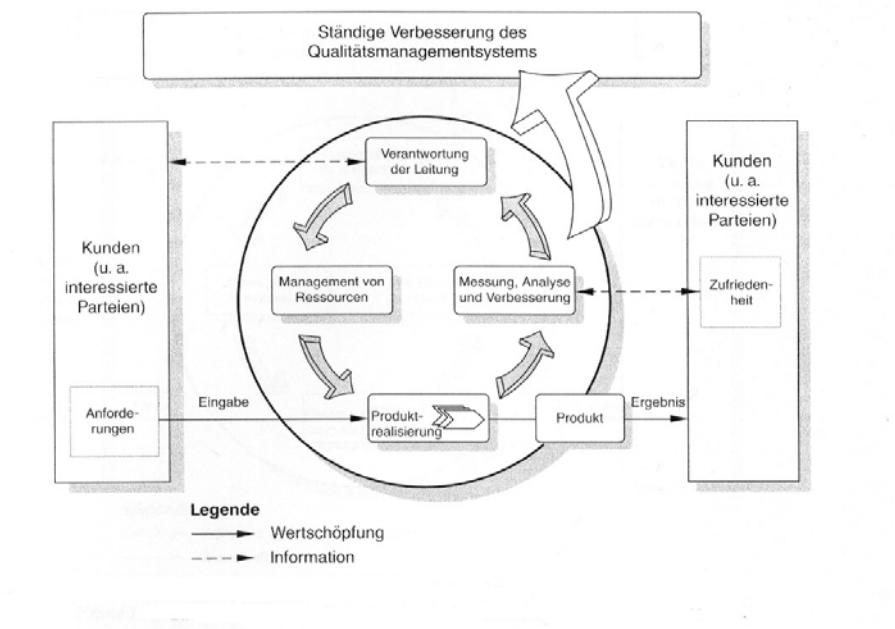
Die Standards der DIN EN ISO 9000 Reihe sind grundsätzlich prozessorientiert aufgebaut. Die Vorgängernormen definierten 20 Elemente des Qualitätsmanagements, die den Standardprozessen der produzierenden Industrie von der Entwicklung über Produk-

[48] DIN EN ISO9000:2000, S. 18
[49] DIN EN ISO9000:2000, S. 23
[50] Vgl. DIN EN ISO9000:2000, S. 23

tion und Montage bis zum Kundendienst entsprachen, so dass der Aufbau der DIN EN ISO 9000:1994 die Übertragung z. B. auf Dienstleistungsorganisationen erschwerte.[52]

Inhalte der DIN EN ISO 9000-Standardreihe

Die DIN EN ISO 9000:2000 definiert Grundlagen und Begriffe zu Qualitätsmanagementsystemen.



Quelle: DIN EN ISO 9001:2000 S.13

Abb. 3.2 Umgesetztes PDCA-Konzept im Qualitätsmanagement

Es werden die Grundlagen für Qualitätsmanagementsysteme und die in der Standardreihe DIN EN ISO 9000 verwendeten Begriffe erläutert. Auch der prozessorientierte Ansatz des Qualitätsmanagements basierend auf dem PDCA-Kreislauf (siehe Abbildung 3.2). Die DIN EN ISO 9000:2000 wurde im Jahr 2005 überarbeitet, um einheitliche Begriffsdefinitionen für die Normen DIN EN ISO 9001:2000 und DIN EN ISO 19011:2002 erweitert, und als DIN EN ISO 9000:2005 Ende 2005 veröffentlicht.

[51] DIN EN ISO9000:2000, S. 20
[52] Vgl. DIN EN ISO9000:2000, S. 6

ISO 9001:2000

Der DIN EN ISO 9001:2000 Standard legt die Anforderungen an ein Qualitätsmanagementsystem für den Fall fest, dass eine Organisation ihre Fähigkeit darlegen muss Produkte bereitzustellen, welche die Anforderungen der Kunden und behördliche Anforderungen erfüllen und anstrebt, die Kundenzufriedenheit zu erhöhen.

Diese Norm beschreibt modellhaft das gesamte Qualitätsmanagementsystem und ist Basis für ein umfassendes Qualitätsmanagementsystem.

Die acht Grundsätze des Qualitätsmanagements gemäß DIN EN ISO 9000:2000[53]:

- Kundenorientierung
- Führung
- Einbeziehung der Personen
- Prozessorientierter Ansatz
- Systemorientierter Managementansatz
- Kontinuierliche Verbesserung
- Sachbezogener Entscheidungsfindungsansatz
- Lieferantenbeziehung zu gegenseitigem Nutzen

Die Einführung eines Qualitätsmanagementsystems ist eine strategische Entscheidung für eine Organisation, die sich stärker an ihren Kunden orientieren will, um Wettbewerbsvorteile zu erlangen. Dieser Standard bietet dazu die nötige Grundlage. Er gibt einen bestimmten Rahmen vor, der viel weiter gefasst ist als die Vorgängerstandards.

Der prozessorientierte Ansatz basiert auf den vier Hauptprozessen einer Organisation, welche einen Input in einen Output umwandeln.

Die vier Hauptkapitel gemäß DIN EN ISO 9001:2000 sind[54]:

- Verantwortung der Leitung
- Management von Ressourcen

[53] Vgl. DIN EN ISO 9000:2000 S. 6 - 7

- Produktrealisierung
- Messung, Analyse und Verbesserung

Die Norm betrachtet diese Prozesse und vergleicht die Eingabe mit der Ausgabe. Die aktuelle DIN EN ISO 9001 wurde letztmalig im Jahr 2000 überarbeitet (9001:2000). Die nächste Veröffentlichung ist für das Jahr 2008 geplant.

Bedeutung der Betrachtung des DIN EN ISO 9001:2000 Standards

Die hier betrachtete DIN EN ISO9001:2000 stellt ein Beispiel für ein Managementsystem dar welches standardisierte ist und weit verbreitet Anwendung findet. Darüber hinaus stellt es die Grundlage weiterer Standardisierungen von Managementsystemen wie dem Informationssicherheits-Managementsystem dar.

3.3 Informationssicherheits-Managementsysteme

Kernpunkt dieser Arbeit ist die Abbildung von Prozessen eines Informationssicherheits-Managementsystem nach BS7799-2:2002. Dazu werden im folgenden Abschnitt die Bedeutung der Informationssicherheit in Organisationen erläutert und der BS7799-2:2002 Standard, welcher die Anforderungen an ein solches Managementsystem beschreibt.

Vom Zeichen zur Information

Ausgangspunkt der Informationssicherheit ist eine Definition von Information. Dieser ist heute ein sehr weitläufig verwendeter und daher auch sehr schwer abzugrenzender Begriff. Dazu wird die Entwicklung vom Zeichen zur Information erläutert.
Daten bestehen aus, zum Zwecke der Verarbeitung, zusammengefassten Zeichen. Sie sind dabei isolierte und uninterpretierte Fakten und Werte der Realitätsbeschreibung. Informationen sind verknüpfte und mit Bedeutung versehene Daten. Dabei lässt sich die

[54] Vgl. EN DIN ISO 9001:2000, S.20 - 34

Information als „Daten mit Bedeutung“[55] definieren. Daten sind also noch weitgehend bedeutungslos, stehen jedoch für sich allein und sind für prinzipiell jedermann abrufbar. Für Informationen gilt hingegen, dass jemand sie in Bezug zueinander gesetzt und ihnen damit Bedeutung verliehen haben muss. Man kann das wie folgt zusammenfassen: Daten müssen interpretiert und verknüpft werden, um Informationen zu gewinnen.

Informationen sind in den letzten Jahren immer mehr zum Produktionsfaktor geworden und stehen nun in gleicher Bedeutung wie Produktionsfaktoren Boden, Kapital und Arbeit. Somit ergibt sich der Schutzbedarf der Informationen als Produktionsfaktor, woraus sich der Begriff der Informationssicherheit ergibt.[56]

Informationen in Organisationen

Innerhalb der Organisationen lässt sich eine Differenzierung zwischen Dokumenten und Aufzeichnungen, welche im Folgenden definiert werden, feststellen.
Dabei stellt ein Dokument „Information und ihr Trägermedium“[57] dar, während eine Aufzeichnung als „Dokument, das erreichte Ergebnisse angibt oder einen Nachweis ausgeführter Tätigkeiten bereitstellt“[58] definiert wird. Ein Dokument kann Papier, eine magnetisches, elektronisches oder optisches Speichermedium, eine Fotografie, ein Bezugsmuster oder eine Kombination daraus sein[59].

Informationssicherheit

Durch den Schutzbedarf bzw. dem Bedarf der Sicherung der Information erfordert es einer Abgrenzung der Informationssicherheit. Sicherheit im Allgemeinen gilt als Grundbedürfnis der Menschen und hat somit den gleichen Stellenwert wie die Versorgung mit Lebensmitteln. Dabei ist das Hauptinteresse die Erhaltung und der Schutz des Vermögens. Dies lässt sich wiederum auf die Sicherheit der Informationen in Organisationen beziehen. Durch die Einordnung der Information als Produktionsfaktor ist die

[55] DIN EN ISO 9000:2000, S. 28
[56] Vgl. Görtz/Stolp (1999), S. 15
[57] DIN EN ISO 9000:2000, S. 29
[58] DIN EN ISO 9000:2000, S. 29
[59] Vgl. DIN EN ISO 14001:2004, S. 10

Sicherheit dieser ein wichtiges Grundbedürfnis der Organisationen. Daraus lässt sich der Bedarf an Informationssicherheit erklären.[60]

Allgemein lässt sich Informationssicherheit wie folgt definieren:

„Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen“.[61]

Dabei stellt die Integrität die „Sicherstellung der Richtigkeit und Vollständigkeit der Informationen und Verarbeitungsmethoden“[62], die Vertraulichkeit „Gewährleistung des Zugangs zu Informationen nur für Zugangsberechtigte“[63] und die Verfügbarkeit „Gewährleistung des bedarfsorientierten Zugangs zu Informationen und zugehörigen Werten für berechtigte Benutzer“[64] dar.

Zu Gewährleistung der Informationssicherheit ist auch die Unterstützung des Staates und seiner Institutionen notwendig, besonders in Bezug auf die Standardisierung geeigneter Vorgehensweisen.

„Informationssicherheit in der Informationsgesellschaft ist ein wichtiger Teil der Sicherheitspolitik, um die sich auch der Staat zu kümmern hat [...].“[65]

Bedrohungen

Durch die zunehmende Globalisierung und Vernetzung, dem technologischen Fortschritt und des breiteren Allgemeinwissens nehmen die Bedrohungen ständig zu.

Vor wenigen Jahren war die IT eine „Wissenschaft“, welche nur wenigen Experten vorbehalten war, während heute entsprechendes Know-how und Hardwareausstattung für einen möglichen Angriff auf die Informationssicherheit einer Organisation nahezu an jedem Punkt der Erde vorhanden und möglich ist.

Dabei können Angriffe mit kleiner Ursache eine große Wirkung zeigen, wie beispielsweise die „denail of service“-Angriffe beweisen. Diese setzen durch tausende gleichzeitige Zugriffe Server oder Netzwerke außer Kraft.

Aber auch natürlicher Ereignisse, wie z.B. Wassereinbruch Erdbeben, sowie Brand, Einbruch oder Ausfall der Stromversorgung stellen Bedrohungen dar.[66]

---

[60] Vgl. Görtz/Stolp (1999), S. 16
[61] BS7799-2:2002, S.4
[62] BS7799-2:2002, S.4
[63] BS7799-2:2002, S.4
[64] BS7799-2:2002, S.4
[65] Görtz, Stolp (1999), S.17

Allgemein lässt sich eine Bedrohung als Aktion oder Ereignis, dass der Sicherheit schaden kann, definieren.[67]

Schwachstellen

Während vor einigen Jahren monolitische Softwaresysteme und Großrechnersysteme im Einsatz waren, sind es heute komponentenbasierte Softwarepakete mit dynamischen Bibliotheken, Plug-ins[68] und Client-Serversysteme[69], welche oft firmenintern oder über das Internet vernetzt sind.
Dabei zeigen diese Systeme durch die verschieden Arten der Anbindung, sei es die feste Vernetzung von PCs, Fernzugriffe, die drahtlose Anbindung von Notebooks und viele mehr, sowie durch die hohe Komplexität der Software eine Vielzahl von Schwachpunkten welche durch Angriffe ausgenutzt werden können.[70]
Eine Schwachstelle ist eine Sicherheitsschwäche, die es möglich macht dass eine Bedrohung eintreten kann.[71] Dabei kann eine Bedrohung mit einer bestimmten Wahrscheinlichkeit eintreten. Die Wahrscheinlichkeit stellt in diesem Zusammenhang die relative Häufigkeit des Auftretens einer Bedrohung dar.

Maßnahmen

Immer mehr Computersysteme unterstützten die Bearbeitung von Geschäftsprozessen, damit steigt auch die Abhängigkeit von diesen Systemen und der Bedarf diese zu schützen. Um mit dieser Entwicklung Schritt halten zu können, ist es daher notwendig, kontinuierliche die Maßnahmen zu verbessern und entsprechende Ressourcen bereitzustellen um die Effektivität des Informationssicherheitsmanagements beständig zu verbessern.

---

[66] Vgl. Hornberger/Schneider (2000), S. 17 - 35
[67] Vgl. ITSEC (1998), S. 116
[68] Ein Plugin ist ein Ergänzungs- oder Zusatzmodul und ist eine gängige Bezeichnung für ein Computerprogramm, das in ein anderes Softwareprodukt "eingeklinkt" wird.
[69] Ein Client-Server-System besteht aus einem Client, der eine Verbindung mit einem Server herstellt. Der Server stellt einen Dienst zur Verfügung während der Client den Dienst des Servers in Anspruch nimmt.
[70] Vgl. Müller (2003), S. 1
[71] Vgl. Bishop (2003), S. 498

Eine Maßnahme lässt sich dabei als eine Handlung oder eine als zusammengehörig verstandene Summe von Handlungen, die der Verwirklichung von Zielen dienen soll, definieren.[72]

Informationssicherheits-Management

Informationssicherheit ist grundsätzlich eine Aufgabe der Leitung einer Organisation und sollte nach einem Top-Down Ansatz aufgebaut sein. Entsprechende Verpflichtungen lassen sich u. a. im deutschsprachigen Raum aus den verschiedenen Gesetzen zum Gesellschaftsrecht, Haftungsrecht, Datenschutz, Bankenrecht herleiten. Dennoch wurde und wird das Thema Informationssicherheit in vielen Organisationen ausschließlich durch die IT-Abteilungen vorangetrieben. Zwar gibt es im Bereich der IT-Sicherheit sehr viele Technologien und Methoden, welche die die Umsetzung der Informationssicherheitskonzepte unterstützen, diese Maßnahmen müssen jedoch in ein ganzheitliches Informationsschutz-Konzept eingebettet sein und vom obersten Management aktiv unterstützt und verantwortet werden. Insbesondere die Verabschiedung von einer Politik zu Informationsschutz und Sicherheitsrichtlinien ist Aufgabe des obersten Managements. Da das Management in der Regel nicht selbst diese Politik ausarbeitet, sollte eine Stelle oder Gruppe eingesetzt werden, die für die Formulierung sowie der Überwachung ihrer Einhaltung innerhalb der Organisation verantwortlich ist.[73]

Informationssicherheits-Managementsystem

„Der Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung der Informationssicherheit abdeckt.“[74]
Die Umsetzung eines solchen Systems erfordert dabei ein standardisiertes Vorgehen. Dies wird durch die Institutionen des Staates unterstützt, die durch Normen und Standards ein einheitliches Vorgehen ermöglichen und somit den Bedarf eines gemeinsamen anerkannten Standards im Vorgehen der Informationssicherheit decken. Einen solchen stellt der in dieser Arbeit betrachtete BS7799-2:2002 Standard des British Standards

[72] Olev (2006)
[73] Vgl. Müller (2003), S. 14
[74] BS7799-2:2002, S. 4

Institution (BSI) dar. Er ordnet sich dabei in eine Reihe vieler nationaler und internationaler Standards, Normen und Richtlinien ein.

Weiter Begriffe im Zusammenhang mit dem ISMS

In diesem Abschnitt werden weitere Begriffe, die im Zusammenhang mit dem Informationssicherheits-Managementsystemen Anwendung finden, vorgestellt.
Die Risikoakzeptanz welche eine „Entscheidung, ein Risiko zu akzeptieren“[75] darstellt. Die Risikoeinschätzung stellt ein „allgemeines Verfahren zur Risikoanalyse und Risikoevaluation“[76] dar. Dabei wird die Risikoanalyse als „systematische Anwendung von Informationen zur Identifikation von Risikoquellen und zur Abschätzung des Risikos“ [77] definiert, während Risikoevaluation ein „Verfahren für den Vergleich des abgeschätzten Risikos mit den festgelegten Risikokriterien für die Bestimmung der Bedeutung des Risikos“[78] darstellen. Die Risikobehandlung ist ein „Behandlungsprozess für die Auswahl und Umsetzung von Maßnahmen zur Modifizierung des Risikos“.[79] Das Risikomanagement wird als „koordinierte Aktivitäten zur Leitung und Steuerung einer Organisation im Hinblick auf Risiken“[80] definiert.

3.3.1 Einordnung des BS7799-2

Im Bereich des Informationssicherheits-Management existieren viele verschiedene Standards, Normen und Richtlinien. Hier soll nun der BS7799-2:2002 in die Gruppe bekanntesten Vertreter eingeordnet werden. Diese werden im Folgenden in kurzer Form vorgestellt.

[75] BS7799-2:2002, S. 5
[76] BS7799-2:2002, S. 5
[77] BS7799-2:2002, S. 5
[78] BS7799-2:2002, S. 5
[79] BS7799-2:2002, S. 5
[80] BS7799-2:2002, S. 5

IT-Grundschutzhandbuch

Das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik empfiehlt Standard-Sicherheitsmaßnahmen für typische IT-Anwendungen und IT-Systeme. Das Ziel dieser Empfehlungen ist, ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann.
Die im IT-Grundschutzhandbuch zusammengestellten Standardsicherheitsmaßnahmen orientieren sich dabei an einem Schutzbedarf, der für die meisten IT-Systeme zutrifft.
Damit kann für die überwiegende Zahl der IT-Systeme der bislang arbeitsintensive Prozess der Erstellung eines IT-Sicherheitskonzepts erheblich vereinfacht werden, da aufwendige und oft komplexe Analysen von Bedrohungen und Eintrittswahrscheinlichkeiten entfallen. Mit Verwendung des Handbuchs bedarf es lediglich eines Abgleichs der Soll-Maßnahmen mit den Ist-Maßnahmen, um Sicherheitsdefizite zu ermitteln und passende Sicherheitsmaßnahmen zu identifizieren. [81]

ITSEC

In den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) sind drei unterschiedliche Arten der Sicherheitspolitik definiert. Die firmenspezifische, die systemspezifischen und die technische Sicherheitspolitik.
Sie enthalten Gesetze, Regeln und Praktiken.[82] Die Sicherheitspolitik stellt hierbei die Gesamtabsichten und Ausrichtung einer Organisation in Bezug auf ihre Sicherheitsleistungen, wie von der obersten Führungsebene förmlich aufgedrückt dar.[83]

ISO/IEC TR 13335-1

Die ISO/IEC TR 13335-1:2004 unterscheidet zwischen drei Arten der Sicherheitspolitik. Der organisationsweiten Sicherheitspolitik, der organisationsweiten IT-Sicherheitspolitik und die Sicherheitspolitik des IT-Systems. Dabei enthält die orgnisationsweite Sicherheitspolitik die Sicherheitsprinzipien und –direktiven für die gesamte

[81] Vgl. IT-Grundschutzhandbuch (2006)
[82] Vgl. ITSEC (1998) S. 7 - 55
[83] Vgl. DIN EN ISO 9000:2000, S.20; Vgl. DIN EN ISO 14001:2004, S.11

Organisation. Die organisationsweite IT-Sicherheitspolitik spiegelt sowohl die grundlegende Prinzipien und -direktiven als auch die für den Einsatz von IT-Systemen und die Sicherheitspolitik des IT-Systems, welche die Sicherheitsprinzipien der IT-Sicherheitspolitik, die spezifischen Sicherheitsanforderungen und Schutzmaßnahmen beinhaltet, wieder. Darüber hinaus wird ein hierarchischer Ansatz gewählt, der die unterschiedlichen Sicherheitspolitiken definiert.[84]

ISO 15408 (Common Criteria CC)

Die Common Criteria for Information Technology Security Evaluation (kurz auch Common Criteria; deutsch etwa: Gemeinsame Kriterien für die Bewertung der Sicherheit von Informationstechnologie) ist ein internationaler Standard über die Kriterien der Bewertung und Zertifizierung der Sicherheit von Computersystemen in Hinblick auf Datensicherheit und Datenschutz. Der Common Criteria Standard soll eine gemeinsame Grundlage für solche Bewertungen bieten. Dabei umfassen die Common Criteria drei Teile.
Dabei wird die Zertifizierung als Prüfung einer Organisation durch einen unabhängigen Dritten zum Erhalt eines Zertifikats, das die Übereinstimmung (Konformität) der Organisation oder von Organisationsbereichen mit bestimmten Anforderungen oder Normen ausdrückt.[85]

Teil 1: Einführung und allgemeines Modell

Hier werden die Grundlagen der IT-Sicherheitsevaluation und der allgemeine Geltungsbereich der CC erläutert. In den Anhängen werden Schutzprofile und Sicherheitsvorgaben für den zu prüfenden Evaluationsgegenstand beschrieben.[86]

Teil 2: Funktionale Sicherheitsanforderungen

Dieser Teil enthält einen umfangreichen Katalog von Funktionalitätsanforderungen. Er stellt ein empfohlenes Angebot für die Beschreibung der Funktionalität eines Produktes

[84] ISO/IEC TR 13335-1:2004 S. 1 - 25
[85] Vgl. Bruhn (2004), S. 291
[86] Vgl. ISO 15408-1:2005

bzw. Systems dar, von dem jedoch in begründeten Fällen abgewichen werden kann. Im Anhang finden sich Hintergrundinformationen. Zusätzlich werden Zusammenhänge zwischen Bedrohungen, Sicherheitszielen und funktionalen Anforderungen aufgezeigt.[87]

Teil 3: Anforderungen an die Vertrauenswürdigkeit

Hier sind die Anforderungen an die Vertrauenswürdigkeit aufgelistet. Wichtig ist, dass ein Evaluationsergebnis immer auf einer Vertrauenswürdigkeitsstufe basieren sollte, eventuell ergänzt durch weitere Anforderungen. Die CC geben sieben hierarchische Stufen vor.[88]

ISO 17799

Die ISO/IEC 17799:2000 definiert sich als „umfassende Auswahl an Kontrollmechanismen, die auf Methodik und Verfahren basieren, die sich in der Informationssicherheit bewährt haben“[89], so genannte best practices. Die Grundlage für die Standardisierung bildete hierbei eine Aufstellung von Erfahrungen, Verfahren und Methoden aus der Praxis im Sinne eines „best practice“ Ansatzes. Sie werden im Weiteren detailliert betrachtet.

BS7799-2

Der BS7799-2:2002 beinhaltet ein Modell, welches den Führungskräften und Mitarbeitern einer Organisation die Einführung und den Betrieb eines effektiven Informationssicherheits-Managementsystems erlaubt. Dabei spielt der vorgestellte Kreislauf der kontinuierlichen Verbesserung eine wesentliche Rolle. Im Folgenden wird dieser Standard detaillierter vorgestellt.[90]

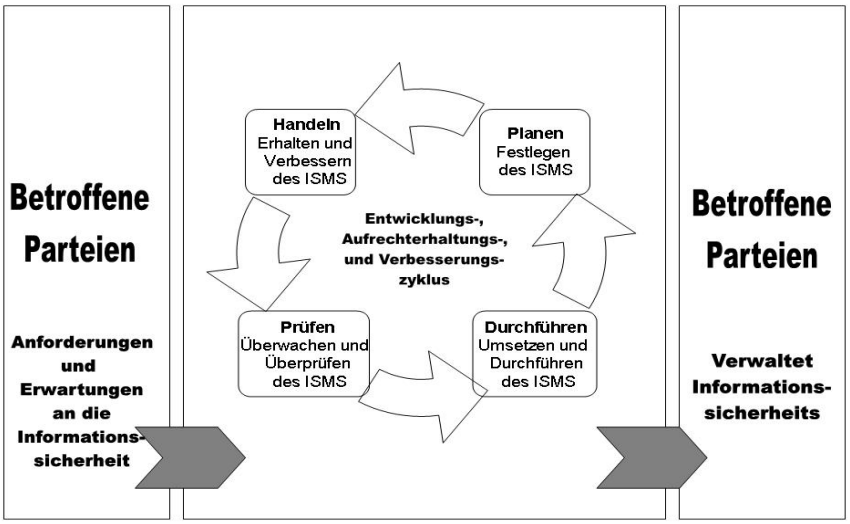
[87] Vgl. ISO 15408-2:2005
[88] Vgl. ISO 15408-3:2005
[89] Vgl. ISO/IEC 17799:2000, S. 1
[90] Vgl. BS7799-2:2002, S. 1 - 4

Ergebnis des Vergleichs

Im Gegensatz zu den zuvor beschriebenen Standards, Richtlinien und Normen, welche Kriterien zur Bewertung und Maßnahmen der Informationssicherheit enthalten, beinhaltet der BS7799-2:2002 Standard einen ganzheitlichen Ansatz eines Informationssicherheits-Managementsystems, welcher alle Bereiche einer Organisation berücksichtigt. Dieser bezieht die bewährten Verfahren der Informationssicherheit aus dem ISO/IEC 17799:2000 Standard mit ein.

3.3.2 BS7799-2:2002 Informationssicherheits-Management

Im Jahr 1992 hat das britische Department of Trade and Industry (DTI) eine Kommission ins Leben gerufen, welche die akzeptierten besten Verfahren (best practices) im Bereich der Informationssicherheit evaluieren sollte. Die Ergebnisse wurden 1993 als „Code of Practice“ veröffentlicht. Dieser wurde 1995 vom British Standard Institute adaptiert und als BS7799:1995 veröffentlicht.



In Anlehnung an BS7799-2:2002, S. 2

Abb. 3.3: PDCA-Konzept angewendet auf den BS7799-2:2002 Standard

Diese Version des Standards fand jedoch keine weite Verbreitung. Primär war dies auf seine geringe Flexibilität zurückzuführen. 1998 wurde der Standard grundlegend über-

arbeitet und erneut veröffentlicht. Erst 1999 wurde er in zwei Teile aufgeteilt. Nun existierte eine Spezifikation, gegen die eine Prüfung stattfinden konnte. Im Jahr 2000 adaptierte die International Organization for Standardization (ISO) den 1.Teil zur ISO17799:2000. Zwei Jahre später gab es erneut signifikante Veränderungen am 2. Teil. Unter anderem die Einführung des PDCA-Konzepts. Aus diesen Änderungen resultierte der BS7799-2:2002 Standard. Abbildung 3.4 zeigt hierzu die Entwicklung des BS7799 Standards.
Diesen Standard verbindet mit der DIN EN ISO 9001:2000 der prozessorientierten Ansatz und den zugrunde liegenden Plan-Do-Check-Act (PDCA) Ansatz (siehe Abbildung 3.3), welcher neben der Planung und Durchführung auch die Kontrolle und Verbesserung in einem kontinuierlichen Prozess zusammenfasst. Damit zeigen sich viele Gemeinsamkeiten zwischen dem Standard DIN EN ISO 9001 und dem BS7799-2:2002 mit dem er auch explizit harmonisiert wurde.

BS7799-2:2002 (Information security management systems – Specification with guidance for use)

Der BS7799-2:2002 stellt die Spezifikation für ein Informationssicherheits-Managementsystem (engl.: Information Security Management System) dar. Dieses Management System fügt sich in eine Reihe anderer internationaler Management Systeme (wie dem DIN EN ISO9001:2000) ein.

Ziel

Der BS7799-2:2002 wurde mit dem Ziel veröffentlicht, Führungskräften und Mitarbeitern einer Organisation ein Modell zur Verfügung zu stellen, das die Einführung und den Betrieb eines effektiven ISMS erlaubt. Die Einführung eines ISMS stellt eine wesentliche strategische Entscheidung dar, die durch die Organisationsstrategie und die Geschäftsziele der Organisation beeinflusst wird. Der BS7799-2:2002 wird zur Prüfung der Organisationsstruktur verwendet.
Dies beinhaltet ebenfalls die Anwendung durch akkreditierte Zertifizierungsorganisationen. Der BS7799-1 (Code of Practice) wurde bereits in einen internationalen Standard (ISO 17799:2000) übernommen. Im Rahmen der Überarbeitung des ISO 17799 wurde ebenfalls eine Überarbeitung des BS7799-2:2002 vorgenommen.

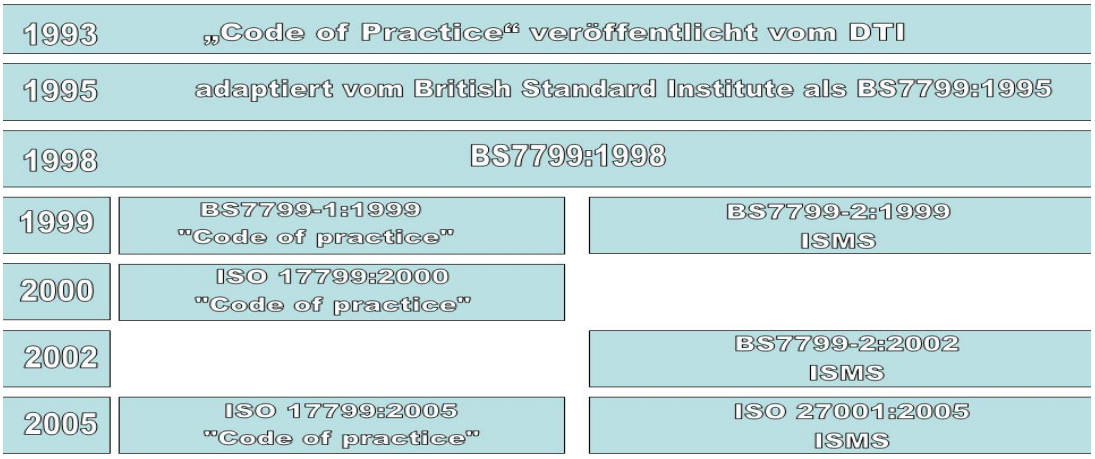


Abb. 3.4 Entwicklung der BS7799 Standards

Ende 2005 ist die ISO 27001:2005, entwickelt aus dem britischen BS7799-2:2002 Standard, in Kraft getreten. Dieser Standard lehnt sich weitestgehend an den BS7799-2:2002 Standard an. Ihm wird ebenfalls die ISO 17799:2000 als „Code of practice for information security management“ welche im Folgenden näher erläutert wird, zugeordnet.
Durch den zu Beginn der Bearbeitung des Themas noch unbekannten Termin der Einführung des ISO27001 Standards bezieht sich die Arbeit weiterhin auf den BS7799-2:2002 Standard. Dem Leser sollte dabei aber die weitestgehende Übereinstimmung beider Standards bewusst sein. Lediglich der Unterschied, dass es sich bei dem BS7799-2:2002 Standard um einen nationalen Standard handelt und bei der ISO27001:2005 um einen internationalen unterscheidet diese.

3.3.3 ISO/IEC 17799:2000 Verfahren für das Informationssicherheits-Management

Das BSI veröffentlichte im Jahr 1999 eine komplett überarbeitete Version des BS7799 Standards und weckte somit erneut das Interesse der ISO (International Organization for Standardization). Die ISO nahm den ersten Teil (der erste Teil umfasst die Kriterien als Basis des Standards) an und veröffentlichte diesen im Jahr 2000 unter dem Namen ISO 17799:2000.

ISO/IEC17799:2000 (Information technology -- Code of practice for information security management)

Die vollständige Bezeichnung lautet: ISO/IEC 17799:2000 (Information technology -- Code of practice for information security management); entspricht inhaltlich dem British Standard Nr. 7799, Teil 1 (BS 7799-1:1999)

Ziel

Die ISO/IEC 17799:2000 stellt eine umfassende Auswahl an Kontrollmechanismen, die auf Methodiken und Verfahren basieren, die sich in der Informationssicherheit bewährt haben. Grundlage für die Standardisierung war hierbei eine Sammlung von Erfahrungen, Verfahren und Methoden aus der Praxis um einen „best practice“ -Ansatz. Eine Zertifizierung nach ISO/IEC 17799 ist grundsätzlich nicht möglich. Soll ein Informationssicherheits-Managementsystem zertifiziert werden, ist dies ausschließlich nach BS7799-2:2002 bzw. dem ISO27001:2005 Standard möglich. [91]

Inhalte

ISO/IEC 17799:2000 befasst sich mit den folgenden Überwachungsbereichen[92]:

- Richtlinien
  Definieren die angestrebte Qualität der Sicherheit in Organisationen.
  Aufgaben
- Definiert Rollen und Zuständigkeiten in Organisationen
- Klassifizierung/Kontrolle organisationskritischer Daten
  Liefert eine Liste organisationskritischer Daten und der Maßnahmen zu ihrem Schutz
- Mitarbeitersicherheit
  Definiert Erwartungen an Mitarbeiter bezüglich Sicherheit und Vertraulichkeit sowie die Rollen der Mitarbeiter

[91] Vgl. ISO/IEC 17799:2000, S. 1
[92] Vgl. ISO/IEC 17799:2000, S. 1 - 65

- Physikalische Sicherheit
  Gerätesicherheit, Zugangsschutz und Kontrollmechanismen
- Kommunikations- und Operationsmanagement
  Befasst sich mit dem Schutz und der Integrität von Informationen und Organisationsdaten und der Verhinderung von Verlust und Missbrauch
- Zugriffskontrolle
  Kontroll- und Überwachungsmaßnahmen für den Zugriff auf Netzwerke und Anwendungen sowie der Schutz vor Eindringlingen
- Systementwicklung- und Wartung
  Befasst sich mit der Sicherstellung der Integration von Sicherheitsmechanismen in Informationssystemen.
- Kontinuitätsmanagement
  Befasst sich mit Maßnahmen bei schwerwiegenden Ausfällen und der Wiederherstellung nach Notfällen.
- Richtlinieneinhaltung
  Befasst sich mit der Prüfung von Sicherheitsrichtlinien und deren Umsetzung sowie mit der Definition von Audit Prozessen.

Rollen sind Aufgaben, die alternativ mehrere Personen ausfüllen können.[93] Ein Audit stellt einen systematischen, unabhängigen und dokumentierten Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln inwieweit Auditkriterien erfüllt sind, dar[94]. Auditkriterien bestehen aus einem Satz von Politiken, Verfahren oder Anforderungen, der als Referenz herangezogen werden kann[95]. Verfahren sind dabei als „Festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen“[96] definiert. Auditnachweise sind Aufzeichnungen, Tatsachenfeststellung oder andere Informationen, die für die Auditkriterien zutreffen und verifizierbar sind[97].

[93] Vgl. Mertens (2004), S. 19
[94] Vgl. DIN EN ISO 9000:2000, S. 31
[95] Vgl. DIN EN ISO 9000:2000, S. 32
[96] DIN EN ISO 9000:2000, S. 25
[97] Vgl. DIN EN ISO 9000:2000, S. 32

3.4 Ergebnis der Betrachtung

Aus der Betrachtung der Entstehung von Managementsystemen lassen sich grundlegende Gestaltungsregeln ausmachen, welche wiederum Anwendung in den vorgestellten Managementsystemen finden.
Dabei sind es Forderung wie die Informationssicherheit und die Erkenntnis, dass Informationen bedeutende Organisationswerte sind, die zu schützen sind und deren Schutz sich nicht durch ad hoc-Maßnahmen wirkungsvoll realisieren lässt, die somit den Bedarf an geregelten Managementsystemen erzeugen. Managementsysteme gewährleisten dabei die Erfüllung der Forderungen, ermöglichen die klare Zurechenbarkeit der Zuständigkeiten und die Dokumentierung gegenüber Dritten. Die Nicht-Erfüllung dieser Forderungen kann hierbei bis zur Bedrohung der Existenz einer Organisation führen.
Durch die Standardisierung von Managementsystemen wurde hierbei eine höhere Transparenz bei der Beurteilung und einheitliche Vorgehensweise bei der Implementierung erreicht.
Bei der flächendeckenden Einführung von Qualitätsmanagementsystemen stellt insbesondere der DIN EN ISO9001:2000 Standard einen etablierten Standard dar. Er ist die Grundlage vieler ihm folgender Standards. Dabei wurde der betrachtete BS7799-2:2002 Standard für Informationssicherheits-Managementsysteme ebenfalls mit diesem explizit harmonisiert. Somit weisen diese beiden Standards viele Gemeinsamkeiten auf.

Aufgabe

Um die Umsetzung des BS7799-2:2002 Standards unterstützen zu können, stellt sich die Aufgabe der Abbildung von Prozessen eines Informationssicherheits-Managementsystems. Dabei gestattet eine möglichst generelle Abbildung, welche möglichst unabhängig von Organisationspezifika ist, einen Einsatz als Muster für ein ISMS. Durch die Vielzahl der zu modellierenden Prozesse einer Organisation bedarf es dazu eines geeignet Prozessmodellierungstools, wie es das durch die Firma IDS Scheer AG bereitgestellte ARIS-Toolset darstellt, welches im Weiteren vorgestellt wird. Somit ermöglicht die Modellierung einerseits die bestehenden Prozesse einer Organisation mit den geforderten Prozessen des ISMS vergleichen zu können. Andererseits kann ein Re-

ferenzmodell den Prozessen eines ISMS als Schablone dienen und mit den Ergebnissen des Vergleichs eine Anpassung, Umsetzung, Dokumentation und kontinuierliche Verbesserung der Prozesse des ISMS ermöglichen. Dabei kann in dieser Arbeit auf das bestehende Referenzmodell des DIN EN ISO9001:2000 Standard, welches ebenfalls durch die Firma IDS Scheer AG zur Verfügung gestellt wurde, aufgebaut werden, um die Umsetzung der Abbildung von Prozessen eines ISMS in Anlehnung an dieses durchzuführen. Durch die Betrachtung u. a. der Bedrohungen und Schwachstellen zeigt sich die Risikoeinschätzung und –behandlung als grundlegender Bereich eines ISMS, welcher durch eine detaillierte Abbildung der Prozesse unterstützt werden soll.

Die somit modellierten Prozessmodelle gestatten es gleichermaßen die Gestaltung von ISMS-Prozessen in Organisationen durchzuführen sowie die Unterstützung der Gestaltung von Software, besonders in dem detailliert zu betrachtenden Bereich der Risikoeinschätzung und -behandlung zu ermöglichen, welche zur Umsetzung des ISMS beitragen kann.

4 Referenzmodellrahmen, -struktur und Komplettierung

In diesem Kapitel werden die Phasen zwei bis vier des Vorgehensmodells zur Referenzmodellierung abgedeckt. Dabei wird vor der eigentlich Modellierung das verwendete ARIS-Toolset und die zugrunde liegende Architektur vorgestellt. Darauf folgen die als Ergebnis der in der zweiten Phase erarbeiteten Konventionen der Modellierung.
Im dritten Abschnitt werden die Phasen drei und vier des Vorgehensmodells betrachtet. Beginnend mit einer detaillierten inhaltlichen Betrachtung des BS7799-2:2002 Standards werden im Weiteren Gemeinsamkeiten mit dem Referenzmodell des Qualitätsmanagements, welche in der Modellierung Anwendung finden konnten, herausgestellt. Auf diese Betrachtung folgt der abschließende Bereich dieses Kapitels, in dem das erstellte Referenzmodell des BS7799-2:2002 erläutert wird. Somit ist am Ende dieses Kapitels die vierte Phase des Vorgehensmodells abgeschlossen.

Toolgestützte Modellierung

Eine Hemmschwelle für den ungeübten Nutzer bezüglicher der Verwendung eines Prozessmodellierungstools ist die zunächst kaum überschaubare Vielfalt von Begriffen, Regeln, Objekten und Methoden. Deshalb ist der Aufwand der Modellerstellung für den Ungeübten meist sehr hoch und es empfiehlt mitunter für die Abbildung kleiner Geschäftsprozesse ein einfaches Grafikprogramm.
Im Gegensatz zur einfachen bildhaften Darstellung eines Geschäftsprozesses werden in einem Geschäftsprozessmodellen Objekte und Symbole mit einer besonders definierten Semantik und Syntax verwendet. Ein Geschäftsprozessmodell zeichnet sich somit durch eine gewisse Standardisierung aus. Dadurch lassen sich Fehlinterpretationen beträchtlich vermeiden. Eindeutig definierte Modell- und Objekttypen sowie die Festlegung möglicher Beziehungstypen legen weiterhin die Grundlage für eine sichere Vorgehensweise. Unterstützt wird dies durch eine, in wesentlichen Teilen, automatisierte Prüfung und Überwachung der Einhaltung.
In der Begründung der Geschäftsprozessmodellierung wurde bereits erwähnt, dass Optimierung und Automatisierung die entscheidende Rolle spielen. Dabei werden hohe

Anforderungen an die Konsistenz und Redundanzfreiheit gestellt, welche durch ein Modellierungstool wie dem ARIS-Toolset unterstützt werden.[98]

4.1 Architektur integrierter Informationssysteme (ARIS)

Das ARIS-Toolset wird für die Umsetzung der Modellierungsaufgabe eingesetzt. Um dieses Werkzeug zur Modellierung kennen zu lernen, wird in diesem Abschnitt ein kurzer Einblick in die ARIS-Architektur und der für die Modellierungsaufgabe benötigten Mittel gegeben.

Hintergrund der ARIS-Toolset-Entwicklung

Erste Idee und Schritte hin zum ARIS Toolset entstanden bereits zwischen 1990 und 1991 an dem von Prof. Scheer geleiteten Institut für Wirtschaftsinformatik an der Universität des Saarlands. Auf Grundlage dieser Forschungsergebnisse begann die IDS Scheer GmbH 1992 mit der Entwicklung eines Produktes zur Modellierung und Analyse von Geschäftsprozessen für den kommerziellen Einsatz. Dieses wurde bereits 1993 auf der CeBIT als ARIS Toolset Version 1.0 vorgestellt. Zu diesem Zeitpunkt gab es kein Produkt in diesem Marktsegment, welches gleichwertig eingesetzt werden konnte.
Wesentliche Grundlage des Erfolgs in den ersten Jahren war das Thema Business Process Reengineering (BPR). Dies veranlasste viele Organisationen Mitte der 1990er ihre Geschäftsprozesse zu analysieren und neu zu gestalten.
Der Grund für Bereitschaft der Organisationen in derartige Projekte zu investieren, ist die Erkenntnis, dass effiziente Geschäftsprozesse für den wirtschaftlichen Erfolg von großer Bedeutung sind. Ein weiterer Grund war dass die SAP AG das ARIS-Toolset zur Referenzmodellierung seines R/3 Systems nutzte. Somit wurde daraus die prozessorientierte Einführung von betriebswirtschaftlicher Standardsoftware begründet.

4.1.1 Das ARIS Konzept

Die Methode ARIS heißt Architektur Integrierter Informationssysteme. Sie beschreibt ein Rahmenwerk bzw. Konzept zur Beschreibung von Organisationen und Anwendungssystemen.

[98] Vgl.: Grief (2005), S. 2 - 3

Einsatzgebiete des ARIS Konzepts

Mit Hilfe der in ARIS angeboten Modelltypen lassen sich die betriebswirtschaftlichen Strukturen einer Organisation, einer Anwendungssoftware oder Vorgehensweisen abbilden. Somit wird ermöglicht, umfassend die Aufbau- und Ablaufstruktur einer Organisation abzubilden und zu dokumentieren. Darüber hinaus lassen sich aber auch allgemeingültige Referenzmodelle darstellen, welche in ihrer Anwendung die Abbildung von speziellen Aufbau- und Ablaufstrukturen in einer Organisation abbilden und dokumentieren. Sie dienen somit als Schablone welche mit Werten zu füllen ist um sie nutzen zu können.

Objekte in der Organisation

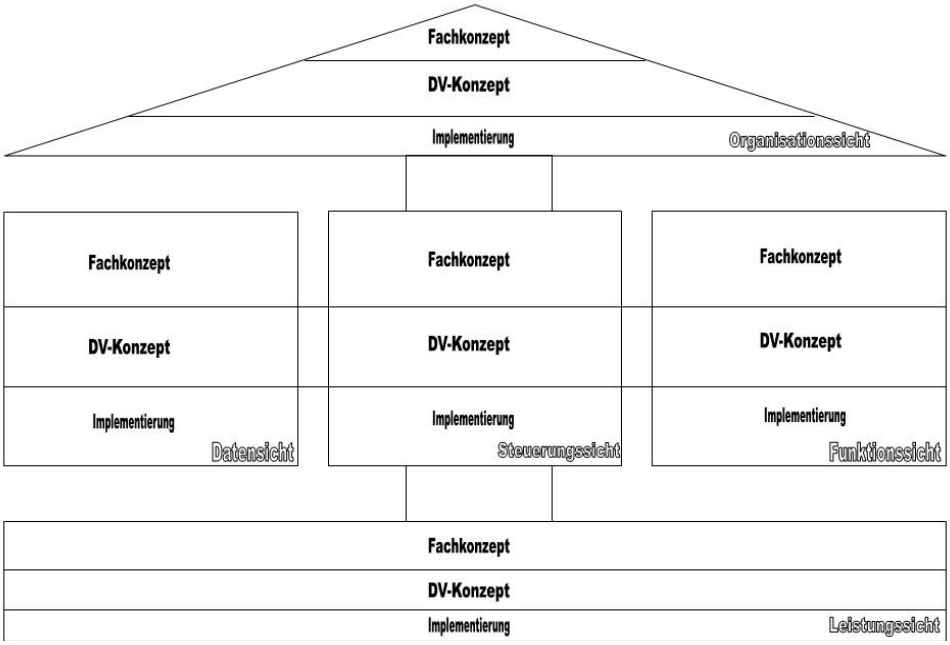
In der ARIS-Architektur werden folgende Objekte in Organisationen identifiziert.

- Funktionen
- Daten
- Organisationseinheiten
- Ereignisse
- Ressourcen
- Leistungen

Diese Objekte stehen untereinander in Abhängigkeit. Daher ist ein Architektur notwendig die diese Beziehungen abbilden kann und durch verschiedene, den Objekten angepasste Modelltypen darstellt.

Beschreibungssichten

ARIS stützt sich größtenteils auf seine eigene Fünf-Sichten-Architektur (ARIS-Haus siehe Abbildung 4.1). Diese fünf Sichten sind die Organisations-, Daten-, Steuerungs-, Leistungs- und Funktionssicht auf einen Geschäftsprozess. Die Einteilung in Sichten erfolgt unter anderem um die Komplexität des Modells in fünf Facetten aufzubrechen und so die Geschäftsprozessmodellierung einfacher zu gestalten.



In Anlehnung an Scheer (2002) S. 41

Abb. 4.1: Das ARIS – Haus

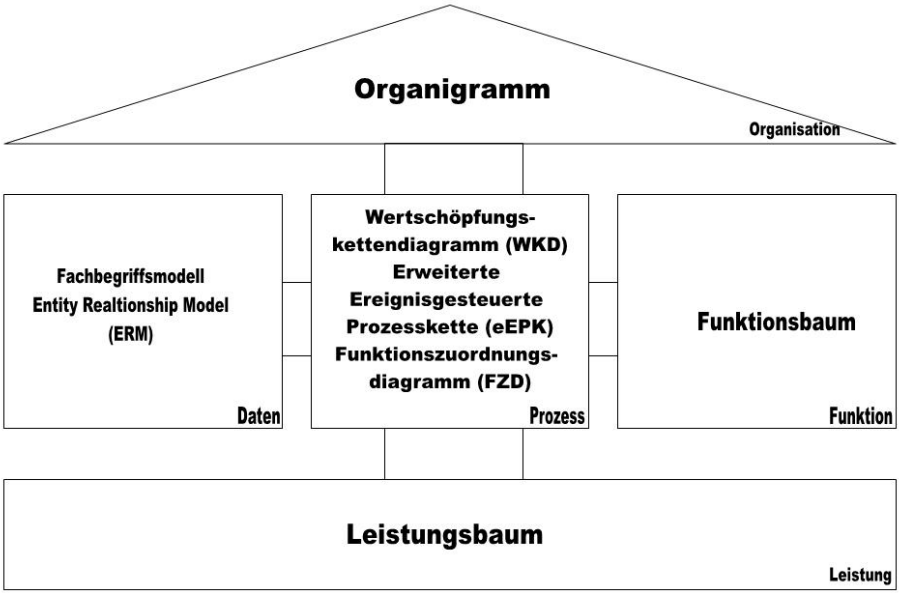
Jede Sicht des ARIS-Konzeptes gibt das Modell eines Geschäftsprozesses unter einem bestimmten Aspekt gemäß Scheer wieder[99]:

- Funktionssicht: beschreibt die auszuführenden Funktionen (Vorgänge) einer Organisation sowie ihre hierarchischen Zusammenhänge
- Organisationssicht: beinhaltet alle Ressourcen (Menschliche Arbeitskräfte, Maschinen, Hardware), d. h. alle Organisationseinheiten und deren Strukturierung
- Datensicht: beinhaltet alle Ereignisse (die Daten generieren) und Umfelddaten sowie Schriftverkehr, Dokumente etc.
- Leistungssicht: Alle Dienst-, Sach- und finanziellen Leistungen
- Steuerungssicht: Integration der vorangegangenen Sichten in einen logischen und zeitlichen Ablaufplan[100]

Alle genannten Sichten bilden das so genannte ARIS Haus (Abbildung 4.1). Dabei bilden die statischen Sichten Organisations-, Daten-, Funktions-, und Leistungssicht die

[99] Vgl. Scheer (2002), S. 32 - 37
[100] Vgl. Scheer (1998), S. 36

äußeren Bestandteile. Die dynamische Prozesssicht (Steuerungssicht) bildet den inneren Teil des ARIS Hauses und verknüpft die statischen Elemente miteinander.
Um durch die Sichtenbildung und Zerlegung des Ausgangsproblems den Zusammenhang der Elemente nicht aus den Augen zu verlieren werden die verschieden Sichten in der Prozesssicht wieder zusammengeführt.
Durch die Aufnahme der Beziehungen in jeweils eigenen Sichten werden diese redundanzfrei und systematisch erfasst. Die Prozesssicht ist somit die wesentlichste Sicht im ARIS-Konzept.



In Anlehnung an Scheer (2002) S. 47

Abb. 4.2: Das ARIS - Haus Modelltypen

Beschreibungsebene

Jede Facette (Sicht) des ARIS-Hauses (Abbildung 4.2) ist in drei Ebenen eingeteilt: Fachkonzept, DV-Konzept (= IV-Konzept) und Implementierungsebene gemäß Scheer[101]:

- Fachkonzept: Strukturierte Darstellung eines Geschäftsprozesses mittels DV-fremden Beschreibungsmodellen (je nach Sicht z.B.: EPK, Organigramm, Funktionsbaum)

Es spezifiziert die fachlichen Anforderungen eines Projektes durch betriebswirtschaftlichen Beschreibung der Problemstellung in Form von Geschäftsprozessmodellen. Somit sind in Fachkonzepten alle relevanten Geschäftsvorfälle mit ihren Randbedingungen detailliert beschrieben. Diese finden Verwendung durch Projektmanager, Fachabteilung und Anwender.

- DV-Konzept: Umsetzung des Fachkonzeptes in DV-nahe Bechreibungsmodelle (je nach Sicht z.B.: Relationen, Struktogramme, Topologien)

  Fachkonzepte werden von Softwareentwicklern nicht im ausreichenden Maße verstanden. Grund ist die Erstellung eines Fachkonzeptes in der Sprache des jeweiligen Anwendungsgebietes. Selbst Fachbegriffsmodelle sind mitunter ohne grundlegendes Wissen über jeweilige Domäne nur schwer zu verstehen. Daher sind fachliche Funktionen in einem DV-Konzept soweit in DV-Funktionen zu transformieren, dass sie auch ohne fachliches Spezialwissen verstanden und umgesetzt werden können.

  Ohne DV-Konzept muss die Implementation direkt auf Basis des Fachkonzeptes erfolgen. Dies führt dazu, dass sich Experten der Domäne mit technischen Problemen auseinandersetzen müssen. Die Modelle des DV-Konzeptes finden durch Projektmanager, Softwarearchitekten, Qualitätssicherung, Vertrieb und Softwareentwickler Verwendung.
- Implementierungsebene: DV-technische Realisierung der beschriebenen Geschäftsprozessteile (je nach Sicht z.B. mittels Erstellung von Programmcode, Datenbanksystemen, Einsatz von Protokollen)

Das ARIS-Konzept wurde die Grundlage verschiedener Software-Produkte, speziell für das bekannte ARIS-Toolset. Derzeit stehen im ARIS-Konzept über 100 Modelltypen zur Beschreibung der Abläufe zur Verfügung. Dabei müssen diese in Abhängigkeit des Projektziels sorgfältig gewählt werden.

[101] Vgl. Scheer (2002), S.32 - 37

4.1.2 ARIS-Toolset

Das ARIS Toolset steht für eine Gruppe von Systemen welche Möglichkeiten zur Dokumentation, Analyse und Neugestaltung von Geschäftsprozessen bieten. Modelle dokumentieren diese Geschäftsprozesse. Methodische Basis dieser Modelle bildet die im vorangehenden Abschnitt vorgestellte Architektur integrierter Informationssysteme,
welche ein von Prof. Scheer entwickeltes konzeptuelles Rahmenwerk darstellt. Dieses Rahmenwerk zeigt unterschiedliche Sichten und Ebenen durch die Organisationen bzw. Geschäftsanwendungen beschrieben werden können. Beschreibungen können somit nach rein funktionellen Gesichtspunkten erfolgen.
Grundlage der Modellierung sind entsprechende Beschreibungstechniken wie beispielsweise das Entity-Realtionship-Modell zur Abbildung logischer Datenstrukturen, die erweiterten ereignisgesteuerte Prozesskette zur Darstellung von Geschäftsprozessen oder das Organigramm zur Dokumentation von Organisationsstrukturen. Im ARIS Meta Modell werden diese Techniken abgebildet. Es umfasst alle Informationsobjekte, welche zur Abbildung der betriebswirtschaftlichen Gegebenheiten notwendig sind sowie deren Beziehung untereinander.

Zurzeit umfasst die ARIS-Familie insgesamt 21 Produkte. Im Zusammenhang dieser Arbeit wird das ARIS-Toolset vorgestellt.
Das ARIS-Toolset stellt die benötigten Funktionalitäten zur Geschäftsprozessmodellierung bereit und darüber hinaus:

- Definition von Reports, Semantikchecks, Methodenfiltern
- Erzeugen und Vergleichen von Modellen
- Konsolidieren von Objekten
- Datenbank-Merge
- Administration der ARIS-Site
    - Bei großer Nutzeranzahl werden mehrere ARIS Business Server zu einer Site zusammengefasst

- Zentraler Dienst zur Verwaltung dieser Site, Filter und Vorlagen werden zur Verfügung gestellt

Die mit dem ARIS-Toolset definierten Methodenfilter, Semantikchecks und Reports können auch von anderen ARIS-Komponenten genutzt werden.

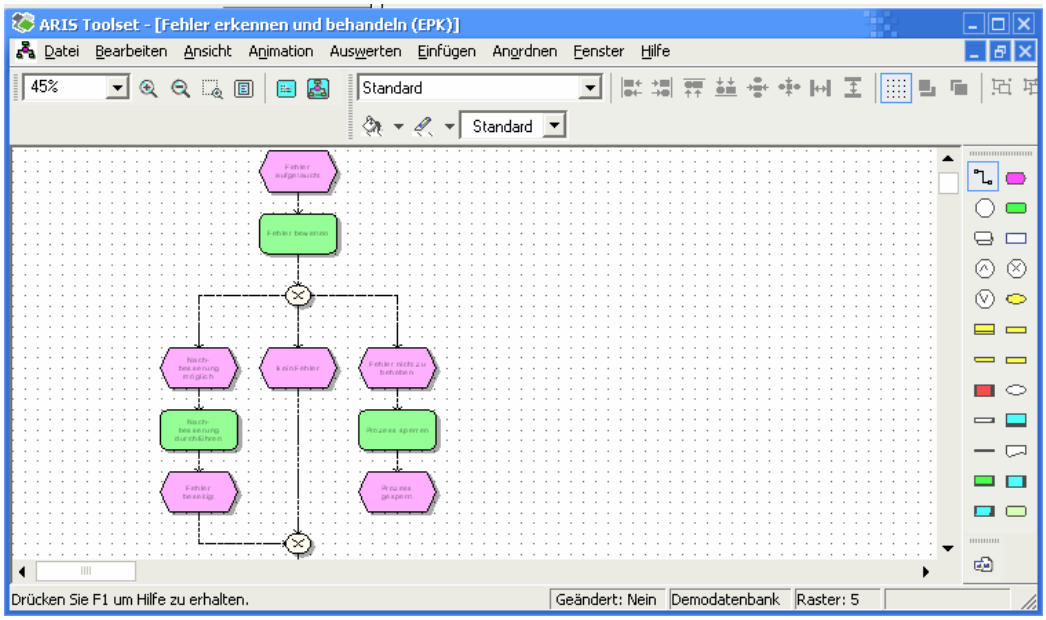


Abb. 4.3: ARIS Modellierung einer eEPK

Das ARIS-Toolset umfasst die folgenden Komponenten:

- Modelleditor (siehe Abbildung 4.4),
- Datenbankverwaltung,
- Benutzerverwaltung,
- Modellverwaltung,
- Objektverwaltung
- Layout- und Modellgenerierung.

Reports

Um die Vielzahl von Informationen, welche bei der Modellierung von Geschäftsprozessen anfallen, auswerten, strukturieren und in leicht verständlicher Form zur Entscheidungsunterstützung darstellen zu können, existiert diese Komponente.

Dabei lässt das Reporting eine große Flexibilität zu, die je nach Reportdefinition verschiedene Reportausgaben ermöglicht.

Konfiguration

Durch die Vielzahl von unterschiedlichen Beschreibungstechniken, die aus der Vielzahl von Problemstellungen resultiert, ist eine angepasst Auswahl und Konfiguration notwendig. Dem Nutzer ist es möglich diese individuell zu konfigurieren. Die Konfiguration lässt eine Anpassung von Objekttypen, Beziehungstypen bis hin zu Attributtypen zu.

Nutzen von ARIS

Der von ARIS gebotene Nutzen lässt sich in den folgenden acht Punkten zusammenfassen.

- Aris stellt sich als defacto Standard für die Geschäftsprozessmodellierung dar.[102]
- Geschäftsprozesse lassen sich aus unterschiedlichen Perspektiven betrachten. (fünf Sichten: Organisations-, Funktions-, Daten-, Prozess- und Leistungssicht)
- In vier der Sichten (ohne Prozesssicht) kann unabhängig von einander ein vollständiges DV Konzept modelliert werden (statisch).
- Die Prozesssicht verbindet die vier statischen Sichten, integriert diese. Daraus folgt die Reduzierung der Komplexität durch Modellierung in Sichten.
- Die unabhängigen Sichten in der gemeinsamen Datenbasis ermöglichen den Zugriff und die konsistente Verknüpfung in der Prozesssicht.
- Die Sichtenintegration führt zu einer redundanzfreien und ganzheitlicher Modellierung.
- Die Semantikchecks ermöglichen eine Konsistenzprüfung der Modelle.
- Der Überblick über Modelle wird durch Vielzahl an Navigationsmöglichkeiten erleichtert.
- ARIS-Modelle sind leicht verständlich.[103]

[102] Vgl. Grief (2005), S. 3
[103] Vgl. Grief (2005), S. 3

4.2 Referenzmodellrahmen

Nachdem im vorangehenden Abschnitt das ARIS-Konzept und das ARIS-Toolset vorgestellt wurden, werden in diesem die Konvention der Modellierung des BS7799-2:2002 Standards als Ergebnis des Referenzmodellrahmens vorgestellt.

4.2.1 Konventionen der Modellierung

Um die Konventionen der Modellierung umzusetzen, stellt das ARIS-Toolset den Methodefilter zur Verfügung. Mit diesem lassen sich u. a. Modelltypen, deren Anwendung, Symboltypen und Attribute festzulegen.

Modelltypen, Symbole und deren Anwendung

Im Zuge der Vorüberlegung der Modellierung galt es das Referenzmodell mit möglichst wenigen der über 100 Modelltypen, die das ARIS-Toolset zur Verfügung stellt, eindeutig beschreiben zu können um eine konsistente Modellierung zu ermöglichen. Die Entscheidung fiel auf das Wertschöpfungskettendiagramm, das Funktionzuordnungsdiagramm, die erweiterte ereignisgesteuerte Prozesskette sowie das Entity Relationship Modell. Die Begründung der Auswahl und deren Anwendung werden im folgenden Absatz näher erläutert. Dabei wird auf die Auswahl der Modelltypen eingegangen und deren Anwendung beschrieben.

Überblicksmodell

Die Aufgabe dieses Modells liegt darin wesentliche Prozesse abzubilden und dabei insbesondere den Kontrollfluss leicht verständlich darzustellen. Dieser Modelltyp wird mit Hilfe des im Weiteren erläuterten Wertschöpfungsdiagramms abgebildet. Der Kontrollfluss stellt dabei den Ablauf der Bearbeitung dar.

Wertschöpfungskettendiagramm

In der Regel werden komplexe Geschäftsprozesse in Organisationen nicht im Detail dargestellt um die Übersichtlichkeit zu gewährleisten. Das Wertschöpfungskettendia-

gramm ermöglicht es einen Gesamtprozess auf hohem Abstraktionsniveau überblicksartig dazustellen. Dabei können sowohl zeitliche Beziehungen innerhalb des Gesamtprozesses als auch hierarchische Beziehungen von Teilprozessen innerhalb eines Gesamtprozesses dargestellt werden. Die eindeutige Beschränkung der sprachlichen Mittel stellt den Vorteil dieses Diagrammtypen dar. Der Modellierer wird gezwungen sich von Detailfragen zu lösen und sich auf wesentliche Abläufe zu konzentrieren. Wertschöpfungskettendiagramme ermöglichen es Kerngeschäftsprozesse innerhalb der Organisation zu identifizieren und deren grundsätzliche zeitliche Reihenfolge festzulegen. Ein Kerngeschäftsprozess stellt hierbei einen Prozess oder Vorgang dar welcher direkt an der Wertschöpfung der Organisation beteiligt ist.
Auf der nächsten Detailstufe lassen sich daraufhin die Zusammensetzung der Kerngeschäftsprozesse durch Ablaufbeschreibungen wie Ereignisgesteuerte Prozessketten oder detaillierter Darstellungen der Teilprozesse zeigen. Neben den zeitlichen und Prozesshierarchien ermöglicht dieser Diagrammtyp weiterhin die Darstellung von Organisationseinheiten und Datenbeschreibungen welche den Funktionen zugeordnet werden können. Durch den überblicksartigen Charakter eignet sich das WKD besonders als fachliches Überblicksmodell der Managementsicht auf die Geschäftsprozesse.

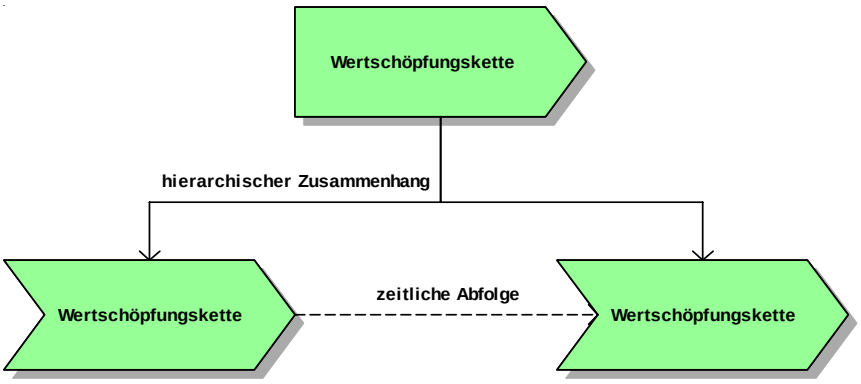


Abb. 4.4: Darstellung WKD

Die besonderen Eigenarten des WKD ermöglichen somit den Einsatz zur Darstellung der einzelnen Kapitel und Unterkapitel des BS7799-2 Standards unter Beachtung der zeitlichen und hierarchische Zusammenhänge. Das WKD beschränkt sich auf die Nutzung des Wertschöpfungskettensymbols und der Darstellung der Beziehungen durch Kanten in gestrichelter und durchgezogener Form (siehe Abbildung 4.4).

Organigramm

Im Organigramm wird die Aufbauorganisation einer Organisation dargestellt. Die Ablauforganisation hingegen wird erst durch Prozessmodelle dargestellt. Dabei lässt ein Organigramm verschiedene Stufen der Abstraktion um die Organisationseinheiten darzustellen. Diese reichen von der allgemeinen Darstellung der Organisationseinheiten bis hin zu einzelnen Personen.
Im Modelltyp Organigramm sind die Symbole für Organisationseinheit und Stelle zulässig. Kanten werden in durchzogener Form dargestellt (siehe Abbildung 4.5).[104]

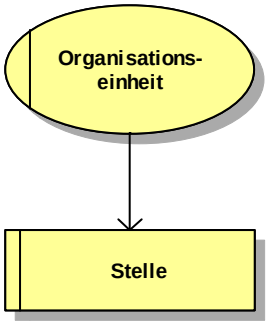


Abb. 4.5: Darstellung der Symboltypen für das Organigramm

Erweiterte Ereignisgesteuerte Prozesskette

Anknüpfend an die Wertschöpfungskettendiagramm und deren detaillierte Darstellung der Funktionen durch erweiterte Ereignisgesteuerte Prozessketten, lassen diese die Darstellung der Ablauforganisation zu. Im Einzelnen bedeutet dies die Darstellung von Ablauffolgen einzelner Funktionen im Rahmen einzelner Geschäftsprozesse. Dabei lassen sich zwei Varianten verfolgen. Einerseits lässt sich die reine zeitliche Abfolge von Prozessschritten modellieren. Es lassen aber auch Objekte aus den statischen Sichten wie Organisation-, Daten-, Funktions- und Leistungssicht integrieren und so Prozesse mit Zusatzinformationen als erweiterte ereignisgesteuerte Prozesskette modellieren. Im Vergleich zum WKD bietet die eEPK darüber hinaus wesentlich umfangreichere Modellierungsmöglichkeiten, durch die größere Anzahl der Objekt-, Symbol-, und Beziehungstypen. Damit eignet sie sich für die fachlich detaillierte Modellierung besser als

WKD. Durch diese Eigenschaften eignet sich die eEPK hervorragend zur Modellierung der Arbeitssicht mit Ablaufbeschreibungen. Der BS7799-2 Standard enthält jedoch keine detaillierten Ablaufbeschreibungen, sodass die eEPK ihren Einsatz in der Abbildung der aus dem Vergleich mit dem Referenzmodell des DIN EN ISO9001:2000 Standard hervorgegangen Ablaufbeschreibungen und der Risikoeinschätzung bzw. Risikobehandlung, welche ebenfalls detailliert betrachtet werden, findet.
Innerhalb der eEPK sind die Symbole für Ereignis, Funktion, Prozessschnittstelle sowie gestichelte Kanten zugelassen (siehe Abbildung 4.6).[105]

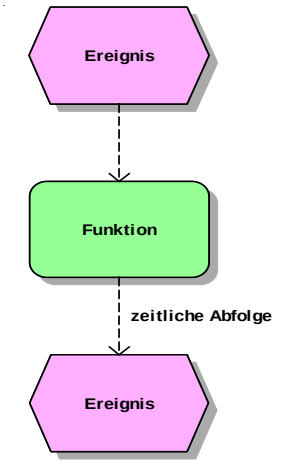


Abb. 4.6: Darstellung der Symboltypen für die eEPK

Funktionszuordungungsdiagramm

Dieser Diagrammtyp ermöglicht die Modellierung von Ein- und Ausgabebeziehungen und die Zuordnung von Organisationseinheiten im System zu einem Prozess. Die dabei beschriebenen Eingaben werden von dem Prozess benötigt bzw. es wird die Ausgabe des Prozesses beschrieben. Die Organisationseinheiten im System gewährleisten die Durchführung des Prozesses. Diese Möglichkeiten werden zur Modellierung des BS7799-2 Standards genutzt indem bei notwendigen detaillierten Datenbeschreibungen die Funktionen der eEPKs mit diesem Diagrammtyp hinterlegt werden. Darüber hinaus beschreibt der BS7799-2 Standard in den Kapiteln 6 und 7.1 Ein- und Ausgaben, welche sich mit dem WKD nicht darstellen lassen. Somit wird dieser Diagrammtyp zu Ab-

[104] Vgl. Scheer (1996), S. 28
[105] Vgl. Scheer (1996), S.49 - 54

bildung der genannten Kapitel ebenfalls eingesetzt. Grundsätzlich, mit diesen zwei Ausnahmen, werden WKD für die Managementsicht eingesetzt.
Innerhalb der FZD sind die Symbole für Funktionen, Dokumente, Fachbegriffe und Organisationseinheiten. Die Herstellung der Beziehungen erfolgt mittels durchgezogener Kanten (siehe Abbildung 4.7).

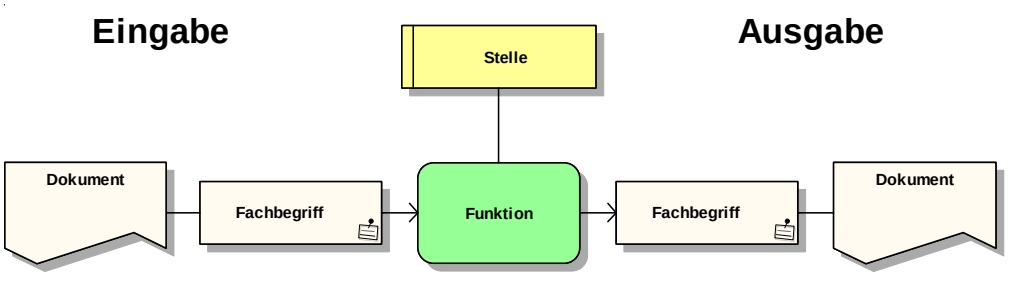


Abb. 4.7: Darstellung der Symboltypen für das FZD

Entity Relationship Modell

Das ERM ist eine häufig genutzte Modellierungstechnik für den Entwurf eines konzeptuellen Datenmodells. Das ER-Modell besteht meist aus einer Grafik und einer Beschreibung der darin verwendeten einzelnen Elemente. Es dient zum einen in der konzeptionellen Phase der Anwendungsentwicklung der Verständigung zwischen Anwendern und Entwicklern, wobei ausschließlich das „Was“, also die Sachlogik, und nicht das „Wie“, also die Technik, wesentlich ist. Zum anderen dient das ERM in der Implementierungsphase als Grundlage für das Design einer Datenbank.
Auf der Ebene des DV-Konzeptes ist eine detaillierte Beschreibung der Zusammenhänge notwendig. Dies geschieht in der Abbildung des BS7799-2 Standards in der Risikoeinschätzung und Risikobehandlung. Zur Darstellung dieser Zusammenhänge wird das Entity Relationship Modell genutzt.
Im letzten der angewendeten Diagrammtypen, dem ERM, sind Entitäten, Beziehungen und durchgezogene Kanten zulässig (siehe Abbildung 4.8).[106]

[106] Vgl. Scheer (1996), S. 31

Abb. 4.8: Darstellung der Symboltypen für das ERM

Der Einsatz der genannten Symboltypen in den entsprechenden Diagrammtypen wird im Weiteren unter dem Punkt Modellierungsmethodik erläutert.

Attribute

Die Attribute für Objekte werden auf Titel und freie Attribute reduziert da diese die Möglichkeit externer Verknüpfungen bieten. Für den Einsatz des Referenzmodells in einer Organisation lassen sich die, entsprechend des Organisationstyps, notwendigen Attribute festlegen.

Gruppenstruktur

Die Gruppenstruktur im ARIS-Eplorer gibt den Rahmen zur Ablage der Modelle vor und ermöglicht eine übersichtliche Darstellung und Zuordnung der erstellten Modelle.

Modellebenen

In dem zu modellierenden Referenzmodell werden drei Ebene, wie in Abbildung 4.9 zu erkennen, angewandt.

- **Übersichtsmodell**
  - **Ebenenübergreifende Modelle**
  - **Kapitel**
    - **Managementsicht**
    - **Arbeitssicht**

Abb. 4.9: Gruppenstruktur im ARIS Explorer

Beginnend bei der Ebene des Übersichtsmodells über die Ebene der Kapitel des BS7799-2:2002 bis hin zur detaillierten Beschreibung der jeweiligen Sicht des Referenzmodells. Auf der Kapitelebene fügt sich die Gruppe der Ebenenübergreifenden Modelle ein. Sie wird im Weiteren ausschließlich für die Modellierung der Organisationsstruktur genutzt.

Sichten innerhalb des Referenzmodells

In dem Referenzmodell des BS7799-2 wird zwischen zwei bereits genannten Sichten unterschieden, der Managementsicht und der Arbeitssicht. Diese finden sich in der Gruppenstruktur eingeordnet in die Gruppen der Kapitel des BS7799-2, als untergeordnete Gruppen, wieder.

Modell- und Objektbibliotheken

Im Referenzmodell des BS7799-2 finden weder Modell- noch Objektbibliotheken Anwendung. Die Festlegung von Konventionen ist deshalb für diese nicht notwendig

Temporär Modelle und Objekte

Modelle dieses Charakters werden in dem zu erstellenden Modell ebenfalls nicht beachtet und bedürfen deshalb keiner gesonderten Konventionen.

Verweise auf Modelle

Die Anwendung von Verweisen auf Modelle ist wiederum eine Möglichkeit die in großen IT-Projekten Anwendung findet. Im Rahmen dieser Arbeit ist dies durch die Bearbeitung einer einzelnen Person nicht notwendig. Deshalb werden für solche Verweise keinerlei Festlegungen getroffen.

Modelldarstellung

Durch die unterschiedlichen Symbol und Verknüpfungstypen lässt sich die Darstellung der verschiedenen Diagrammtypen nur schwer vereinheitlichen. Grundsätzlich gilt:

- Modelle werden links oben angelegt
- Sie halten sich im Verlauf am linke Rand der Modellierungsfläche

- Attribute werden unter den Symbolen mittig als Symbol angeordnet
- Hinterlegung befinden sich an der rechten Seite der Unterkante des Symbols
- Die Bezeichnung des Symbols befindet sich zentriert im Symbol und überragt dieses nicht
- Der Abstand zwischen den modellierten Objekten ist konstant

Für eEPKs gilt darüber hinaus:

- Der zentrale Pfad ist mittig anzuordnen
- Verzweigungen werden gleichmäßig zur linken und rechten Seite des zentralen Pfades angelegt

Modellierungsmethodik

Ebenenanzahl der Modellhierarchie

Wie bereits im Punkt der Gruppenstruktur erläutert besteht die Modellhierarchie aus drei Ebenen.

- Überblickmodellsebene
- Kapitelebene / Ebenenübergreifende Modelle
- Sichtenebene

Zu verwendende Modelltypen

Zur Modellierung des Übersichtsmodells wird das bereits genannte WKD genutzt. Dieser Modelltyp wird ebenfalls für die Darstellung auf der Ebene der Kapitel des BS7799-2:2002 eingesetzt. Darüber hinaus wird in den beiden bereits genannten Fällen, Kapitel 6. und 7.1 zur Gewährleistung der optimalen Darstellung des Sachverhalts das FZD eingesetzt. In der Gruppe der Ebenenübergreifenden Modelle wird ausschließlich das Organigramm genutzt. Auf der Ebene der Sichten wird zur Darstellung der Managementsicht das WKD festgelegt. In der Arbeitssicht sind sowohl eEPK, FZD und ERM aus den bereits genannten Gründen zulässig.

Datenmodellierung

Bei der Datenmodellierung gilt es, den Standard, welcher in Textform vorliegt, in relevante Modelle umzusetzen. Dabei findet das ERM zur Datenmodellierung auf der DV-Konzeptebene Anwendung. Die dabei angewendeten Begriffe werden durch die Begriffswelt des BS 7799-2:2002 Standards vorgegeben. Somit bedarf es keiner Darstellung der Zusammenhänge verschiedener Begriff, wie es ein Fachbegriffsmodell ermöglichen würde. Es lässt sich festhalten, dass die Bezeichnungen der notwendigen Daten dem Standard entnommen und mit Hilfe des ERM dargestellt werden.

Funktionsmodellierung

Funktionen erhalten in den Wertschöpfungsketten der Kapitelebene und in denen der Managementsicht die Bezeichnungen der den Funktionen entsprechenden Punkte im Standard. Sollten sich diese, durch eine ausführliche Beschreibung nicht in Benennung einer Funktion einfügen lassen so werden diese gekürzt. Dabei wird darauf geachtet, dass der Sinn erhalten bleibt. Zusätzlich zur Bezeichnung wird die Nummerierung aus dem Standard übernommen um einen leichten Vergleich mit dem Standard zu ermöglichen. Werden Funktionen durch den Modellierer selbst erstellt und sind nicht dem Standard entnommen so werden diese farblich durch einen dunkleren Grünton und in der Bezeichnung durch das Fehlen der Nummerierung kenntlich gemacht. Mit Funktionen innerhalb der FZD auf Kapitelebene und in der Managementsicht wird gleich verfahren. Eine Ausnahme bildet hierbei ausschließlich das Übersichtsmodell. Hier werden die Funktionen gleich dem Standard beschriftet, tragen aber keine Kapitelnummerierung. Die farbliche Kennzeichnung entspricht dabei jedoch den direkt dem Standard entnommenen Funktionen. Innerhalb der eEPK und der FZD der Arbeitssicht werden die Bezeichnungen der Objekte, auf die sich die Funktion bezieht, in die Namensgebung dieser einbezogen.

Ereignismodellierung

Um eine konsistente Modellierung zu ermöglichen werden einheitliche Ereignisnamen angewendet. Diese beginnen diese immer mit der Objektbezeichnung.

4.3 Referenzmodellstruktur und Komplettierung

In diesem Abschnitt wird die Modellierung des BS7799-2:2002 Standard an Hand des Vorgehens erklärt. Ziel dieses Abschnittes ist es die Modellierung und somit die Entstehung der Modelle zu erklären. Dabei ordnet sich dieser Abschnitt in die Phasen drei und vier des Vorgehensmodells zur Referenzmodellierung ein.
Dazu wird anfangs der Inhalt des BS7799-2:2002 Standards detailliert beschrieben. Darauf hin folgen die Ergebnisse der Betrachtung des zur Verfügung gestellten Referenzmodells zum Qualitätsmanagement im Vergleich mit dem BS7799-2:2002 Standard.
Nachdem dies abgeschlossen ist folgt die Darstellung des Referenzmodells zum Informationssicherheits-Managementsystem.
Weiterführend wird der Kern der Modellierung die Risikobehandlung und Risikoeinschätzung sein. Dieser wird in dem Referenzmodellmodell detailliert beschrieben. Auf Basis dieser Betrachtung wird in Kapitel 5 eine Implementierung vorgestellt. Diese wird mittels der Möglichkeiten des ARIS-Toolsets mit dem Referenzmodell verknüpft.
Grundsätzlich handelt es sich bei den in diesem und im folgenden Kapitel betrachteten Geschäftsprozessen des ISMS um Sicherheitsprozesse.

4.3.1 Inhalt des BS7799-2:2002 Standards

Vor der inhaltlichen Beschreibung des Standards sei darauf verwiesen, dass sich die Kapitelbezeichnungen im Abschnitt 4.3.1 der Diplomarbeit ausschließlich auf die Kapitel des BS7799-2:2002 beziehen.

Der Beschreibung des Inhalts geschieht dabei gemäß BS7799-2:2002 Standard.[107]

Eingeleitet wird der Standard mit der Erklärung des Anwendungsbereichs und der grundlegenden Begriffsdefinitionen. Der Anwendungsbereich bezieht sich dabei auf die Sicherstellung des Verhältnisses von Sicherheitsmaßnahmen und dem Schutz der Informationen in einer Organisation. Diese sollen somit Vertrauen beim Kunden und an-

deren betroffenen Parteien wecken. Dabei ist die Einhaltung gesetzlicher und behördlicher Vorschriften grundlegendes Ziel.

Im Kapitel 4 des Standards wird das Informationssicherheits-Managementsystem beschrieben. Dazu werden in Kapitel 4.1 „Allgemeine Anforderungen an ein ISMS“ aufgezeigt. Diese finden sich aufgeschlüsselt in den Unterkapiteln wieder.
Die Forderung besteht dabei in einem dokumentierten ISMS, welches auf alle organisationsbezogenen Geschäftsaktivitäten und -risiken entwickelt, umgesetzt, aufrechterhalten und kontinuierliche verbessert wird. Dabei basiert der anwendbare Prozess auf dem PDCA-Modell.

Auf die allgemeinen Anforderungen folgt in Kapitel 4.2 „Festlegen und Verwalten des ISMS“ dabei teilt sich dieses Kapitel in die vier Unterkapitel:

- 4.2.1 „Festlegung des ISMS“, welches Schritte zum Festlegen eines ISMS beschriebt. Beginnende bei den Anforderungen der betroffenen Parteien über die Definition systematischen Vorgehensweise und dem Identifizieren, Einschätzen und der möglichen Behandlung der Risiken.

- 4.2.2 „Umsetzung und Durchführung des ISMS“, enthält die Schritte der Formulierung und Umsetzung eines Risikobehandlungsplans, der Umsetzung ausgewählter Maßnahmen aus Kapitel 4.2.1, Schulung, Verwaltung von Vorgängen und Ressourcen sowie die Umsetzung von Verfahren und Maßnahmen zur sofortigen Reaktion auf Sicherheitsvorfälle. Dabei wird bei der Verwaltung von Ressourcen auf das Kapitel 5 verwiesen. Dieses befasst sich explizit mit deren Verwaltung.

- 4.2.3 „Überwachung und Überprüfung des ISMS“, welches die Ausführung von Überwachungsverfahren, regelmäßige Prüfung der Wirksamkeit des ISMS, Überprüfung des Restrisikos und akzeptablen Risikoniveaus, die Durchführung regelmäßiger Überprüfungen des ISMS durch das Management und Aufzeichnung von Zwischenfällen beinhaltet. Dabei wird bei der ISMS-Überprüfung

[107] Vgl. BS7799-2:2002

durch das Management auf das 6. Kapitel verwiesen, welches sich diesem Thema widmet.

- 4.2.4 „Aufrechterhaltung und Verbesserung des ISMS“, umfasst die Umsetzung der identifizierten Verbesserungen, Ergreifung geeigneter Korrekturmaßnahmen und Mitteilung der Ergebnisse sowie die Sicherstellung, dass die Ziele erreicht werden. Die Korrekturmaßnahmen lehnen sich dabei direkt an die in Kapitel 7 beschriebene ISMS-Verbesserung an.

In Kapitel 4.3 werden die Dokumentationsanforderungen an das ISMS herausgestellt. Kernpunkte sind dabei:

- die dokumentierte Erklärung zur Sicherheitspolitik
- die Dokumentation des Anwendungsbereichs sowie der Verfahren und Maßnahmen zur Unterstützung des ISMS
- der Risikoeinschätzungsbericht
- der Risikobehandlungsplan
- die dokumentierten Verfahren zur Sicherstellung der wirksamen Planung, Durchführung und Kontrolle der Informationssicherheitsprozesse. Dieser Punkt bezieht sich direkt auf die ISMS-Audits.
- die Erklärung zur Anwendbarkeit

Dabei stellen die Audits einen systematischen, unabhängigen und dokumentierten Prozess zur objektiven Auswertung, ob bestimmte Merkmale vorhanden und bestimmte Forderungen erfüllt sind, dar. Kapitel 4.3 zeigt somit eine umfassende Dokumentation des ISMS. Die Erklärung zur Anwendbarkeit ist „ein Dokument, dass die Sicherheitsziele und –maßnahmen festlegt, die für das ISMS einer Organisation relevant und anwendbar sind. Die Basis hierfür liefern die Ergebnisse und Schlussfolgerungen aus den Prozessen zur Risikoeinschätzung und Risikobehandlung.“[108]

[108] BS7799-2:2002, S. 5

Darüber hinaus werden im 5. Kapitel die Verantwortung des Managements, im 6. Kapitel die Managementbewertung des ISMS und im 7. Kapitel die ISMS Verbesserung beschrieben.

Die in Kapitel 5 erläuterte Verantwortung des Managements bezieht sich dabei auf die Verpflichtungen, welche

- die Entwicklung der Informationssicherheitspolitik
- die Sicherstellung des Erreichens der Ziele und Pläne in Bezug auf die Informationssicherheit
- die Festlegung der Rollen und Verantwortlichkeiten
- die Vermittlung der Bedeutung des ISMS gegenüber der Organisation
- die Bereitstellung ausreichender Ressourcen zur Umsetzung des ISMS
- die Entscheidung über ein akzeptables Risikoniveau
- sowie die Bewertung des ISMS

umfassen.

Das Management der Ressourcen welches die Ermittlung und Bereitstellung der Ressourcen sowie die Schulung, das Bewusstsein und die Kompetenz des Personals sicherstellt.

Im 6. Kapitel wird die Managementbewertung des ISMS durch Eingaben, Ergebnisse und die Anforderungen an ISMS-Audits näher gebracht.
Eingaben sind hierbei:

- Ergebnisse der ISMS-Audits und –Überprüfungen
- Rückmeldungen betroffener Parteien
- Mögliche Techniken, Produkte o. ä. zur Verbesserung der Leistung des ISMS
- Status von Vorbeugungs- und Korrekturmaßnahmen
- Schwachstellen und Bedrohungen, welche bei der Risikoeinschätzung (Kapitel 4.2.1) nicht berücksichtigt wurden
- Folgemaßnahmen vorangegangener Managementbewertungen
- Änderungen die sich auf das ISMS auswirken können

- sowie Empfehlungen für die Verbesserung

Die dabei erwarteten Ergebnisse sind:

- Verbesserung der Wirksamkeit des ISMS
- Bedarfsgerechte Anpassung der Verfahren zur Gewährleistung der Informationssicherheit

In einem weiteren Unterkapitel werden die Anforderungen an ISMS-Audits auf die folgenden Punkte reduziert.

- Feststellung der Erfüllung der Anforderungen des BS7799-2 Standards sowie gesetzlicher und behördlicher Vorschriften
- Festellen der Einhaltung der identifizierten Anforderungen an die Informationssicherheit
- Feststellen der wirksamen Umsetzung der Maßnahmen, Verfahren und Prozesse des ISMS
- Festellen der Entsprechung der Leistungserwartungen

Abschließend werden im Kapitel 7 die Punkte der ISMS-Verbesserung erläutert. Dazu zählen die kontinuierliche Verbesserung, welche auf der Grundlage der Managementbewertung das ISMS verbessert sowie die Korrekturmaßnahmen welche aus der Identifikation, der Ermittlung von Ursachen, der Beurteilung des Handlungsbedarfs, der Ermittlung und Umsetzung von Maßnahmen, der Aufzeichnung von Ergebnissen sowie der Überprüfung der Maßnahmen von notwendigen Korrekturen bestehen.

Darüber hinaus werden im Anhang A die Abschnitte 3 bis 12 des ISO/IEC 17799:2000 Standards zur Unterstützung der Implementation des ISMS bereitgestellt. Anhang B enthält eine Anleitung zur Anwendung der Norm, dabei werden die Phasen des ISMS noch einmal näher erläutert. Im dritten Anhangteil dem Anhang C werden die Beziehungen zu anderen Standards hergestellt.[109]

[109] Vgl. BS7799-2:2002, S. 15 - 40

4.3.2 Vergleich mit dem Referenzmodell des Qualitätsmanagements

Grundlage der Modellierung des BS7799-2:2002 Standards ist der Vergleich mit dem Referenzmodell der DIN EN ISO9001:2000 (QMRef11), welches durch die Firma IDS Scheer AG bereitgestellt wurde. Dazu werden die bereits in Kapitel drei dieser Arbeit betrachteten Standards herangezogen und in den Ideen und Ansätzen vergleichen. Auf diese Betrachtung folgt eine Aufstellung der Gemeinsamkeiten welche wiederum in der Modellierung des BS7799-2:2002 Standards wieder verwendet werden können.

Grundlegend gleiche Ideen und Ansätze

Der BS7799-2:2002 Standard wurde explizit mit dem DIN EN ISO9001:2000 Standard harmonisiert um die Implementierung und Durchführung von konsistenten und integrierten Managementsystemen zu ermöglichen. Zur Umsetzung dieses Managementsystems zur Entwicklung, Umsetzung und Verbesserung des Informationssicherheits-Managementsystems wurde der PDCA-Kreislauf zur kontinuierlichen Verbesserung eingeführt.

Somit gewährleistet die BS7799-2:2002 ein stabiles Modell zur Implementierung der Grundsätze in den Richtlinien welche die Risikoeinschätzung, Sicherheitsgestaltung und -umsetzung, das Sicherheitsmanagement, die Überprüfung und die Neufestlegung regelt.

Für die betrachteten Standards lassen sich fünf allgemeine Anforderungen ausmachen, welche explizit in diesen Anwendung finden.[110]

1. Erste Forderung ist ein **Managementsystem**, welches im Hinblick auf alle organisationsbezogenen, im Standard betrachteten, Geschäftsaktivitäten und –risiken entwickelt, wird.

2. Zweite Forderung ist die **Umsetzung des entwickelten Managementsystems.**

3. Die dritte Forderung ist die **kontinuierliche Verbesserung** des umgesetzten Managementsystems.

[110] Vgl. BS7799-2:2002, S. 1; Vgl. DIN EN ISO 9001:2000, S. 10 - 17

4. Die vierte Forderung ist die **Dokumentation** dieses Managementsystems.

5. Das Managementsystem stellt die Umsetzung des **PDCA-Konzept** nach Dr. William Edwards Deming dar.

Aus diesen fünf Forderungen ergeben sich somit Gemeinsamkeiten in der Umsetzung der Standards, die sich wiederum in gleichen oder ähnlichen Elementen der Standards widerspiegeln. Um diese herauszustellen, wurde, wie bereits erwähnt, das QM-Referenzmodell in die Betrachtung einbezogen. Dabei ergeben sich die im Folgenden genannten Übereinstimmungen, welche bei der Abbildung der Prozesse des ISMS nach BS7799-2:2002 Anwendung finden können.

- **Managementbewertung**
    1. Audit
- **Management von Ressourcen**
    1. Ressourcen
    2. Schulung und Einstellung im Bedarfsfall
- **Ständige Verbesserung**
    1. Korrekturmaßnahmen

Managementbewertung

Im Bereich der Managementbewertung wird in beiden Standards auf das Mittel der Auditierung zurückgegriffen um die geforderte Überprüfung und Bewertung des Managementsystems durchführen zu können. Im BS7799-2 Standard werden Audits als Mittel genannt, die mögliche Durchführung eines solchen aber offen gelassen. In diesem Fall bietet das Referenzmodell des DIN EN ISO9001:2000 Standards Unterstützung. Der Ablauf eines Audits wurde im Qualitätsmanagement-Referenzmodell abgebildet. Dieser Umstand lässt es zu, in Anlehnung an diese vorhandenen Modelle, den Bereich der Auditierung ebenfalls in dem Referenzmodell des BS7799-2 im gleichen Detaillierungsgrad abzubilden.

Management von Ressourcen

Im BS7799-2:2002 Standard wird im Bereich des Managements der Ressourcen ausschließlich auf die Bereitstellung der Ressourcen für das Managementsystem verwiesen.

Ressourcen wiederum werden nicht benannt. Im Vergleich mit dem Referenzmodell des DIN EN ISO9001:2000 Standards stellt sich eine Benennung allgemeiner Ressourcen in diesem heraus. Hier wurden speziell Personal, Infrastruktur, Information und Arbeitsumgebung benannt. Diese Ressourcen lassen sich wiederum plausibel für das Information Security Management System einsetzen. Somit folgt eine Anlehnung an das Ressourcenmanagement in diesem Fall. Die Ressourcenbenennung wird somit in das Referenzmodell des BS7799-2 einbezogen.
Ein weiterer Punkt ist die Schulung der Mitarbeiter und Einstellung im Bedarfsfall. Der BS7799-2 Standard benennt diesen Punkt, lässt aber wiederum ein Vorgehen offen. Im Vergleich mit dem Qualitätsmanagement-Referenzmodell zeigt sich die detaillierte Abbildung dieser Prozesse, welche somit eine Anlehnung an diese Vorgehensweise bezogen auf das ISMS zulässt.

ISMS - Verbesserung

Der in beiden Standards gleichermaßen angewandte Grundsatz der kontinuierlichen Verbesserung bedarf Korrekturmaßnahmen im Fall der Auffindung von Verbesserungspotenzialen. In den beiden verglichenen Standards werden diese genannt, jedoch bietet das Referenzmodell des Qualitätsmanagements in diesem Fall wiederum einen höheren Detailgrad. Die hier abgebildeten Prozesse lassen sich durch ihren generischen Charakter ebenfalls plausibel auf das ISMS anwenden.

Ergebnis

Im Ergebnis zeigt sich, dass die Elemente Audit, Ressourcen, Schulung der Mitarbeiter und Einstellung im Bedarfsfall sowie die Korrektrumaßnahmen des Referenzmodells der DIN EN ISO9001:2000 eine hohe Übereinstimmung mit dem BS7799-2:2002 Standard zeigen und dieses bereichern können. Sie sind somit für die Verwendung im Referenzmodell des BS7799-2:2002 durch spezifische Anpassungen, auf die im Kapitel 4.2.4 dieser Arbeit näher eingegangen wird, geeignet. Darüber hinaus bieten diese Gemeinsamkeiten die Möglichkeit das Referenzmodell des BS7799-2:2002 in den genannten Bereichen durch eine detaillierte Darstellung zu unterstützen.

4.3.3 Das Referenzmodell

Dieser Abschnitt gibt einen Überblick über das Referenzmodell und zeigt dabei anhand markanter Modelle aus dem Referenzmodell wie die Konventionen der Modellierung Anwendung finden. Markante Modelle sind dabei das Übersichtsmodell, das Organisationsmodell, die Modelle der Kapitelebene sowie ausgewählte Modelle der Mangementsicht und Arbeitssicht. Dabei werden die Abläufe welche in Anlehnung an das Referenzmodell des DIN EN ISO 9001:2000 Standards erstellt werden konnten und die Betrachtung der Risikoeinschätzung und Behandlung einzeln erläutert.
Dieser Abschnitt der Arbeit ordnet sich somit in die Phasen drei und vier des Vorgehensmodells zur Referenzmodellierung ein.
Zuvor werden jedoch die grundlegenden Strukturen, welche im ARIS-Explorer erstellt werden, betrachtet. Die Umsetzung der Gruppenstruktur als Teil der Konventionen der Modellierung wird dabei in die dritte Phase des Vorgehensmodells eingeordnet.

Gruppenstruktur

Aus den Konventionen der Modellierung geht eine Gruppenstruktur hervor welche sich in drei Ebenen aufteilt. Dabei werden die Gruppen, wie in Abbildung 4.10 dargestellt, jeweils in die Gruppe des Übersichtsdiagramms (hier Referenzmodell), die Kapitelgruppe (hier von 4.2.1 Festlegen des ISMS bis 7 ISMS-Verbesserung im Standard) und die Sichten innerhalb der Kapitel (Arbeits- und Managementsicht) eingeteilt.
Auf der Ebene der Kapitel ordnet sich des Weiteren die Gruppe „0. Ebenenübergreifende“ Modelle ein.
In der Gruppe Referenzmodell findet sich dabei neben den untergeordneten Gruppen ausschließlich das Übersichtsmodell. Wird nun weiter in die darunter liegenden Gruppen vorgegangen so zeigt sich auf der Kapitelebene ein ähnliches Bild. Lediglich die untergeordneten Sichten und das Modell zu dem jeweiligen Kapitel des Standards werden hier eingefügt. In der Gruppe der ebenenübergreifenden Modelle werden im Gegensatz dazu keine weiteren Untergruppen dargestellt. Hier findet sich ausschließlich ein Modell. Auf der Ebene der Sichten werden ebenfalls keine weiteren Untergruppen angelegt. Es werden hier ausschließlich Modelle abgelegt.

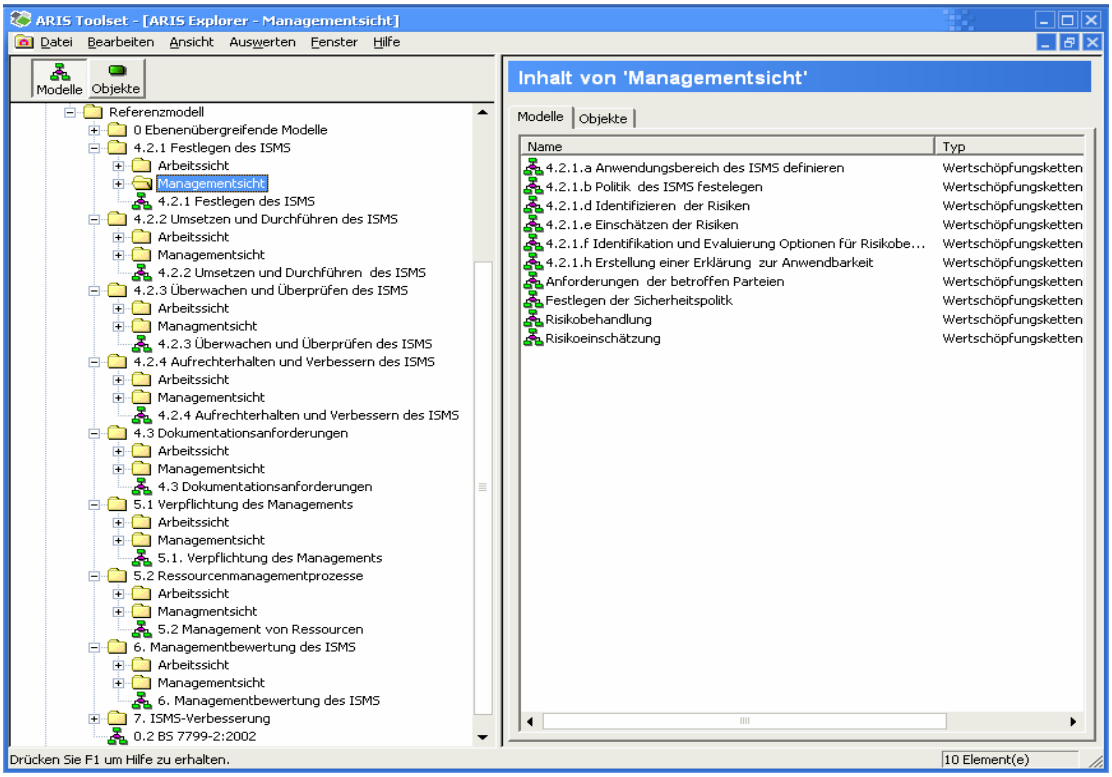


Abb. 4.10: Gruppenstruktur des Referenzmodell im ARIS Explorer

Referenzmodellsichten

Das Referenzmodell bietet, wie bereits in der Gruppenstruktur beschrieben, zwei Sichten die mit Modellen hinterlegt sind.
Erste Sicht ist die Managementsicht, welche in der Gruppenstruktur, durch die gleichnamige Gruppe vertreten ist. Sie zeigt dabei die bereits genannte Top-Down-Sicht und umfasst ausschließlich den Standard und den Vergleich mit dem QM-Referenzmodell entnommene Elementen.
Zweite Sicht in der Gruppenstruktur ist die Arbeitssicht, welche die Prozesse im Detail durch erweiterte ereignisgesteuerte Prozessketten (eEPKs) und Funktionszuordnungsdiagrammen (FZDs) beschreibt. Es werden spezielle Arbeitsschritte für das Vorgehen bei der Anwendung des Referenzmodells in einer Organisation beschrieben.

Übersichtsdiagramm WKD: 0.2 BS 7799-2:2002

Den Einstieg in das Referenzmodell bildet das, in Abbildung 4.11 gezeigte, WKD „0.2 BS7799-2:2002“ in welchem der in Kapitel 3.1 beschriebene PDCA-Kreislauf auf den BS7799-2:2002 Standard angewendet, dargestellt ist. Als Übersichtsdiagramm ist es

dabei gemäß den Konventionen der Modellierung mittels des Wertschöpfungsketten-diagramms modelliert. Dabei finden die Symboltypen Wertschöpfungskette und Fachbegriff Verwendung. Zur Erleichterung des Einstiegs in das Referenzmodell sind dabei lediglich die wesentlichen Funktionen des Referenzmodells dargestellt. Durch die grafische Anordnung der Symbole lässt sich der Kontrollfluss leicht erkennen. Dieser zeigt den Verlauf des Kreislaufs beginnend bei dem Festlegen des ISMS über das Umsetzen und Durchführen, dem Überwachen und Überprüfen, Erhalten und Verbessern bis hin zum erneuten Festlegen des ISMS. Somit zeigt sich ein geschlossener Kreislauf, welcher Input durch die betroffenen Parteien durch Anforderungen und die Verwaltung der Informationssicherheit bekommt und dessen Output ebenfalls an die Verwaltung der Informationssicherheit durch die betroffenen Parteien geht.

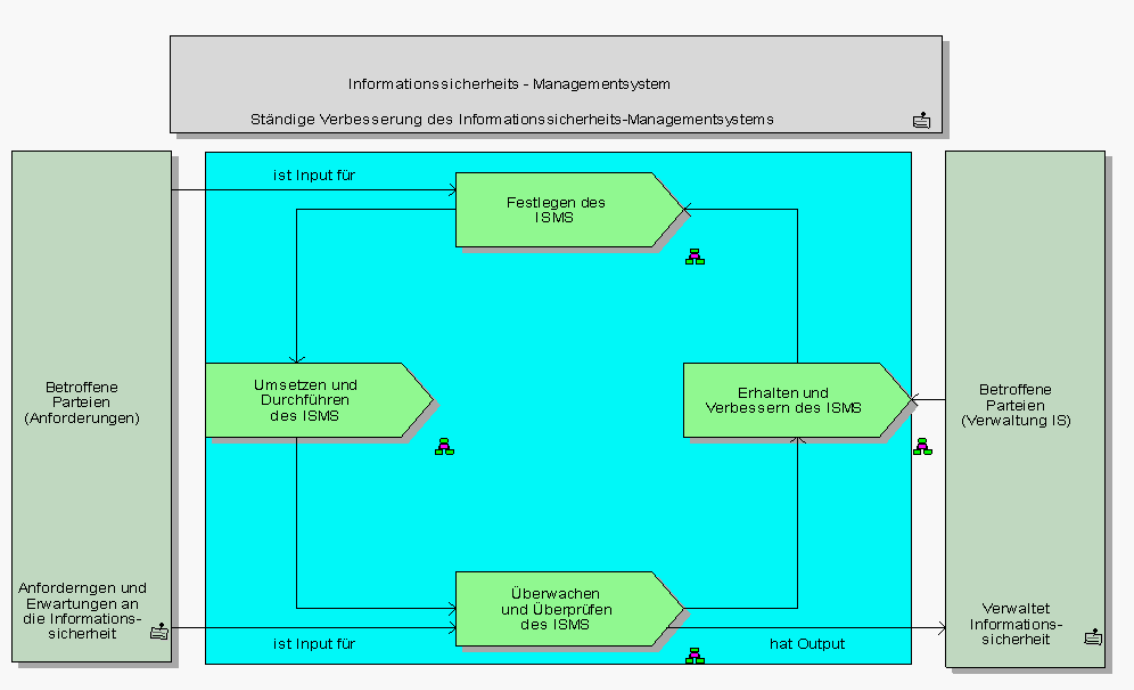


Abb. 4.11: Übersichtsmodell WKD: 0.2 BS7799-2:2000

Als Übersichts- bzw. Einstiegsdiagramm ordnet es sich in der Gruppenstruktur des ARIS-Toolsets auf der 1. Ebene, der Kapitelebene übergeordnet, ein.
Die Modelldarstellung entspricht dabei der den Konventionen der Darstellung sowohl in der Anordnung der Symbole als auch in der Anordnung des gesamten Modells auf der Modellierungsfläche. Des Weiteren sind die Hinterlegungen wie in den Konventionen gefordert an der rechten unteren Kante der Symbole angeordnet. Die Benennung

der Wertschöpfungsketten und Fachbegriffe konnte direkt dem Standard entnommen werden[111]. Somit war ein Anpassen bzw. Kürzen bei der Benennung nicht notwendig.
Um eine detailliertere Darstellung der einzelnen Wertschöpfungsketten zu erhalten lässt sich für jedes Wertschöpfungskettensymbol im Modell eine Hinterlegung aufrufen, welche auf ein weiteres WKD auf Kapitelebene verweist.
In den folgenden Abschnitten wird nun die Organisationsstruktur gefolgt von den Hinterlegungen der Wertschöpfungskettensymbole des Übersichtdiagramms betrachtet

Ebenenübergreifende Modelle Organigramm: Organisation

Der Standard gibt für das ISMS ausschließlich zwei Organisationseinheiten vor. Diese sind die Organisation und das Management. Die Organisation zeigt hierbei Verantwortung für das gesamte ISMS, speziell für:

- die Festlegung
- die Umsetzung
- die Überwachung (hierbei die ISMS-Audits)
- die Überprüfung
- die Aufrechterhaltung
- die Verbesserung des ISMS
- Schulung, Bewusstsein und Kompetenz.

Das Management wird explizit für:

- die Informationspolitik
- die Sicherstellung das Ziele und Pläne für die Informationssicherheit festgelegt
- Rollen und Verantwortlichkeiten für Informationssicherheit bestimmt
- Bedeutung des Erreichens von Sicherheitszielen und der Einhaltung der Informationssicherheitspolitik, seine Verantwortlichkeiten im Rahmen des Gesetzes und die Notwendigkeit für kontinuierliche Verbesserung vermittelt
- Bereitstellung der Ressourcen
- Entscheidung über ein akzeptables Risikoniveau
- Managementbewertung des ISMS genannt.

[111] Vgl. BS7799-2:2002, S. 2

Darüber hinaus werden die Rollen Auditor, Informationssicherheitsverantwortlicher und Informationsverantwortlicher für die Bereiche Audit und Risikoeinschätzung bzw. Risikobehandlung, welche im Weiteren detailliert betrachtet werden, herangezogen. Dabei übernimmt der Auditor die Planung, Durchführung und Auswertung der Audits. Der Informationssicherheitsverantwortliche begleitet den gesamten Prozess der Planung, der Implementation, des Einsatzes und der Verbesserung des ISMS. Die Rolle des Informationsverantwortlichen wird von einer Person mit Kenntnis der jeweiligen Abteilung, der bedrohten Werte dieser Abteilung sowie deren Bedrohungen und Schwachstellen, übernommen.

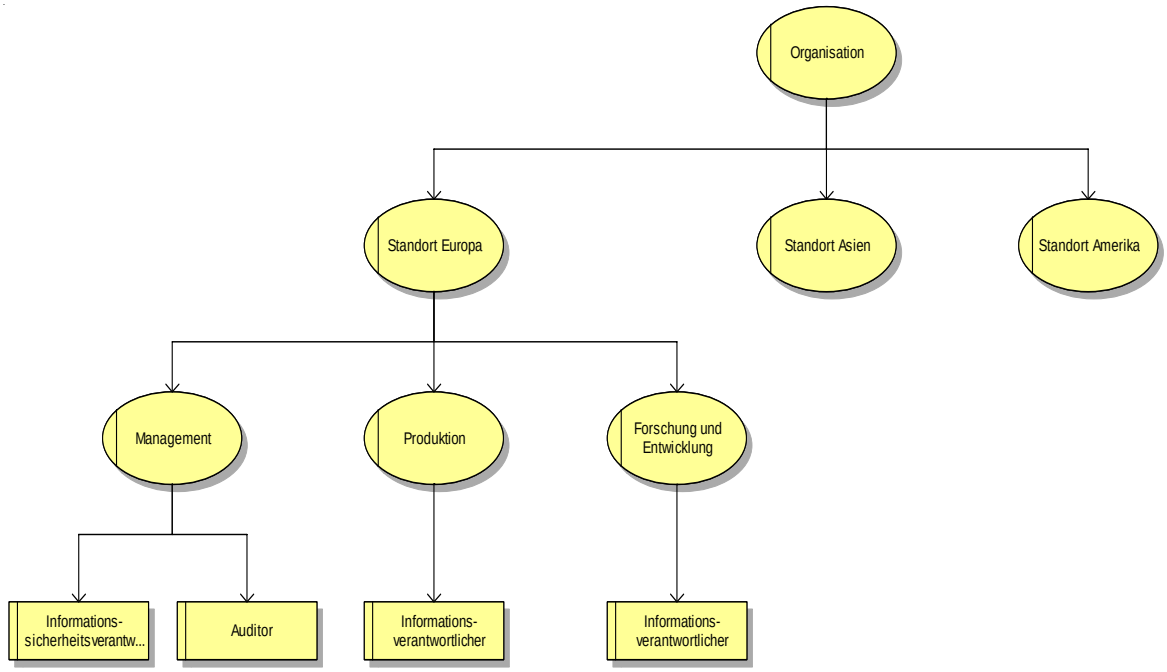


Abb. 4.12: Organigramm: Organisation

Abbildung 4.12 zeigt die Darstellung der möglichen Organisationsstruktur mit Bezug auf die Rollen in der Organisation, welche in der Abbildung des Standards, den detailliert betrachteten Audit sowie der weiteren Betrachtung der Risikoeinschätzung und -behandlung Anwendung finden.

Kapitelebene WKD: 4.2.1 Festlegen des ISMS

Während in dem übergeordneten WKD die Wertschöpfungskette „Festelegen des ISMS“ in den PDCA-Kreislauf eingebunden ist, ist in der Abbildung 4.13, welche die Hinterlegung der Wertschöpfungskette zeigt, die Wertschöpfungskette detaillierter dar-

gestellt. Dabei werden die Schritte des Festlegens übersichtsartig dargestellt. Beginnend bei den Anforderungen der betroffenen Parteien, welche Beachtung finden, über die Definition einer systematischen Vorgehensweise, der Risikoeinschätzung, Risikobehandlung und dem Erstellen einer Informationssicherheitspolitik. All diese Maßnahmen bedürfen am Ende einer Genehmigung und Autorisation durch das Management. Gemäß den Konventionen ordnet sich dieses Modell auf der Kapitelebene in die Gruppe „4.2.1. Festlegen des ISMS“ ein welche wiederum in der Bezeichnung mit dem entsprechenden Kapitel im Standard übereinstimmt. Entsprechend der Festlegung wurde der Diagrammtyp WKD, unter Verwendung der Wertschöpfungsketten-Symbole, angewendet. Das Modell ordnet sich dabei gemäß den Konventionen auf der Modellierungsfläche an. Bei der Verwendung der Symbole lässt sich die unterschiedliche Färbung, welche die dem Standard entnommenen (blass grün dargestellt) von den durch den Modellierer selbst erstellten Wertschöpfungsketten (kräftiger Grünton) gut erkennen. Die Darstellung der Kanten weist ebenfalls in diesem Modell zwei Varianten auf, welche den Konventionen entsprechen. Der hierarchische Zusammenhang wurde mittels der durchgezogenen Kanten dargestellt, während der zeitliche Zusammenhang durch die gestrichelten Kanten sichtbar gemacht wurde. Dabei lässt sich ein zeitlicher Zusammenhang, beginnend bei den Anforderungen bis zur abschließenden Genehmigung durch das Management erkennen. Weiterhin werden bei der Darstellung der Symbole die Hinterlegungen auf der rechten Seite der unteren Kante der Wertschöpfungsketten angezeigt, sowie Symbole für externe Verknüpfungen mittig unterhalb der Wertschöpfungsketten. Die hier dargestellten externen Verknüpfungen ermöglichen den Zugriff auf die Software zur Unterstützung der Risikoeinschätzung und Risikobehandlung. Diese wird im 5 Kapitel dieser Arbeit näher betrachtet. Um den Einsatzzweck zu verdeutlichen sind diese Verknüpfungen an den Wertschöpfungsketten „Risikoeinschätzung durchführen“ und „Risikobehandlung durchführen“ angebracht. Die Hinterlegungen durch weitere WKD und eEPK der beiden genannten Wertschöpfungskettensymbole werden in Kapitel 4.3.2 betrachtet.

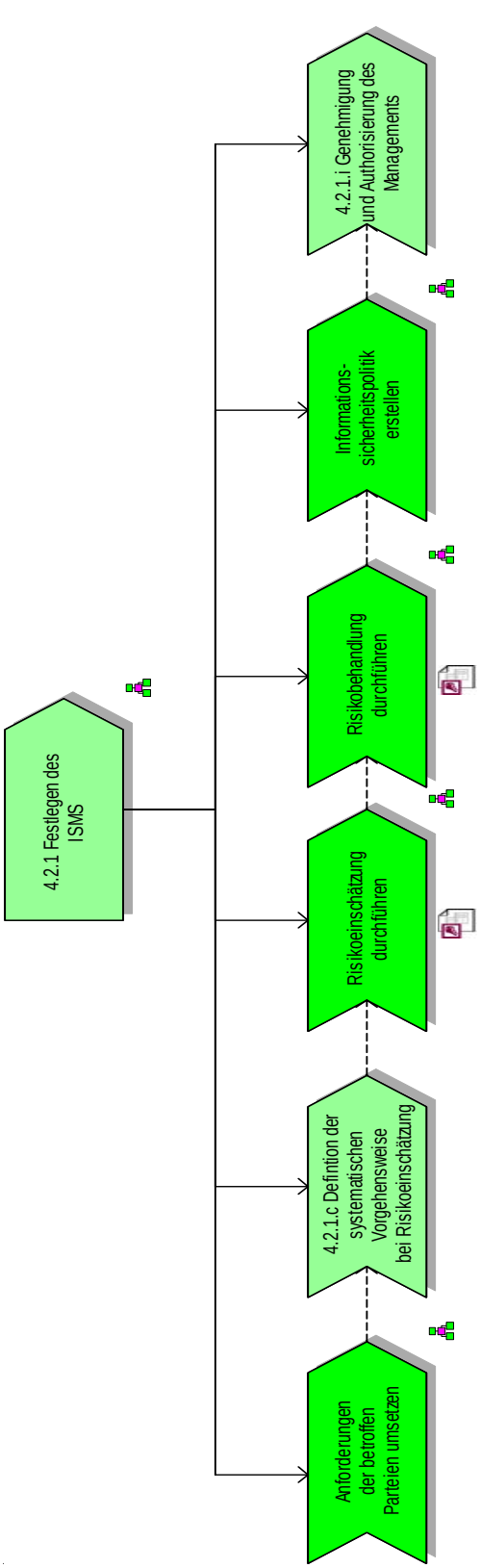


Abb. 4.13: WKD: 4.2.1 Festlegen des ISMS

Kapitelebene WKD: 4.2.2 Umsetzen und Durchführen des ISMS

Wird die Hinterlegung der Wertschöpfungskette „Umsetzen und Durchführen des ISMS“ im WKD 0.2 BS7799-2:2002 geöffnet so ergibt sich die Sicht auf die detaillierte Darstellung des Kapitels 4.2.2 „Umsetzen und Durchführen des ISMS“. In Abbildung 4.14 lässt sich diese erkennen. Darin wird der Ablauf des Durchführens und Umsetzens wie folgt beschrieben. Nach Formulierung des Risikobehandlungsplanes folgt die Umsetzung dieses Planes. An dieser Stelle wird durch die Darstellung mittels der gestrichelten Kante besonders auf die zeitliche Abfolge hingewiesen. Weiterhin umfasst dieses Kapitel die Verwaltung von Vorgängen, Verweist auf die Verwaltung von Ressourcen und das sofortige Erkennen und Behandeln von Sicherheitsvorfällen.

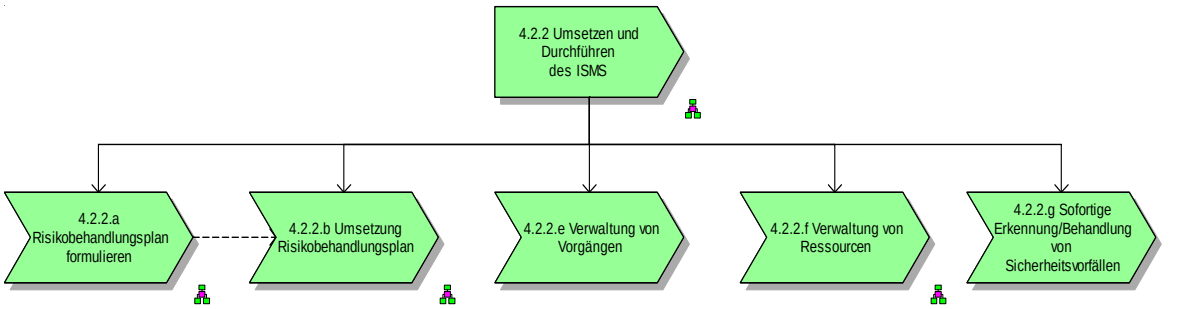


Abb. 4.14: WKD: 4.2.2 Umsetzen und Durchführen des ISMS

Gemäß den festgelegten Konventionen ist dieses Modell wiederum in der mit gleichem Namen versehenen Gruppe auf Kapitelebene zu finden. Die eingesetzten Symbole und Kanten entsprechen den für WKD vorgegebenen Typen. Einige der Wertschöpfungsketten sind mit Hinterlegungen versehen. Wobei im Folgenden die Hinterlegung der Wertschöpfungskette „4.2.2.a Risikobehandlungsplan formulieren“ näher betrachtet wird.

Managementsicht WKD: 4.2.2.a Risikobehandlungsplan formulieren

Diese WKD (siehe Abbildung 4.15) geht als Hinterlegung des in Abbildung 4.14 dargestellten WKD aus der Wertschöpfungskette „4.2.2.a Risikobehandlungsplan formulieren“ hervor und ordnet sich in die Managementsicht und in die gleichnamige Untergruppe des Kapitels „4.2.2 Umsetzen und Durchführen des ISMS“ ein.

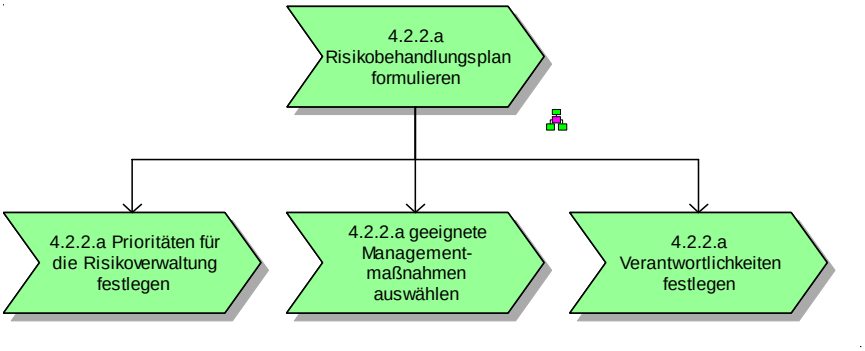


Abb. 4.15: WKD: 4.2.2.a Risikobehandlungsplan formulieren

Sie zeigt die drei notwendigen Maßnahmen zur Formulierung des Risikobehandlungsplanes. Diese umfassen die Festlegung der Prioritäten der Risikoverwaltung, Auswahl geeignete Managementmaßnamen sowie die Festlegung der Verantwortlichkeiten. Dabei ist keine zeitliche Reihenfolge dieser drei Maßnahmen vorgesehen. Lediglich die hierarchische Zuordnung der drei Maßnahmen ist durch die Verwendung der durchgezogenen Kante kenntlich gemacht. Des Weiteren entsprechen auch in diesem Modell Symboltypen und Anordnung den festgelegten Konventionen. Da der Standard hier keine detaillierten Informationen bereitstellt, wurde auf Hinterlegungen verzichtet.

Kapitelebene WKD: 4.2.3 Überwachen und Überprüfen des ISMS

Als weitere Hinterlegung des Übersichtsmodells findet sich die WKD „4.2.3 Überwachen und Überprüfen des ISMS“, welche in Abbildung 4.16 dargestellt ist. Sie ist dem Wertschöpfungskettensymbol „Überwachen und Überprüfen“ im Übersichtsmodell hinterlegt. Die Darstellung zeigt dabei die notwendigen Prozesse. Diese sind im einzelnen Überwachungsverfahren ausführen, Überprüfung der Wirksamkeit des ISMS, Restrisiko und Risikoniveau prüfen, ISMS Überprüfung durch das Management und Aufzeichnung der Maßnahmen und Zwischenfälle. Dabei stellt sich im Vergleich zum Standard das Fehlen der ISMS-Audits heraus. Diese wurden bewusst ausgelassen, da der Punkt „ISMS Überprüfung durch das Management“ auf das Kapitel 6. des Standards verweist und somit die Auditierung enthält. In der Darstellung und Anordnung der Symbole unterscheidet sich dieses WKD nicht von den bereits vorgestellten WKD auf Kapitelebene. Es finden wiederum gemäß der Konvention Wertschöpfungskettensymbole und durchgezogenen Kanten Verwendung.

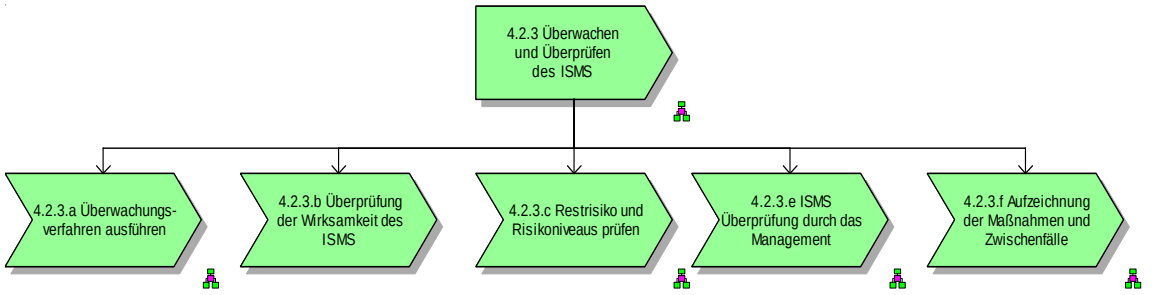


Abb. 4.16: WKD: 4.2.3 Überwachen und Überprüfen des ISMS

Dabei findet sich in diesem Diagramm kein zeitlicher Verlauf. Soweit dies im Standard beschrieben wurde, sind die einzelnen Prozesse des Überwachen und Überprüfen durch weitere WKD in der Managementsicht hinterlegt. Allgemein ordnet sich dieses WKD in die gleichnamige Gruppe auf der Kapitelebene ein. Durch den Verweis auf die Überprüfung durch das Management zeigt diese Hinterlegung auf das WKD „6. Managementbewertung des ISMS“ während die weiteren Hinterlegungen in der Untergruppe „Managementsicht“ angesiedelt sind.

Kapitelebene WKD: 4.2.4 Aufrechterhalten und Verbessern des ISMS

Diese Hinterlegung schließt den im Übersichtmodell dargestellten Kreislauf. Dabei handelt es sich um die Hinterlegung des Wertschöpfungskettensymbol „Aufrechterhalten und Verbessern des ISMS“ dargestellt in Abbildung 4.17. Er umfasst die Prozesse Umsetzung der identifizierten Verbesserungen im ISMS, Ergreifen geeigneter Korrektur- und Vorbeugungsmaßnahmen, Mitteilung der Ergebnisse und Abstimmung betroffener Partei sowie die Sicherstellung des Erreichens der Verbesserungen und Ziele. Diese sind keiner zeitlichen Reihenfolge unterworfen. Das WKD ordnet sich gemäß der Konventionen in der Gruppenstruktur auf Kapitelebene in die gleichnamige Gruppe ein. Die dargestellte Hinterlegung am Wertschöpfungskettensymbol „Ergreifen geeigneter Korrektur- und Vorbeugungsmaßnahmen“ verweist dabei auf ein weiteres gleichnamiges WKD welches sich in der Untergruppe Managementsicht einordnet.

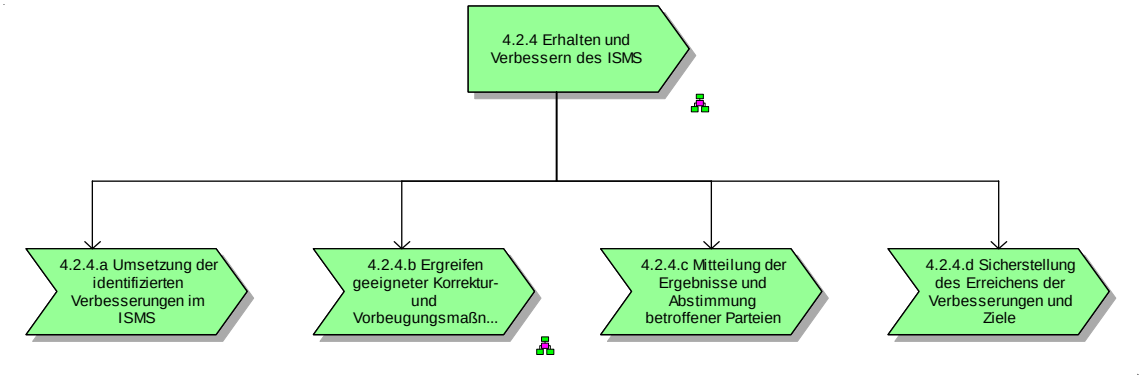


Abb. 4.17: WKD: 4.2.4 Aufrechterhalten und Verbessern des ISMS

Kapitelebene WKD: 4.3 Dokumentationsanforderungen

Im Gegensatz zu den vorherigen Modellen ist die WKD „4.3 Dokumentationsanforderungen“ nicht direkt mit dem Übersichtsmodell verknüpft. Der Grund hierfür liegt in der Beziehung der Dokumentationsanforderungen zu dem im Übersichtsmodell beschriebenen Kreislauf. Die Dokumentationsanforderungen beziehen sich dabei auf Kapitel 4 bis 7 des Standards. Die Dokumentation stellt, wie bereits im Vergleich herausgestellt, eine grundlegende Forderung des Standards dar. Dazu wird in den Modellen der Kapitel des Standards an den entsprechenden Stellen durch Hinterlegungen auf die Dokumentationsanforderungen verwiesen. Im Einzelnen beinhalten diese die Dokumentation, die Lenkung von Dokumenten und die Lenkung von Aufzeichnungen.

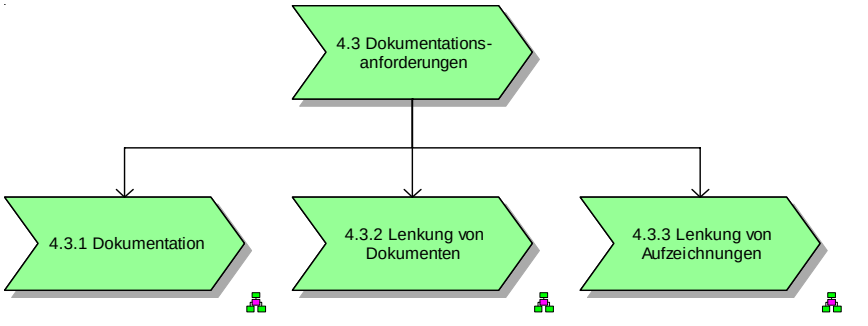


Abb. 4.18: WKD: 4.3 Dokumentationsanforderungen

Diese sind wiederum in ihrem hierarchischen Zusammenhang, unter Ausnutzung der in den Konventionen vorgestellten Mittel, in Abbildung 4.18 dargestellt. Dabei ordnet sich das WKD in die Gruppe „4.3 Dokumentationsanforderungen“ auf der Kapitelebene ein.

Die dargestellten Hinterlegungen verweisen wiederum auf die detailliertere, in der Gruppe „Managementsicht“ abgelegte, WKD.

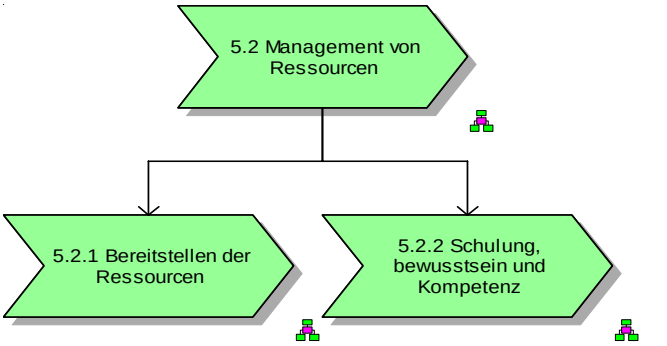


Abb. 4.19: WKD: 5.2 Management von Ressourcen

Für die Abbildungen 4.19, 4.20 und 4.21 gilt die gleiche Vorgehensweise zur Erstellung gemäß der Konventionen der Modellierung. Dabei ordnet sich das WKD „5.2 Management von Ressourcen“ sowie die in Abbildung 4.21 dargestellte „6. Managementbewertung“ und die in Abbildung 4.22 dargestellte „7. ISMS-Verbesserung“ in die gleichnamigen Gruppen auf der Kapitelebene ein. Weitere Diagramme, welche diesen Abschnitt vertiefen, finden sich im Anhang dieser Arbeit.

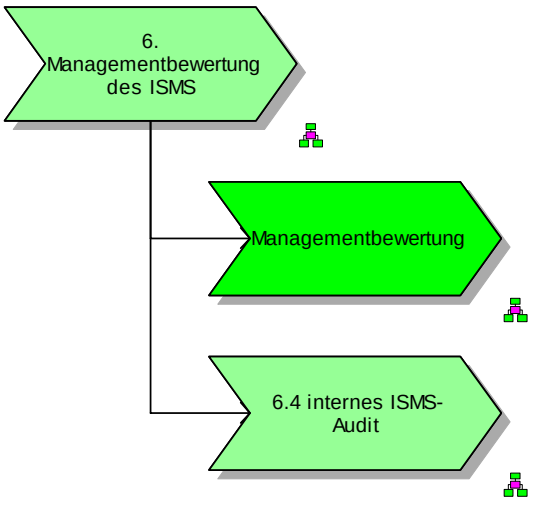


Abb. 4.20: WKD: 6. Managementbewertung des ISMS

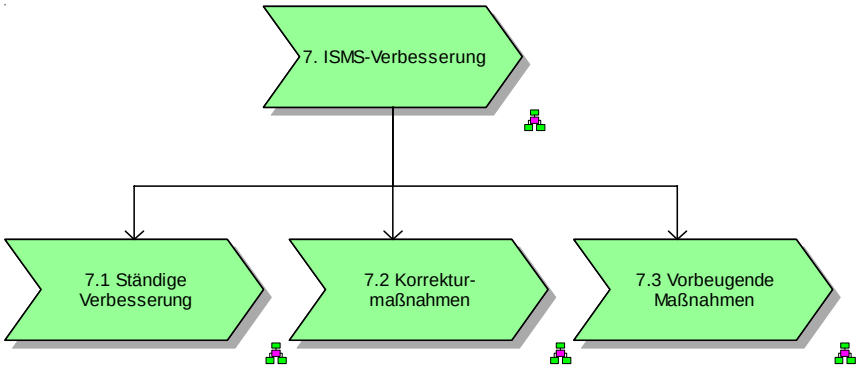


Abb. 4.21: WKD: 7. ISMS-Verbesserung

4.3.4 Abbildung der Gemeinsamkeiten zum Referenzmodell des Qualitätsmanagement

In diesem Abschnitt wird ins besondere auf die in Kapitel 4.3.2 dieser Arbeit festgestellten Gemeinsamkeiten eingegangen und die in dem Referenzmodell des BS7799-2:2002 angewendeten Modelle, welche dem Referenzmodell des Qualitätsmanagements entnommen und durch Anpassung eingesetzt werden konnten. Dabei werden die bereits genannten Punkte Bereitstellen der Ressourcen, Schulung Bewusstsein, Kompetenz, das Durchführen internen Audits sowie die Umsetzung von Korrekturmaßnahmen betrachtet. Die erste betrachtet Gemeinsamkeit stellt das Bereitstellen der Ressourcen dar.

Managementsicht WKD: 5.2.1 Bereitstellen der Ressourcen

In Kapitel 4.3.2 wurde dazu bereits festgestellt, dass der BS7799-2 Standard auf die Bereitstellung der Ressourcen für das ISMS verweist. Er lässt aber konkrete Ressourcen offen. Im Vergleich zum Referenzmodell der DIN EN ISO 9001:2000 konnte die konkrete Nennungen der Ressourcen erkannt werden. Die benannten Ressourcen sind für die Anwendung im Bereich des ISMS plausibel und wurden deshalb in die Abbildung des BS7799-2:2002 Standards einbezogen (siehe Abbildung 4.22). Dabei sind speziell die Ressourcen Budget, Informationen, Personal, Infrastruktur und, Arbeitsumgebung, wie in Abbildung 4.22 zu erkennen, einbezogen worden. Diese heben sich, wie in den Konventionen festgelegt, durch ihre farbliche Darstellung und Beschriftung von den dem Standard entnommenen Werten ab.

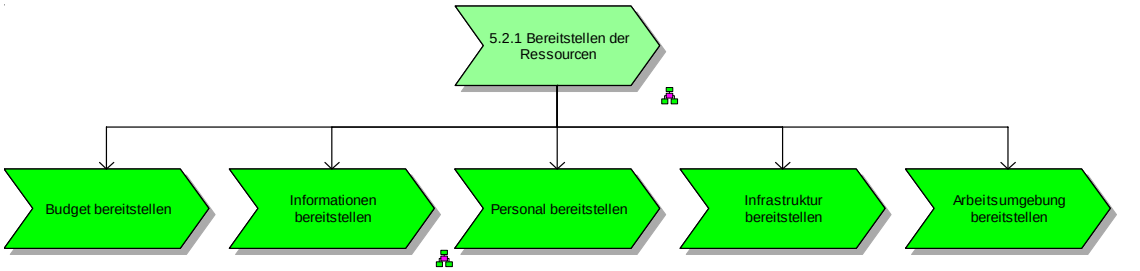


Abb. 4.22: WKD: 5.2.1 Bereitstellen der Ressourcen

In der Gruppenstruktur wird das WKD in die Untergruppe „Managementsicht“ und dort in die Gruppe „5.2. Ressourcenmanagementprozesse“ eingeordnet. Lediglich die Wertschöpfungskette „Informationen“ ist mit einer Hinterlegung versehen. Diese beinhaltet die Arbeitsabläufe zur Bereitstellung von Informationen, welche mittels eEPK erstellt wurden. Die hinterlegten eEPK ordnen sich als Arbeitsabläufe in die Untergruppe „Arbeitssicht“ der gleichen Kapitelgruppe ein.

Managementsicht FZD: 6.4. Internes ISMS-Audit

Eine weitere Anwendung der festgestellten Gemeinsamkeiten der beiden Standards findet sich in der detaillierten Abbildung internen Audits. Sie werden in diesem Referenzmodell mit Hilfe von FZD und eEPK abgebildet. Dabei unterstützt die Abbildung der Arbeitsabläufe zum Durchführen interner Audits im Referenzmodell der DIN EN ISO 9001:2000 die Abbildung dieser Prozesse. Abbildung 4.23 zeigt hierbei bereits den Ablauf auf einer hohen Abstraktionsebene. Dabei ordnet sich das FZD in die Managementsicht ein und wird in der entsprechenden Untergruppe der Gruppe „6. Managementbewertung des ISMS“ zugeordnet. In der Modellierung wurden als eingehende Dokumente, welche im BS7799-2 als Eingaben gekennzeichnet sind, die Anforderungen des BS7799 Standards, die gesetzlichen und behördlichen Vorgaben und die identifizierten Anforderungen an die Informationssicherheit gekennzeichnet. Diese Dokumente enthalten einerseits Vorgaben und andererseits Anforderungen, welche durch Fachbegriffe kenntlich gemacht sind und mittels Kanten mit den Dokumenten verbunden sind. Nachdem das interne Audit durchgeführt wurde liegt ein Ergebnis vor (Fachbegriff: Ergebnis), welches in das Dokument Auditbericht einfließt. Diese Darstellung ist sehr generisch und erfordert eine detaillierte Beschreibung, welche durch weitere eEPK und FZD gegeben wird.

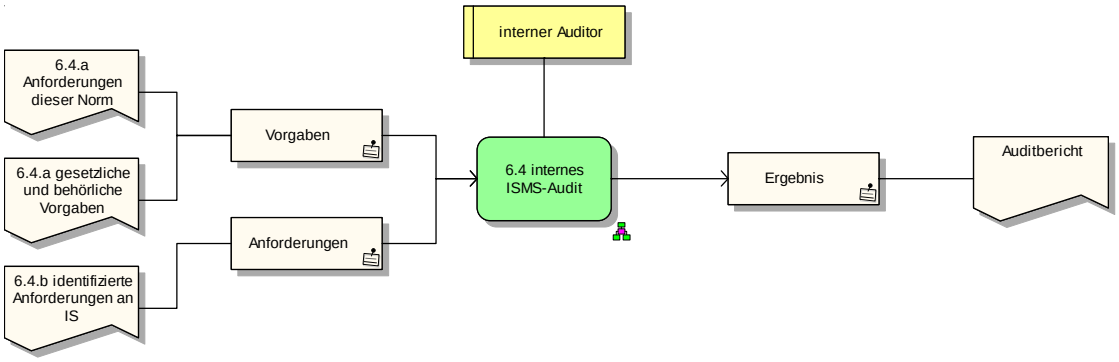


Abb. 4.23: FZD: 6.4 internes ISMS-Audit

Dabei werden in den eEPK und den hinterlegten FZD die Schritte vom Erstellen eines Auditjahresplanes über die Durchführung bis zur Bereitstellung der Ergebnisse abgebildet. Da die Betrachtung der Prozessketten den Rahmen der eigentlichen Arbeit sprengen würde, sei auf den Anhang verwiesen in welchem das erstellte Referenzmodell mit allen Diagrammen dargestellt wird.

Managementsicht WKD: 5.2.2.b Schulung und Einstellung im Bedarfsfall

Die Schulung und Einstellung im Bedarfsfall ist ebenfalls ein Punkt, welcher sich auf beide betrachteten Standards anwenden lässt. Durch die generische Art ist es sehr plausibel diesen im Referenzmodell des BS7799-2 einzubringen. Dabei werden, wie in Abbildung 4.24 dargestellt, die Einstellung im Bedarfsfall und der Punkt Schulung, Bewusstsein, Kompetenz angeführt.

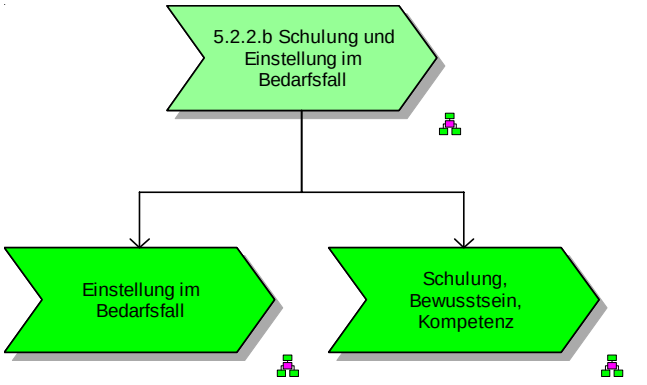


Abb. 4.24: WKD: 5.2.2.b Schulung und Einstellung im Bedarfsfall

Beide sind wiederum nicht dem Standard entnommen und weisen daher die für diesen Fall festgelegten Benennungs- und Farbkonventionen der Symbole auf. Beide sind jeweils mit Hinterlegungen durch eEPKs versehen. Das WKD ordnet sich in die Untergruppe Managementsicht der Gruppe „5.2. Ressourcenmanagementprozesse“ ein.
In Abbildung 4.25 ist die Hinterlegung des Wertschöpfungskettensymbols „Schulung, Bewusstsein, Kompetenz“ aus Abbildung 4.24 zu erkennen. Diese eEPK beschreibt den Ablauf einer Prüfung auf Schulungsbedarf. Dabei ist das Startereignis eine nicht ausreichende Qualifikation. Diese wird geprüft, ein Schulungsplan erstellt und die Schulung durchgeführt. Im Ergebnis ist der Schulungsbedarf ausreichend gedeckt oder nicht ausreichend gedeckt.
Wie bereits in der Beschreibung der übergeordneten Prozesskette erwähnt, ist dieser Prozess sehr generisch und lässt somit die Anwendung im Referenzmodell des BS7799-2:2002 zu. Die Modellierung dieser eEPK orientiert sich dabei wiederum an den Konventionen. Die Anordnung der Elemente und speziell für die in der Modellierung der eEPK vorgesehene Anordnung bei Verzweigung entspricht den Vorgaben. Durch die Namenskonventionen wurden Bezeichnungen der Objekte sowohl für die Ereignisse als auch für die Funktionen eingehalten. Die hier betrachtete eEPK ordnet sich dabei in die Gruppe „Arbeitssicht“ der übergeordneten Gruppe „5.2 Ressourcenmanagementprozesse“ ein.

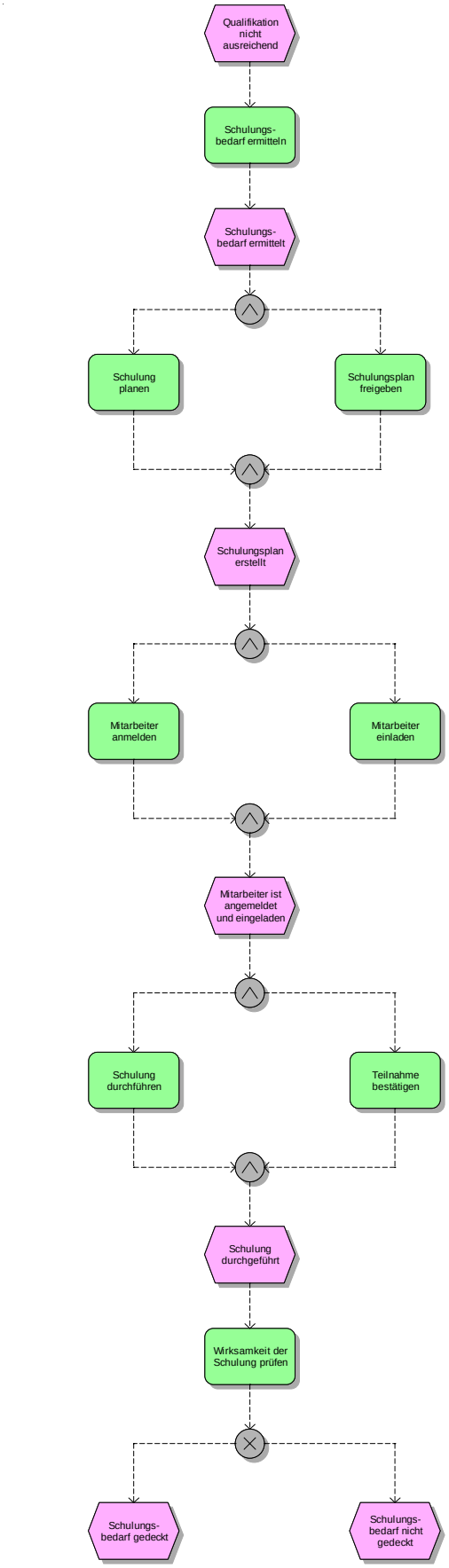


Abb. 4.25: eEPK: 5.2.2 Schulung, Bewusstsein, Kompetenz

4.3.5 Abbildung der Risikoeinschätzung und Risikobehandlung

Kernpunkt der Abbildung des BS7799-2:2002 Standards mit Hilfe des ARIS-Toolsets ist die detaillierte Darstellung der Prozess der Risikoeinschätzung und Risikobehandlung. Diese werden anhand charakteristischer Modelle in diesem Abschnitt vorgestellt und näher beleuchtet. Dabei werden zur Modellierung des Fachkonzeptes gemäß der vorgestellten Konventionen eEKP und FZD genutzt, während zur Modellierung des DV-Konzeptes ERM genutzt werden.

Arbeitssicht eEPK: 4.2.1.d.1 Identifikation der Werte innerhalb des ISMS

Initiale eEPK der Risikoeinschätzung ist die „Identifikation der Werte des ISMS“ (siehe Abbildung 4.26). Dabei werden bedrohte Werte in Organisationen und die für jeden einzelnen Wert verantwortliche Person identifiziert. Startereignis ist die notwendige Identifikation der bedrohten Werte in der Organisation. Darauf folgt deren Identifikation als Funktion mit Hinterlegung einer FZD. Diese wird in Abbildung 4.27 dargestellt und beschreibt die notwendigen Dokumente und beteiligten Personen der Feststellung der Werte. Dabei werden als Eingang alle Werte der Organisation und als Ergebnis der Funktion die identifizierten bedrohten Werte, welche für das ISMS relevant sind, dargestellt. Dem einfließenden Dokument ist dabei der Fachbegriff Werte vorgelagert welcher durch den Standard als Begriff vorgegeben wird. Diese Vorgehensweise wird im Weiteren bei allen FZDs der Risikoeinschätzung und -behandlung angewandt um den Zusammenhang mit den Begriffen, welche durch den Standard geprägt werden, herzustellen.
Nachdem diese festgestellt wurden, werden in der Ausgangs- eEPK die Personen bestimmt, welche für die identifizierten Werte zuständig sind. Dazu wird die Hinterlegung der Funktion „Feststellen der verantwortlichen Personen“ in Abbildung 4.27 betrachtet.

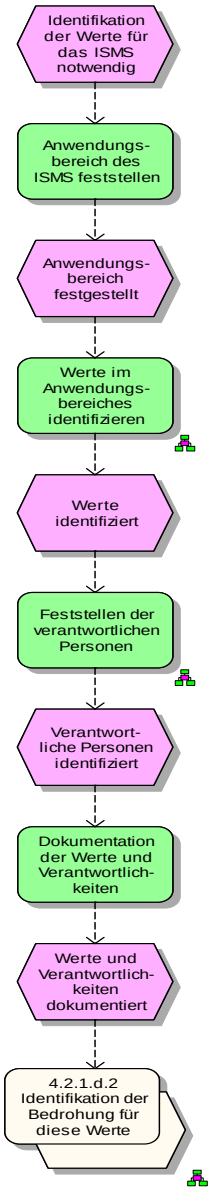


Abb. 4.26: Arbeitssicht eEPK: 4.2.1.d.1 Identifikation der Werte innerhalb des ISMS

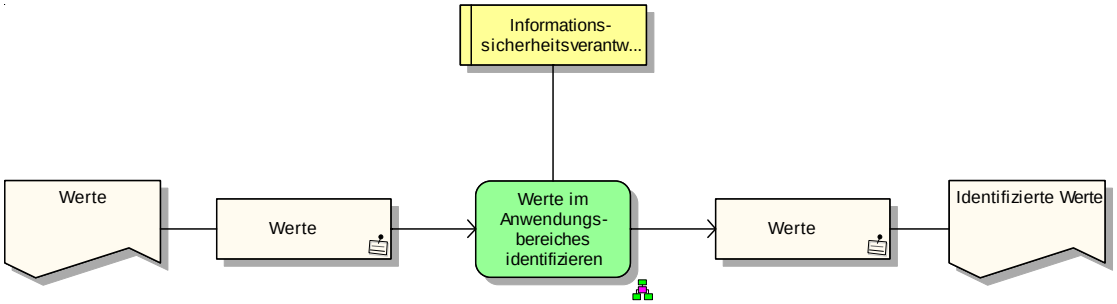


Abb. 4.27: Arbeitssicht FZD: Werte innerhalb identifizieren

Abbildung 4.28 zeigt die Feststellung der Verantwortlichen und bezieht dabei die identifizierten Werte und alle verantwortlichen Personen ein. Dabei werden wiederum die Fachbegriff Verantwortlichkeiten und Werte, welche aus den Dokumenten hervorgehen, den einzelnen Dokumenten zugeordnet und stellen somit eine Beziehung zum Standard her. Diese fließen in die Entscheidung ein. Dabei werden im Ergebnis die identifizierten Wert und die zugehörigen verantwortlichen Personen in einem Dokument hinterlegt. Somit zeigen die drei vorgestellten Modelle Arbeitsabläufe in unterschiedlichem Detaillierungsgrad und ordnen sich dabei gemäß der Konventionen in die Gruppe „Arbeitssicht“ der Gruppenstruktur ein.

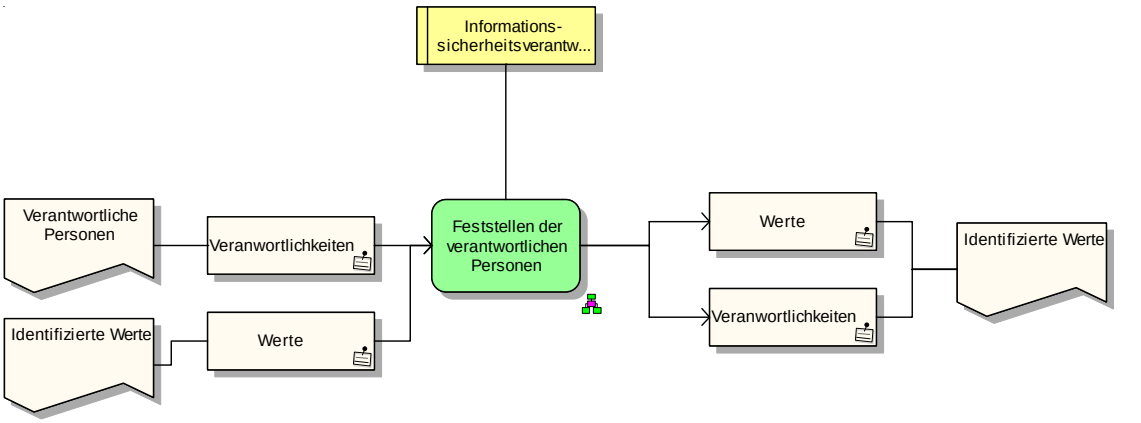


Abb. 4.28: Arbeitssicht FZD: Feststellen der verantwortlichen Personen

Die Abbildung auf der Fachkonzeptebene, welche die WKD, eEPK und FZD gemäß den festgelegten Konventionen der Modellierung nutzt, ist für eine DV-technische Umsetzung zu stark ausformuliert und lässt u. a. keine konsistente Modellierung der Beziehungen im Sinne der DV-Technik zu. Um die Beziehungen konsistent abbilden zu können werden ERM eingesetzt. Dazu zeigt Abbildung 4.29 das ERM zur Identifikation der Werte. Es beschreibt dabei die Beziehung „jeweils ein Wert hat einen Informationsverantwortlichen“. Diese Beschreibung ermöglicht es im Weiteren die Struktur in einer Datenbank konsistent umzusetzen.

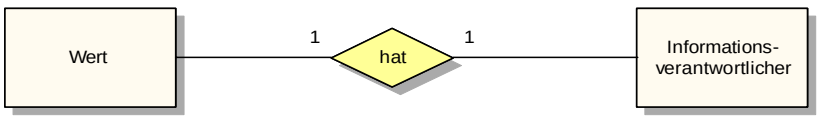


Abb. 4.29: DV-Konzept ERM: 4.2.1.d.1 Identifikation der Werte innerhalb des ISMS

Arbeitssicht eEPK: 4.2.1.d.2 Identifikation der Bedrohungen für diese Werte

Die Identifikation der Bedrohungen folgt der Identifikation der Werte. Dabei werden den dokumentierten bedrohten Werten mögliche Bedrohungen zugeordnet. Die eEPK beginnt mittels einer Prozessschnittstelle, welche die Verbindung zwischen der vorangehenden eEPK (siehe Abbildung 4.30) und dieser eEPK herstellt. Nachdem das Startereignis „Werte und Verantwortlichkeiten dokumentiert“ eingetreten ist, werden die Bedrohungen festgestellt. Dazu ist diese Funktion mittels der FZD „Feststellen der möglichen Bedrohungen der Werte“, welche in Abbildung 4.31 zu sehen ist, hinterlegt. Diese zeigt wiederum die Eingaben, Ausgaben und beteiligten Organisationseinheiten der Funktion. Eingaben sind die identifizierten Werte mit den dazugehörigen Verantwortlichen sowie alle möglichen Bedrohungen. Die Durchführung der Funktion unterliegt dabei der für diesen Wert verantwortlichen Person. Im Ergebnis werden jedem Wert die möglichen Bedrohungen zugeordnet und in einem Dokument festgehalten.

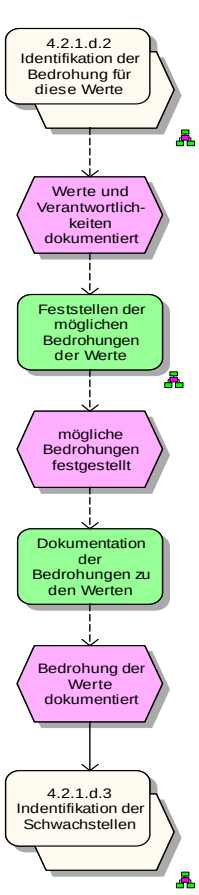


Abb. 4.30: Arbeitssicht eEPK 4.2.1.d.4 Identifikation der Bedrohungen

Die verwendeten Fachbegriffe, Werte, Verantwortlichkeiten und Bedrohungen, werden dabei gemäß Standard genutzt. In ihrer Einordnung finden sich die Modelle in der Gruppe „Arbeitssicht“ der Gruppenstruktur wieder und entsprechen somit der in den Konventionen festgelegten Zuordnung der Diagrammtypen.

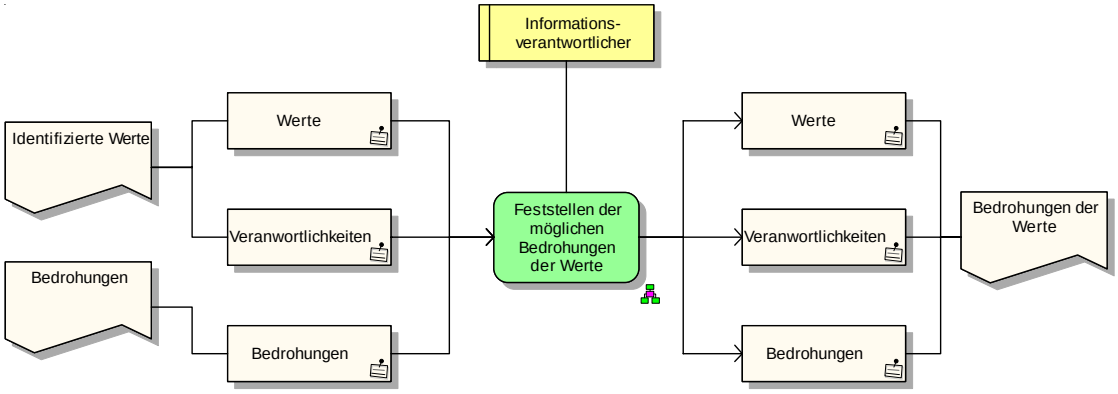


Abb. 4.31: Arbeitssicht FZD: Feststellen der möglichen Bedrohungen der Werte

Der Darstellung der Fachkonzeptebene folgt die DV-Konzeptebene, welche durch das ERM dargestellt wird. Dabei zeigen sich in Abbildung 4.32 die Beziehungen „jeder Wert hat einen Informationsverantwortlichen“ und „jeder Wert hat n Bedrohungen“. Die erste Beziehung ist aus dem ERM Abbildung 4.29 bereits bekannt, während die zweite Beziehung durch das Hinzufügen der Bedrohungen eingeführt wird. Somit ist die Anzahl der Bedrohungen, welche jedem identifizierten Wert zugeordnet werden, als maximal unendlich gekennzeichnet.

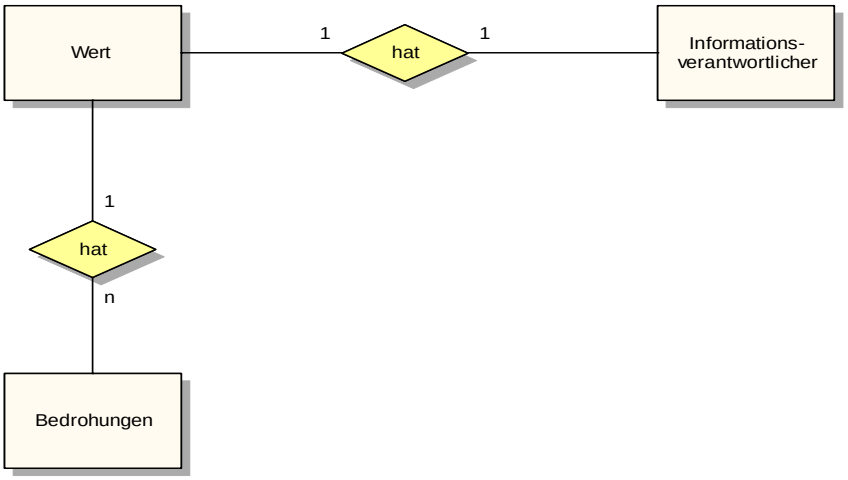


Abb. 4.32: DV-Konzept ERM: 4.2.1.d.4 Identifikation der Bedrohungen

Arbeitssicht eEPK: 4.2.1.f.2 Bewusste, objektive Akzeptanz der Risiken gemäß Politik

Werden nun die Schritte 4.2.1.d und e im Standard übersprungen, so ergeben sich im Standard vier Möglichkeiten der weiteren Behandlung von identifizierten Risiken. Unter Punkt 4.2.1.f werden dazu im Standard die Möglichkeiten „Ergreifung geeigneter Maßnahmen“, „bewusste Akzeptanz der Risiken sofern sie eindeutig der Politik der Organisation und den Kriterien für die Risikoakzeptanz genügen“, „Vermeidung von Risiken“ und die „Übertragung der entsprechenden Geschäftsrisiken auf andere Parteien, wie Versicherungen und Lieferanten“ genannt. Aus dieser Auswahl wird die „Bewusste, objektive Akzeptanz der Risiken gemäß Politik“ vorgestellt. Auf die drei weiteren Punkte, die dem vorgestellten Modell in Struktur und Abbildung ähnlich sind, wird verzichtet. Diese lassen sich wiederum im Anhang dieser Arbeit betrachten.
Abbildung 4.33 zeigt die eEPK zur bewussten und objektiven Akzeptanz der Risiken. Ausgangspunkt ist die Prozessschnittstelle zur WKD „4.2.1.f Identifikation und Evaluierung Optionen für Risikobehandlung“ welche die vier bereits genannten Möglichkeiten der Risikobehandlung zusammenfasst. Startereignis ist die Feststellung, dass geeignete Maßnahmen zur Behandlung der Risiken gewählt wurden. Gefolgt wird dieses Ereignis von der „Entscheidung über die Akzeptanz bei gewählten Maßnahmen“.
Diese Entscheidung lässt entweder die Akzeptanz des Risikos zu und führt zur dokumentierten Beendung des Prozesses der Risikobehandlung für diesen Wert oder das Risiko wird nicht akzeptiert und eine Entscheidung über ein weiteres Vorgehen wird notwendig. Dabei lässt sich zwischen dem Vermeiden der Risiken, der Übertragung von Risiken oder beiden Möglichkeiten entscheiden.
Die Entscheidung zur Akzeptanz des Risikos ist mit dem FZD „Entscheidung über Akzeptanz bei gewählten Maßnahmen“, welches in Abbildung 4.34 zu erkennen ist, hinterlegt.

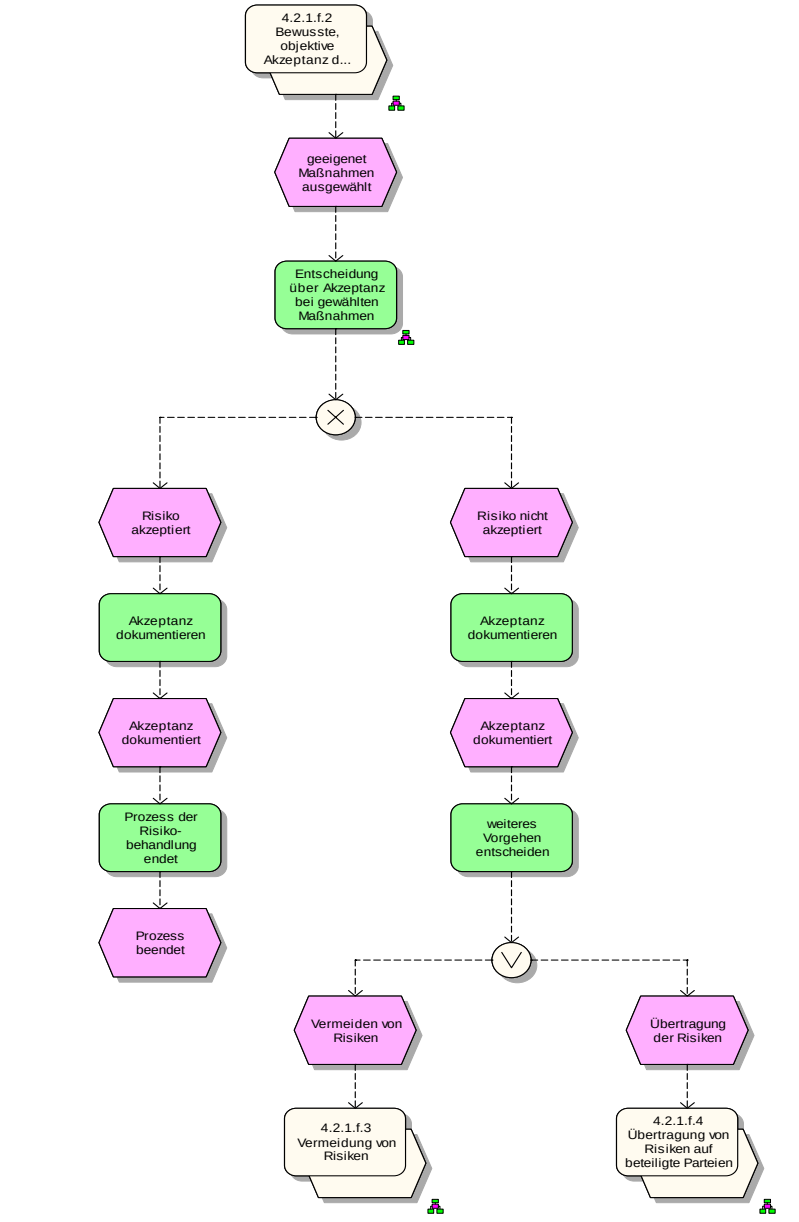


Abb. 4.33: Arbeitssicht eEPK: 4.2.1.f.2 Bewusste, objektive Akzeptanz der Risiken gemäß Politik

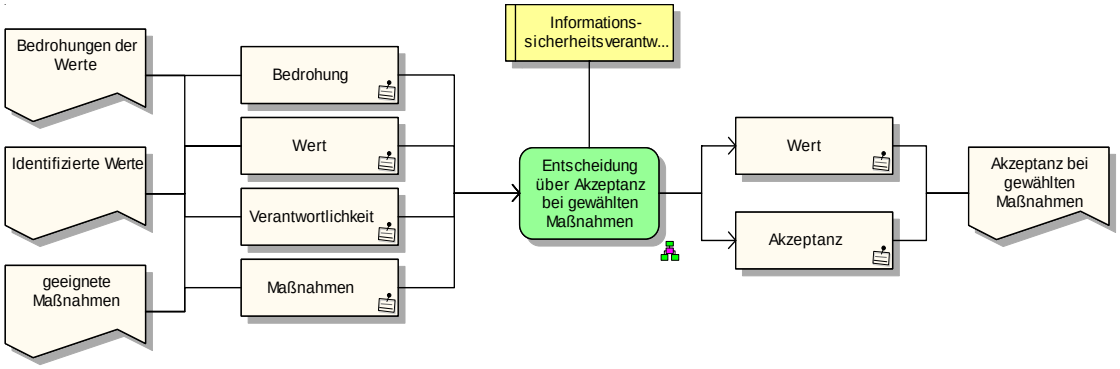


Abb. 4.34: Arbeitssicht FZD: Entscheidung über die Akzeptanz bei gewählten Maßnahmen

Das FZD zeigt dabei wiederum detailliert die Dokumente und Organisationsmitglieder, die an der Entscheidung beteiligt sind sowie deren Ergebnis. Im Einzelnen fließen die identifizierten Werte, Bedrohungen und geeigneten Maßnahmen ein. Wiederum sind hier die Fachbegriffe den Dokumenten zugeordnet. Die Entscheidung über die Akzeptanz wird durch den Informationsverantwortlichen getroffen. Somit zeigt sich im Ergebnis die dokumentierte Akzeptanz.

Die DV-Konzeptebene wird in diese Fall durch das ERM „4.2.1.f.2 Bewusste, objektive Akzeptanz der Risiken laut Politik“ in Abbildung 4.35 dargestellt. Im Mittelpunkt steht wiederum der Wert, welcher genau einen Informationsverantwortlichen, mehrere Bedrohungen und genau eine Festlegung über die Risikoakzeptanz haben kann. Dabei werden den einzelnen Bedrohungen jeweils mehrere Maßnahmen zugeordnet.

Die in diesem Zusammenhang dargestellten Modelle sind als Beispiele für die weiteren abgebildeten Prozesse der Risikobehandlung und Risikoeinschätzung zu sehen. Diese werden im Anhang im Einzelnen aufgeführt.

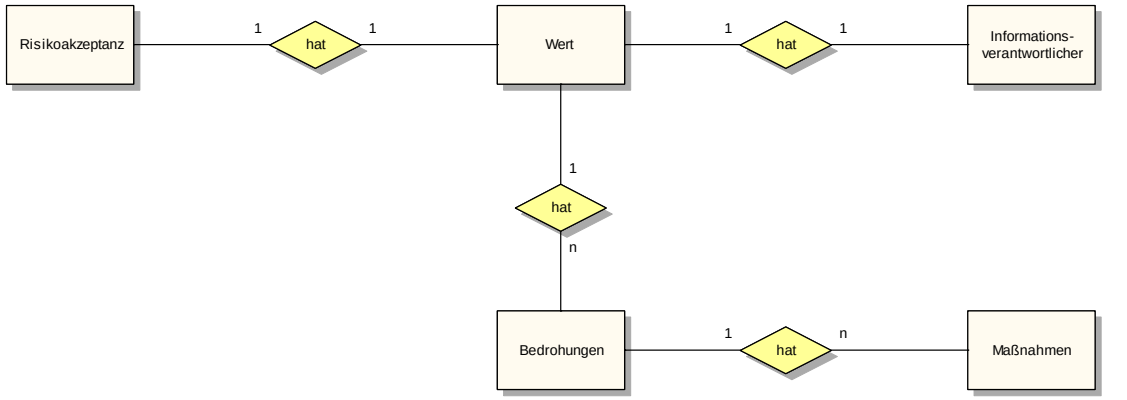


Abb. 4.35: DV-Sicht ERM: 4.2.1.f.2 Bewusste, objektive die Akzeptanz der Risiken laut Politik

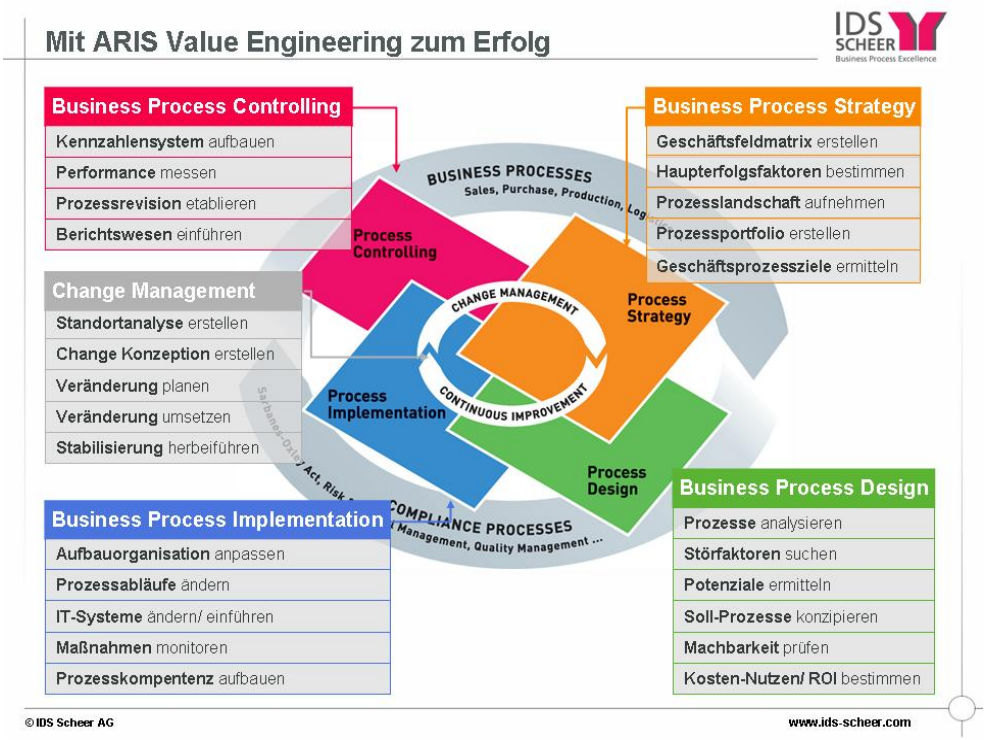
Aus dieser detaillierten Betrachtung ergibt sich nun die Möglichkeit die Struktur einer Datenbank abzuleiten, um somit diesen Bereich durch eine Software zu unterstützten. Dabei sei auf das Kapitel 5 dieser Arbeit verwiesen, welches sich diesem Thema widmet.

5 Anwendung

Im Anschluss an die Komplettierung des Referenzmodells folgt die fünfte Phase des Vorgehensmodells. Diese befasst sich mit der Anwendung des Referenzmodells. Dabei wird einerseits anhand des ARIS Value Engineering- Ansatzes der IDS Scheer AG eine mögliche Anwendung erläutert. Andererseits wird die Implementation der Risikoeinschätzung und –behandlung, welche im Rahmen dieser Arbeit mit Hilfe von Microsoft Access 2000 und Visual Basic entstanden ist, detailliert erläutert.

5.1 ARIS Value Engineering (AVE)

Ein allgemeines Modell für den Einsatz des Referenzmodells zeigt Abbildung 5.1. Hier wird der ARIS Value Engineering – Ansatz (AVE) der IDS Scheer Unternehmensberatung präsentiert, welcher auf dem vorgestellten PDCA-Konzept beruht. Dieser umfasst das Festlegen der Strategie, indem die Kernziele und -Prozesse der Organisation festgehalten werden, das Design welches die Analyse und Abbildung des IST-Zustands und die Abbildung des SOLL-Zustands der Organisation beinhaltet. Dabei wird die Abweichung zwischen diesen beiden Zuständen ermittelt, um das Verbesserungspotenzial festzustellen und die Möglichkeiten der Umsetzung festzulegen. Auf die Analyse und Abbildung folgt die Phase der Implementation, welche einerseits die Anpassung der Aufbauorganisation und Prozessabläufe sowie ggf. die Einführung neuer oder Änderung bestehender IT-Systeme beinhaltet. Die vierte Phase des Kreislaufs befasst sich mit der Erfolgskontrolle der umgesetzten Maßnahmen indem Kennzahlen gebildet werden und die Performance gemessen wird. Die Ergebnisse dieser Überprüfung lassen wiederum den Kreislauf erneut beginnen, um die kontinuierliche Verbesserung zu ermöglichen. Dabei unterstützt das Change Management diese Verbesserung durch das Planen und Umsetzen der Veränderungen. Dabei werden vor möglichen Veränderungen Standortanalysen durchgeführt und Konzeptionen der Veränderungen erstellt. Sind diese erstellt werden die Änderungen geplant, umgesetzt und eine Stabilisierung der umgesetzten Änderungen durchgeführt.



Quelle: IDS Scheer AG Hamburg 2006

Abb. 5.1: ARIS Value Engineering

ARIS Process Performance Manager

Im Rahmen des AVE-Ansatzes wird ein Werkzeug benötigt, welches die Kontroll-Phase unterstützt. Der ARIS Process Performance Manager ist ein Werkzeug zur Analyse, Bewertung und Überwachung von Organisationsprozessen. Aus IST-Prozessen generiert ARIS PPM übersichtliche Darstellungen der Leistungsdaten. Ein integriertes Frühwarnsystem überwacht dabei automatisch alle laufenden Vorgänge und alarmiert bei Abweichungen. Es bietet darüber hinaus, die Möglichkeit Abläufe optimieren zu können. Prozessrelevante IT-Daten (z.B. Auftragsnummer, Zeitstempeln) aus unterschiedlichen Quellsystemen bilden dabei die Grundlage zur Visualisierung von innerbetrieblichen Abläufen, Vorgängen und Geschäftsprozessen.

Anwendung auf das bestehende Referenzmodell

Mit Hilfe des AVE-Ansatzes lässt sich die Anwendung des Referenzmodells in einer Organisation in vier Phasen spezifizieren.

Strategie

In der Phase der Strategie wird die Organisation auf einem sehr hohen Abstraktionsgrad betrachtet. Dabei werden Geschäftfelder der Organisation analysiert und die IST-Prozesse aufgenommen. Dies geschieht im ARIS-Toolset mit Hilfe der Geschäftsfeldmatrix und WKD. Dabei werden in die Betrachtung das Referenzmodell und die Geschäftfelder bzw. die Prozesse der Organisation, welche eine hohe Relevanz für das ISMS haben, einbezogen. Das Referenzmodell bietet in dieser Phase eine Vorlage für die Herangehensweise bei der Einführung eines ISMS. Der Organisation ist es dadurch möglich sich entlang des Referenzmodells zu „hangeln“. Somit lässt sich in dieser Phase bereits feststellen, welche Bereiche stärker in die Betrachtung einbezogen werden bzw. welche Bereiche sensibel auf Sicherheitsverletzungen der Informationssicherheit reagieren. Im Ergebnis dieser Phase wird eine Strategie festgelegt, welche das weitere Vorgehen und die Betrachtung besonders relevanter Geschäfts- und Organisationsbereiche für das ISMS einbezieht.

Design

Nachdem die Strategie festgelegt wurde, wird nun auf der Prozessebene das Design durchgeführt. Dabei werden die für das ISMS relevanten Prozesse im IST-Zustand abgebildet und der SOLL-Zustand konzipiert. Dies geschieht, indem das Referenzmodell mit Prozessmodellen gefüllt wird. Es dient somit als Schablone bei der Modellierung der Prozesse. Mittel der Modellierung ist hierbei das ARIS-Toolset welches somit einen konsistenten Ablauf gewährleistet. Werden Abweichungen zwischen IST und SOLL festgestellt, werden diese dokumentiert. Diese Dokumentation dient im Anschluss an den Vergleich zur Erstellung eines Maßnahmenkatalogs welcher den Ausgangspunkt der Implementation darstellt. In diesem werden notwendige Änderungen der Aufbauorganisation, der Prozesse in der Organisation und die Einführung neuer bzw. Änderung bestehender IT-Systeme festgehalten. Dabei wird die generelle Machbarkeit dieser Maßnahmen festgestellt sowie der Vergleich von Kosten und Nutzen herangezogen.

Implementation

Nachdem die Maßnahmen unter Beachtung der Konventionen der Machbarkeit sowie Kosten und Nutzen festgelegt wurden, werden in der Phase der Implementation diese Maßnahmen umgesetzt und das ISMS implementiert.
Dabei werden notwenigen Anpassung der Aufbauorganisation, wie u. a. die Einführung der Stelle eines Informationssicherheitsverantwortlichen, sofern diese nicht existiert, durchgeführt. Ebenso wird die Ablauforganisation d.h. die Prozessabläufe ggf. geändert oder angepasst um eine Umsetzung des ISMS zu gewährleisten. Vorgaben sind hierbei die im ARIS-Toolset erstellten Prozessmodelle für den SOLL-Zustand. Dabei spielt der Einsatz von IT-Systemen in der Unterstützung des Informationssicherheits-Managementsystems eine entscheidende Rolle. Diese werden, sofern sie nicht vorhanden bzw. angepasst sind, auf die notwendigen Anforderungen des ISMS angepasst um die Umsetzung wirkungsvoll unterstützen zu können. Dazu lässt sich beispielsweise eine Software, wie sie in diesem Kapitel beschrieben wird, einsetzen um die Risikoeinschätzung und Risikobehandlung wirkungsvoll unterstützen zu können. Weithin ist die Überwachung und Dokumentation dieser Maßnahmen erforderlich um die kontinuierliche Verbesserung zu gewährleisten.

Kontrolle

Auf die Implementation folgt die Kontrolle der umgesetzten Maßnahmen. Dabei wird der Erfolg anhand von Kennzahlen, bezogen auf die Informationssicherheit in der Organisation gemessen. Mögliche Kennzahlen sind u. a. erfolgreiche und abgewehrte Einbruchsversuch auf die Server der Organisation oder Verletzung der Integrität, Verfügbarkeit oder Vertraulichkeit der Informationen in der Organisation in einem bestimmten Zeitrahmen. Anhand dieser Kennzahlen lässt sich die Wirkung (Performance) des eingeführten ISMS messen und Verbesserungspotenziale aufdecken. In diesem Bereich besteht die Möglichkeit das ARIS-Toolset einzusetzen um definierte Attribute in den Prozessmodellen mit Werten zu füllen und diese mittels der Reportfunktionalität auszuwerten. Eine Automatisierung ist hier nicht möglich sodass sich ein hoher Eingabeaufwand ergibt. Mittel der Wahl ist der vorgestellte ARIS Process Performance Manager, welcher die Möglichkeit bietet den IST-Zustand automatisch zu erfassen. Dazu

lassen sich Messpunkt definieren an welchen aus einem IT-System Daten extrahiert werden. Diese lassen sich dazu nutzen die Prozessmodelle mit Werten zu füllen und diese auszuwerten. Somit lassen sich verschiedene Arten der Auswertung realisieren. Dazu zählt u.a. die Visualisierung der IST-Prozesse, Analyse dieser Prozesse und Management-Cockpit für den Top-Level Überblick. Daraus lassen Informationen für die Verbesserung der laufenden Prozesse ermitteln und diese im Prozess der kontinuierlichen Verbesserung einbeziehen.

Ergebnis

Im Ergebnis zeigt sich ein aktives ISMS, welches durch Kontrolle und kontinuierliche Verbesserung effektiv in der Organisation im Einsatz ist. Dabei fand das Referenzmodell in allen Phasen Einsatz. Besonders in den Phasen der Strategie und Design bietet ein solches Referenzmodell den Vorteil einer anerkannten Herangehensweise, welche durch den Einsatz des ARIS-Toolsets zur Einhaltung der Konsistenz beiträgt.

5.2 Toolbasierte Unterstützung der Risikoeinschätzung und -behandlung

In diesem Abschnitt wird das zur Unterstützung der Risikoeinschätzung und -behandlung, welche im Abschnitt „4.2.1 Festlegen des ISMS“ des BS7799-2:2002 Standards beschrieben wird, entwickelte Tool in Funktionsweise und Anwendung beschrieben. Es ist als logische Konsequenz aus der detaillierten Betrachtung der Risikoeinschätzung und Risikobehandlung zu sehen. Dabei wurde die Umsetzung durch die Modellierung des DV-Konzeptes mittels ERM unterstützt. Um die Verknüpfung zwischen dem, mit Hilfe des ARIS-Toolsets erstellten Referenzmodell und dieser Software herzustellen wurde, wie bereits in Kapitel 4 beschrieben, das Referenzmodell durch externe Verknüpfungen an den Wertschöpfungsketten der Risikoeinschätzung und der Risikobehandlung hinterlegt. Darüber hinaus wurden die Reports, welche sich mit Hilfe der Software generieren lassen, ebenfalls den Wertschöpfungsketten zugeordnet und durch externe Verknüpfungen hinterlegt. Die Software bietet zudem die Möglichkeit, sowohl Daten aus dem Standard abzurufen, insbesondere Anhang A, als auch Daten zur Bewertung anzulegen und schrittweise den im BS7799-2:2002 beschriebenen Prozess

der Risikoeinschätzung und der Risikobewertung zu durchlaufen. Dabei lassen sich bereits erwähnten Reports der in den einzelnen Schritten angelegten Werte ausgeben und somit der Prozess der Risikoeinschätzung und Risikobehandlung schrittweise, wie im BS7799-2:2002-Standard gefordert, dokumentieren.

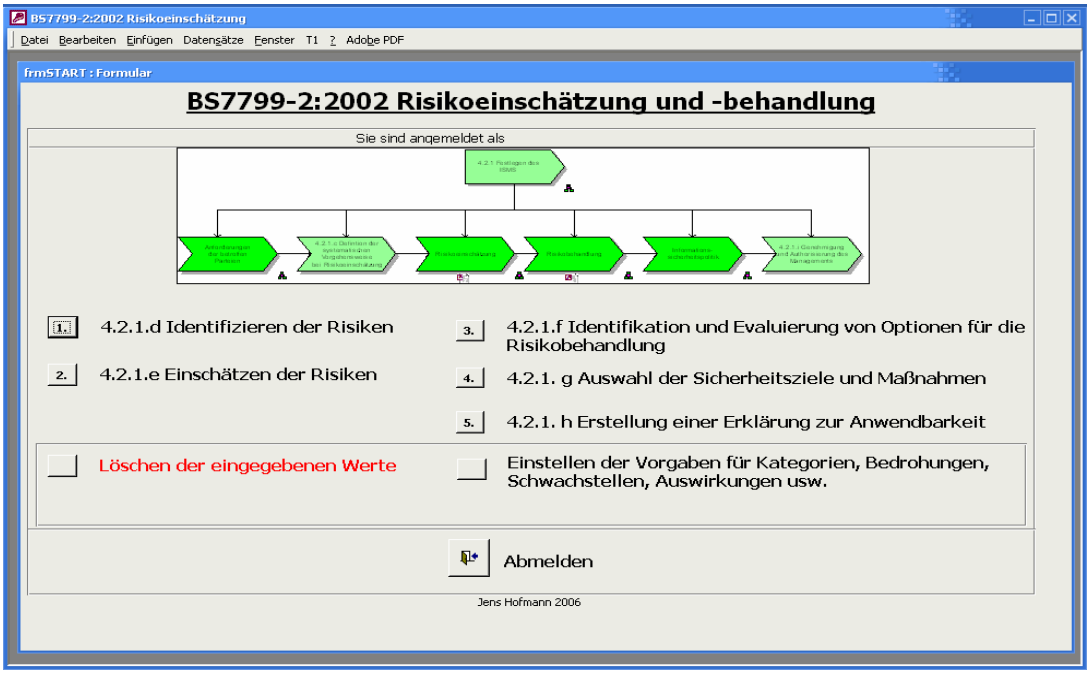


Abb. 5.2: Tool zur Risikoeinschätzung und -behandlung

Zur Erleichterung der Anwendung, im Zusammenspielt mit dem mit Hilfe des ARIS-Toolsets entworfenen Referenzmodells werden, wie in Abbildung 5.2 zu erkennen, Abbildungen der jeweiligen WKD zu den Auswahlformularen hinzugefügt. Somit ist es dem Anwender jeder Zeit möglich sowohl den entsprechenden Abschnitt im Standard als auch im Referenzmodell zu lokalisieren.

5.2.1 Konzept der Anwendung

Ausgangspunkt für die Anwendung war die Überlegung wie sich die Risikoeinschätzung und Risikobehandlung, welche im Referenzmodell detailliert abgebildet wurde, unterstützen lässt.

Erste Überlegungen

Ein erster Ansatzpunkt in Richtung der Unterstützung der Anwender war die Hinterlegung von Excel-Listen oder ähnlichen Dokumenten, welche dem Anwender Vorlagen für die Auswahl bedrohten Werte bis hin zur Risikobehandlung bieten. Die Komplexität und Übersichtlichkeit dieser Listen ist aber in diesem Zusammenhang sehr hoch. Allein entsprechende Listen von Risiken und Schwachstellen können leicht mehrere tausend Werte beinhalten. Wählt nun der Anwender die möglichen bedrohten Werte aus und führt schrittweise den Prozess der Einschätzung durch so kann er bei möglichen 100 Werten, mit jeweils fünf Bedrohungen und jeweils fünf Schwachstellen leicht eine Liste mit 2500 Schwachstellen zu den gewählten Werten erhalten. Dieses Beispiel verdeutlicht wie schnell ein Anwender hier die Übersicht verlieren kann. Ein weiterer Nachteil ist die Dokumentation welche hierbei wiederum einen hohen Arbeitsaufwand durch das Zuordnen der Listen bedeutet. Will der Anwender beispielsweise Werte einem bestimmten Verantwortlichen zuordnen, wird er wiederum in den Listen mit einer Vielzahlen von Werten und der daraus resultierenden Unüberschaubarkeit konfrontiert. Ein weiterer Grund für den Verzicht auf diese Listen liegt in der Darstellung von Beziehungen. In den ERM der Risikoeinschätzung und -behandlung werden Beziehungen eingesetzt sodass diese in der Verknüpfung der möglichen Tabellen ebenfalls abgebildet werden müssen. Dieses lässt sich aber mit Excel-Tabellen nicht realisieren.

Lösung

Durch die detaillierte Abbildung der Risikoeinschätzung und Risikobehandlung im Referenzmodell des BS7799-2:2002 Standards, ist es möglich, diesen Bereich in Software umzusetzen. Somit ist die Lösung des beschriebenen Problems ist eine Datenbankanwendung welche es dem Anwender ermöglicht, sowohl leicht über den Bestand an Daten zu navigieren als auch auf einfache Art und Weise die für ihn relevanten Daten aufzurufen und die Beziehungen darzustellen. Diese Anwendung ermöglicht es dem Anwender, in jedem Schritt der Risikoeinschätzung und Risikobehandlung eine geeignete Sicht, die ihn ausschließlich mit den, für diesen Arbeitsschritt, notwendigen Informationen versorgt, zu erhalten. Weiterhin kann diese Anwendung leicht Vorgaben für Schwachstellen, Bedrohungen und Maßnahmen in Kategorien bieten. Diese Vorgaben

lassen sich dabei erweitern und verändern. Ein weiterer wesentlicher Vorteil liegt in der Dokumentation. Die Anwendung lässt dem Nutzer die Möglichkeit jeden Schritt der Risikoeinschätzung und Risikobehandlung zu dokumentieren indem er Reports je nach Anwendungszweck aus dem Datenbestand erzeugen lassen kann. Weiterhin kann nach Eingabe der bedrohten Werte, durch die Beeinflussung der Sicht, der jeweilige Verantwortliche für die Werte, die möglichen Schwachstellen und Bedrohungen einschätzen und diese in die Datenbank einfügen.[112]

5.2.2 Weitere Softwarelösungen

Vor der Entwicklung einer solchen Anwendung werden entsprechend ähnliche Lösungen am Markt betrachtet und die Frage verfolgt, welche Möglichkeiten der Anwendung diese bieten. Durch den Einsatz im Bereich der Zertifizierung sind viele Softwarelösungen im Umlauf die den Prozess der Auditierung und Zertifizierung nach BS7799-2:2002 und ISO/IEC 17799:2000 unterstützen.
Für die studentische Arbeit bieten die Organisationen, welche diese Software einsetzen oder vertreiben, größten Teils keine Demonstrationsversion an. Dadurch sind die Informationen zu den Anwendungen sehr begrenzt und lassen ausschließlich eine Betrachtung eines grob gehaltenen Funktionsumfanges der vorgestellten Softwarelösungen zu.
Die Übersicht zeigt ausschließlich einen Teil der am Markt befindlichen Softwarelösungen lässt aber durch die genannten Gründe keinen detaillierten Vergleich der einzelnen Funktionen der Softwarelösungen zu.

1. Callio Toolkit Pro 17799

Die Firma Callio Technologies bietet eine Webanwendung (siehe Abbildung 5.3) und Server zur Unterstützung der Risikoeinschätzung, Risikomanagement, Vorlagen zur Implementation, Generator für Sicherheitspolitiken, Auditvorbereitung und Dokumentenverwaltung an. Dabei orientiert sich die Software an den ISO17799 und BS7799-2

[112] Vgl. Brosius (1999), S. 167 - 175

Standards und unterstützt dabei die Umsetzung sowie Diagnose des gegenwärtigen Sicherheitsstandards und zur Vorbereitung auf ein BS7799-Audit.[113]

Quelle: Callio Technologies (2006)

Abb. 5.3: Callio Toolkit Pro Startbildschirm

2. Informationssicherheitsmanagement / ISO 17799

Das von der Firma Northwest Controlling Corporation Ltd. angeboteten Anwendungspaket bietet drei Softwarelösungen zum ISO 17799 und BS7799 Standard an. Dabei werden Audit, Risikoanalyse (siehe Abbildung 5.4), Risikobehandlung und Überprüfung der Informationssicherheit durch Vorgabe von Prüflisten sowie das Verwalten eines ISMS unterstützt.

Auditierung

Die Software verwaltet Auditpläne, unterstützt die Checklistenvorbereitung und Bearbeitung, ermöglicht die Aufnahme von Maßnahmen und umfasst Berichte.

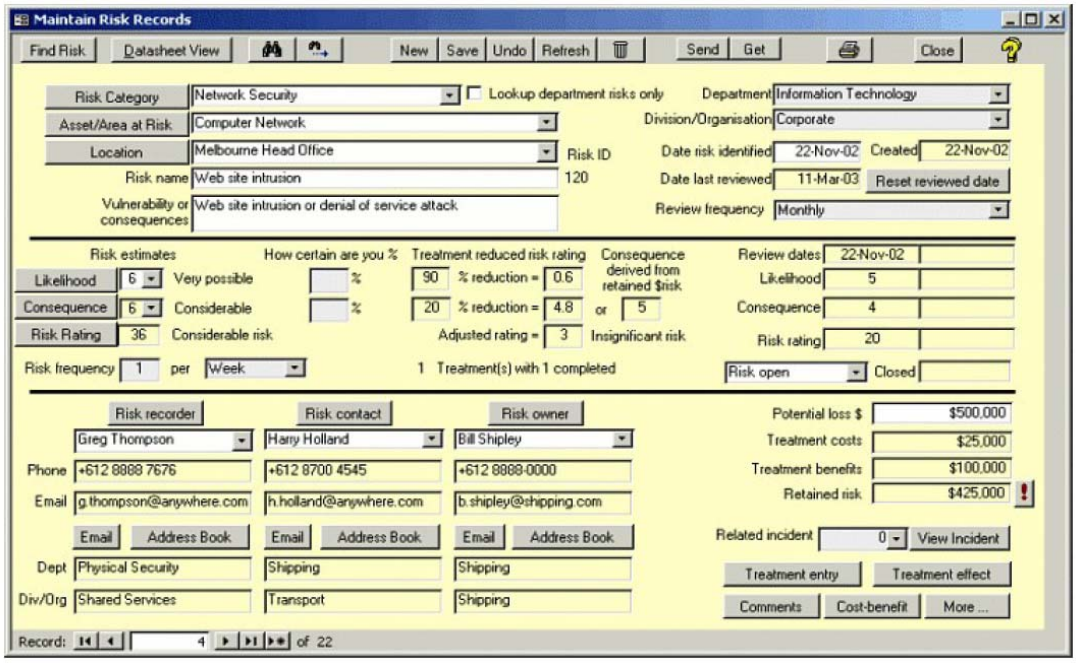
Risikoanalyse und -behandlung

Die Komponente ermöglicht die Risikobewertung, Maßnahmen auszuwählen sowie das Erstellen von Risikoberichten.

[113] Callio Technologies (2006)

Management der Informationssicherheit

Hiermit lassen sich die Prozesse eines ISMS planen, steuern und kontrollieren sowie Dokumente verwalten.[114]



Quelle: Northwest Controlling Corporation Ltd. (2006)

Abb. 5.4: Risikobewertung mit Risk Register

3. Secuquest

Mit SecuQuest lassen sich Stärken und anfälliger Problemgebiete im Bereich Security Management darstellen.

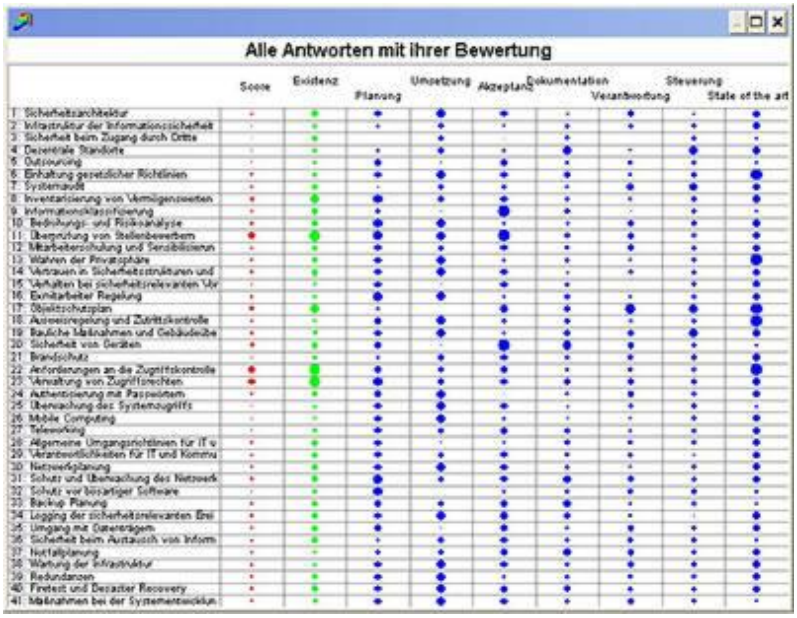
Die Software (siehe Abbildung 5.5) orientiert sich diesbezüglich an den gängigen Standards:

- ISO 17799 bzw. BS 7799
- Grundschutzhandbuch (Deutschland)
- IT-Sicherheitshandbuch (Österreich)

Dazu wird die Möglichkeit der Aufnahme und Auswertung sicherheitsrelevanter Merkmale der Organisation und deren Auswertung ermöglicht. SecuQuest stellt dabei eine

[114] Northwest Controlling Corporation Ltd. (2006)

Vorgehensmethode die sich an dem ISO TR 15504 Standard orientiert sowie die Softwareunterstützung dieser Methode dar.[115]



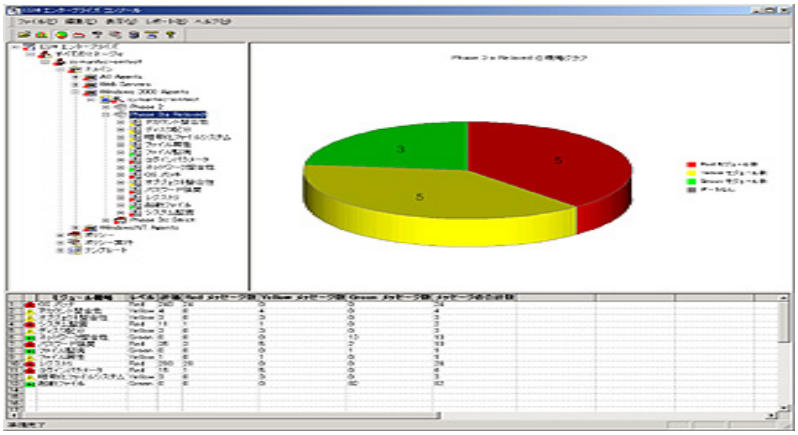
Quelle: MPS consult Unternehmensberatung GmbH (2006)

Abb. 5.5: Secuquest Auswertung

4. Symantec Enterprise Security Manager

Symatec bietet mit dem Symantec Enterprise Security Manager (siehe Abbildung 5.6) Vorlagen für die wichtigsten Sicherheitsrichtlinien, Sicherheitsprüfungen, Maßnahmen zur Risikobehandlung, identifizieren von Schwachstellen sowie Reports für Manager. Die hierzu notwendigen Daten lassen sich mit diesem Tool aus einer Vielzahl von Informationsquellen automatisch abrufen. Hierzu zählen u. a. die Symantec Firewall und Virenscanner-Produkte. Dabei wird u. a. der ISO 17799 Standard zur Umsetzung von Sicherheitsrichtlinien eingesetzt.

[115] MPS consult Unternehmensberatung GmbH (2006)



Quelle: Symantec (2006)

Abb. 5.6: Symantec Enterprise Security Manager

Die Software ist wird dabei ausschließlich für den Einsatz in Großunternehmen angeboten.[116]

Ergebnis

Keine der betrachteten Softwarelösung orientiert sich direkt am Ablauf der Risikoeinschätzung und -behandlung gemäß BS7799-2:2002, wie sie im Referenzmodell vorgestellt wurde. Dies bietet die Möglichkeit eine eigene Softwarelösung zu entwickeln, welche das Referenzmodell des BS7799-2:2002 in diesem Bereich unterstützt.

5.2.3 Die Anwendung

Grundlage der Anwendung zur Unterstützung der Risikoeinschätzung und -behandlung ist ein komplexes Datenbankschema, welches es ermöglicht die Beziehungen der Risikoabschätzung und der Risikobehandlung geeignet abzubilden.

[116] Symantec (2006)

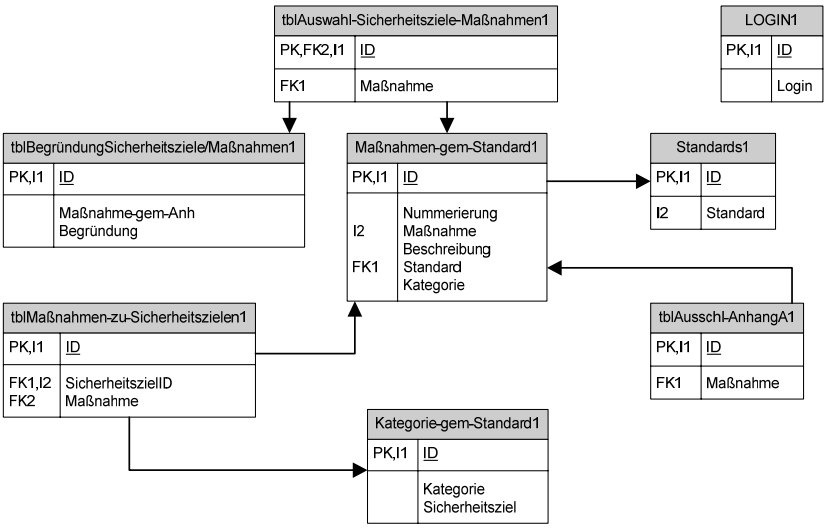


Abb. 5.7: Datenbankstruktur: Auswahl der Sicherheitsziele und Maßnahmen

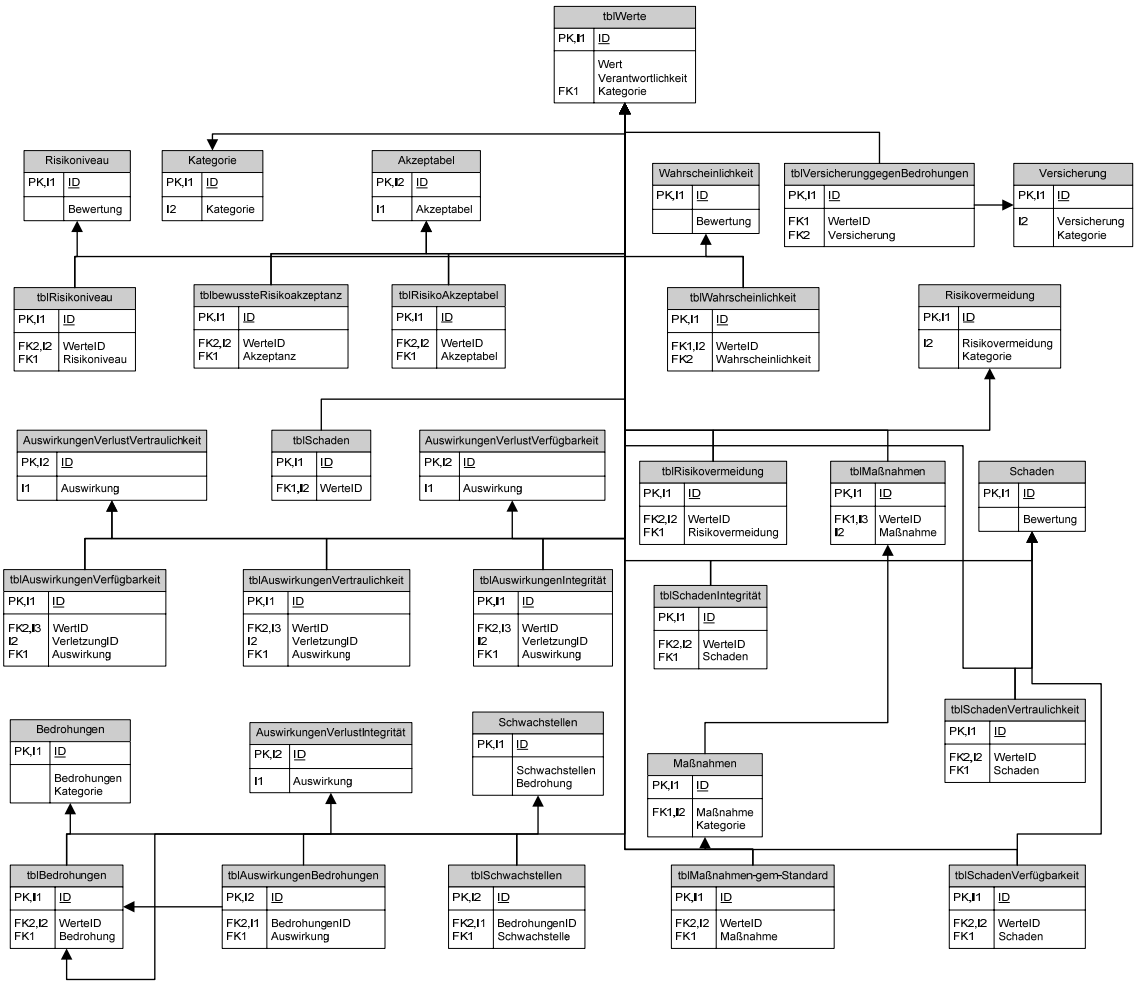


Abb. 5.8: Übersicht Datenbankstruktur: Risikoeinschätzung und –Behandlung

Durch die detaillierte Betrachtung dieses Bereichs in dem vorgestellten Referenzmodell lässt sich die Datenbank aus den dort gezeigten ERM ableiten. In Abbildung 5.7 und 5.8 sind die dazu notwendigen Tabellen und deren Beziehungen, welche abgeleitet werden konnten, im relationalen Datenmodell dargestellt. Während in Abbildung 5.7 die Tabellen der Sicherheitspolitik und der generische Maßnahmen (im BS7799-2:2002 Standard 4.2.1g und h) dargestellt sind, sind in Abbildung 5.8 die komplexen Beziehungen der Risikoeinschätzung und -behandlung zu erkennen. Ausgehend von der Tabelle der identifizierten Werte sind dabei Bedrohungen, Schwachstellen, Maßnahmen und deren Einschätzungen in Beziehung gesetzt.
Der direkte Vergleich des bereits in Kapitel 4.3.5 vorgestellten ERM „Bewusste, objektive Akzeptanz der Risiken laut Politik“ (siehe Abbildung 5.9) und des relationalen Datenmodells des gleichen Bereichs in der Access-Datenbank in Abbildung 5.10 zeigt wie die im Referenzmodell entworfenen Beziehungen umgesetzt werden konnten.
Dabei wurde der Informationsverantwortliche in die Tabelle Werte eingefügt. Die Tabelle Bedrohungen beinhaltet die Verknüpfung mit den Werten über den Fremdschlüssel (FK) WerteID und die Bedrohungen. Die Maßnahmen, welche wiederum den Bedrohungen zugeordnet sind beinhalten Maßnahmen und den FK BedrohungenID welcher diese mit den Bedrohungen verknüpft.

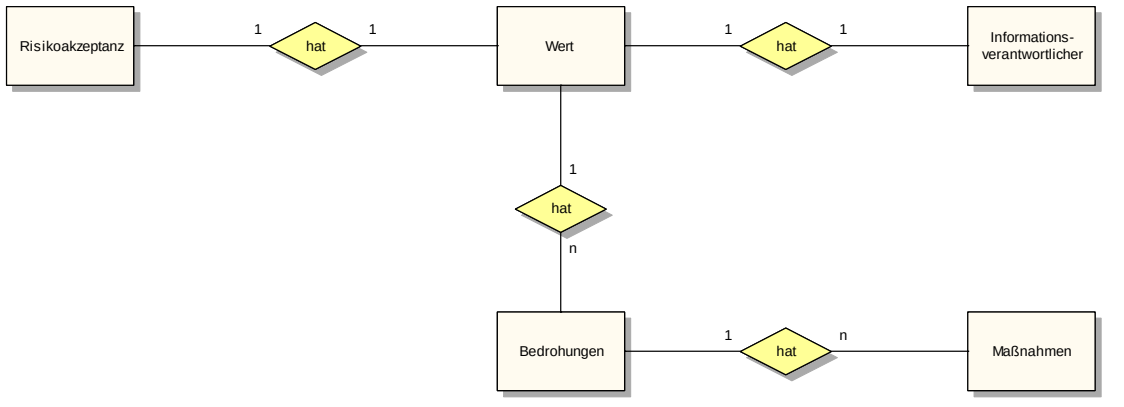


Abb. 5.9: ERM: Bewusste, objektive Akzeptanz der Risiken laut Politik

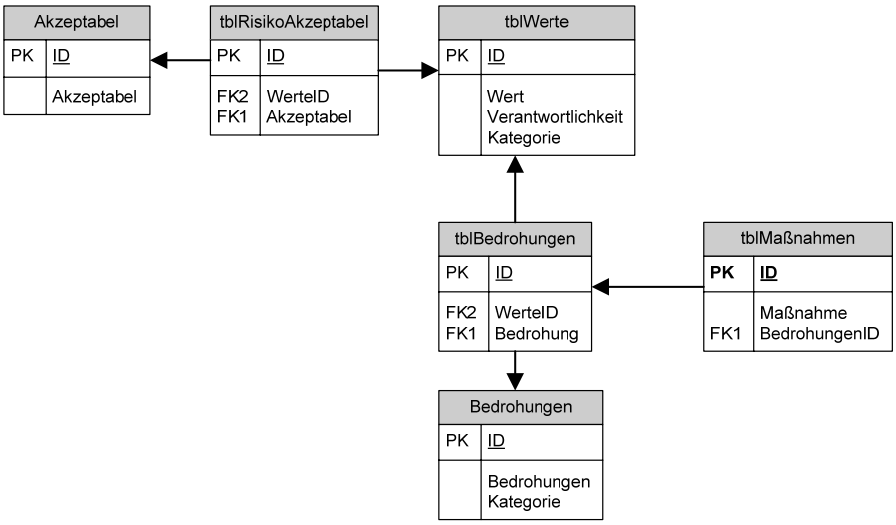


Abb. 5.10: Datenbankstruktur: Bewusste, objektive Akzeptanz der Risiken laut Politik

Die Tabelle RisikoAkzeptabel verknüpft wiederum die Werte mit der Entscheidung über ein akzeptables Risiko. Dazu wird die WerteID über eine Fremdschlüsselbeziehung mit der ID des Wertes verknüpft.
Dieser Ausschnitt aus der Datenbankstruktur zeigt somit, wie die ERM des DV-Konzeptes in der Access Datenbank umgesetzt werden konnte.

Einstieg in die Anwendung

Einstiegspunkt in die Anwendung ist das Login-Formular (siehe Abbildung 5.11). Es bietet die Möglichkeit die Sicht des Verantwortlichen für die Information auf die gewählten Werte zu beeinflussen. So kann beispielsweise der Administrator als zuständiger für die Server Bedrohungen und Schwachstellen der ihm unterstellten Systeme einschätzen. Es besteht zusätzlich zur Auswahl der einzelnen Verantwortlichen die Möglichkeit, alle Werte zu bearbeiten. Dies ist notwendig um alle Werte in der Organisation zu identifizieren und die Verantwortlichen herauszustellen. Die so benannten Verantwortlichen werden durch Abfragen aus der Datenbank ermittelt und dem Login-Formular zur Verfügung gestellt

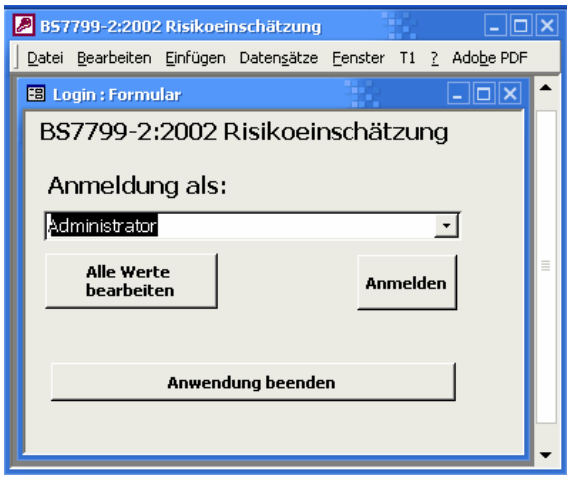


Abb. 5.11: Login-Formular

Auf den Einstieg in die Anwendung folgt die Risikoeinschätzung und Risikobehandlung wie sie in Abbildung 5.12 dargestellt ist. Dabei enthalten Identifizieren und Einschätzen der Risiken sowie die Auswahl der Sicherheitsziele und Maßnahmen gemäß Anhang weitere Unterschritte, die im Folgenden herausgestellt werde.

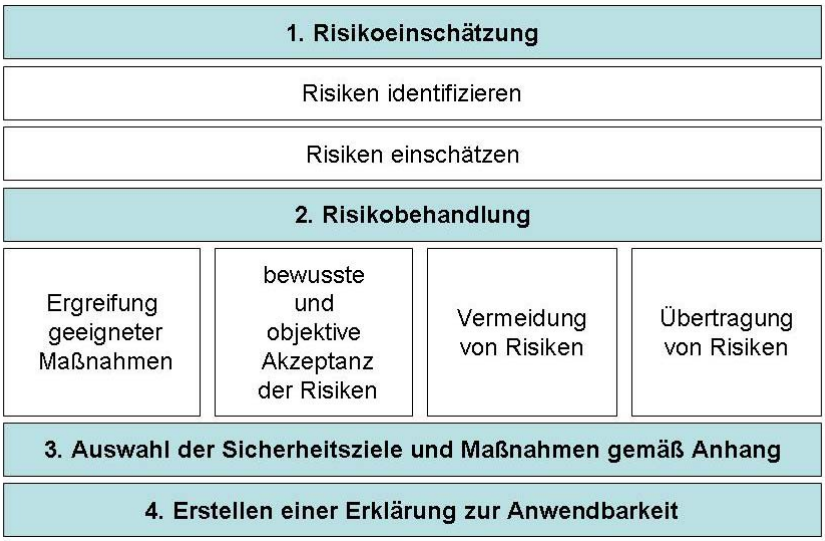


Abb. 5.12: Risikoeinschätzung und -behandlung

Risikoidentifikation

Hat sich der entsprechende Verantwortliche angemeldet, lassen sind in der Risikoeinschätzung die identifizierten Werte (siehe Abbildung 5.13) anzeigen.
In den folgenden Schritten gibt dieser die möglichen Bedrohungen und Schwachstellen an. Dabei lassen sich jedem identifizierten Wert theoretische unendlich viele Bedrohun-

gen und jeder dieser Bedrohungen zu einem Wert unendlich viele Schwachstellen zuordnen. Vorgaben dieser Werte lassen sich ausschließlich aus den entsprechenden Tabellen entnehmen. Dabei werden die Werte und ihre Kategorien angezeigt.

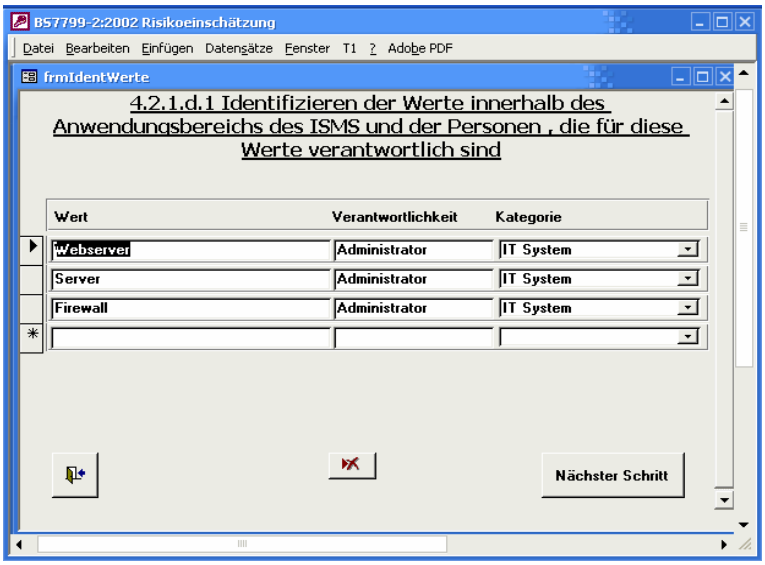


Abb. 5.13: Identifizieren der Risiken

Ist dieser Schritt abgeschlossen, werden gemäß Standard Punkt 4.2.1.d.4 die Auswirkungen des Verlustes der Integrität, Verfügbarkeit und Vertraulichkeit eingegeben. Wie bereits beschrieben, ist auch in der Abbildung 5.14 zu erkennen, dass der dem Standard entsprechende Punkt in den Eingabeformularen jeweils erscheint, um dem Nutzer die Führung durch den Standard zu erleichtern.

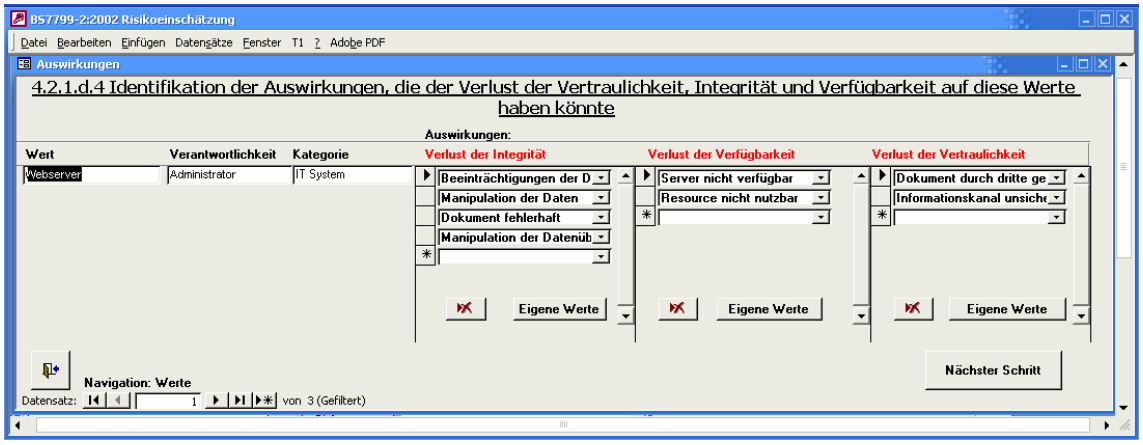


Abb. 5.14: Formular zur Eingabe der Auswirkungen

Mit der Identifizierung der Auswirkungen ist die Identifizierung der Risiken in der Anwendung abgeschlossen. Dem Anwender bleibt nun die Möglichkeit alle identifizierten Werte mit ihren Bedrohungen, Schwachstellen und den für die Informationssicherheit wichtigen Auswirken in einem Report ausgeben zu lassen. Diese entspricht der geforderten Dokumentation welche im Standard unter Punkt 4.3 zu finden ist.

Risikobewertung

Nachdem die Identifizierung abgeschlossen ist, folgt die notwendige Einschätzung der Risiken. Dabei wird gemäß Standard der mögliche Schaden für das Geschäft bei Verlust der Integrität, Verfügbarkeit und Vertraulichkeit eingeschätzt, die Eintrittswahrscheinlichkeit für jede einzelne Bedrohung bewertet, das Risikoniveau für jeden Wert festgelegt und bewertet ob das Risiko akzeptabel für die Organisation ist.

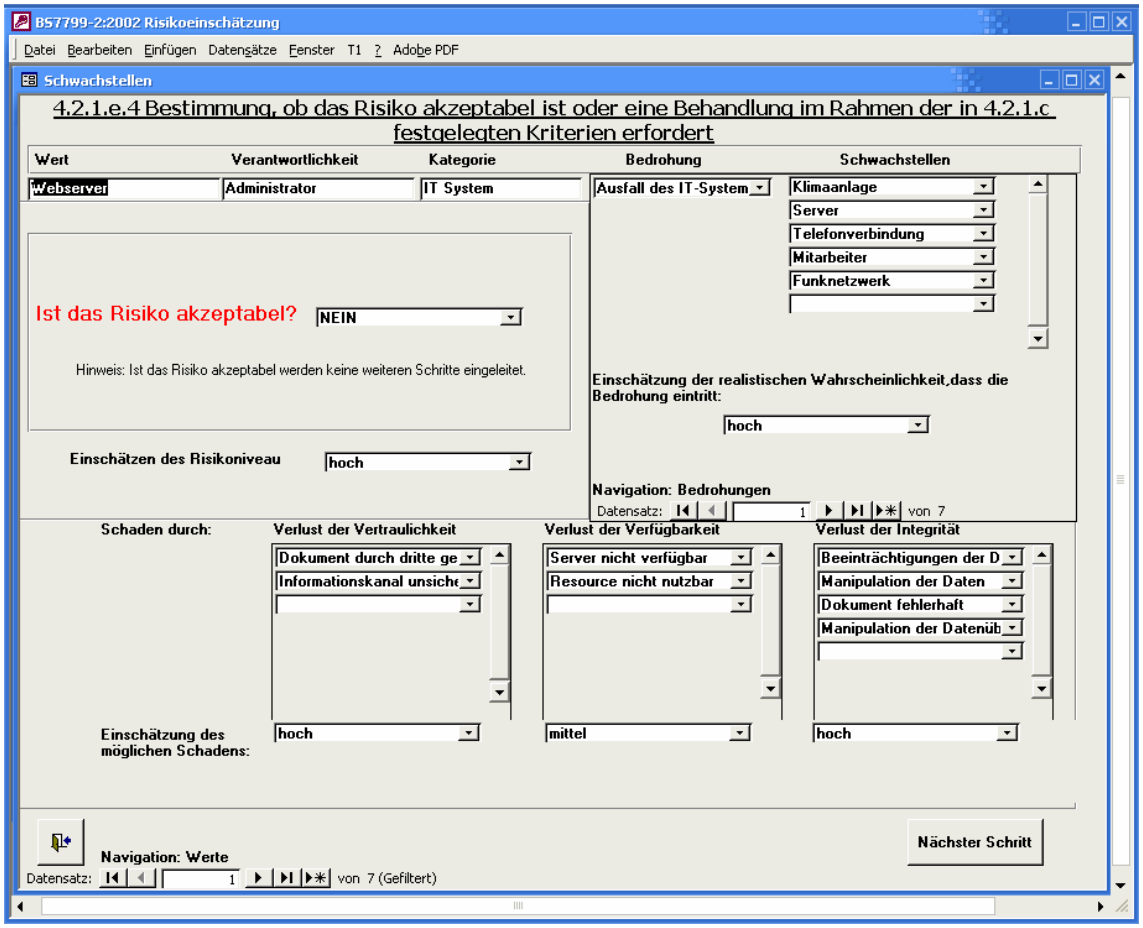


Abb. 5.15: Formular Übersicht an Informationen zur Festlegung der Risikoakzeptanz

Wird das Risiko für den einzelnen Wert dabei akzeptiert, so entfällt ein weiteres Vorgehen, wird es aber nicht akzeptiert, wie in Abbildung 5.15 zu erkennen, so schließt sich

die Risikobehandlung an. Dieses Vorgehen entspricht wiederum dem Standard in den Punkten 4.2.1.e.1 bis 4.

Risikobehandlung

Wie im vorherigen Abschnitt beschrieben, werden für die weitere Behandlung ausschließlich Werte angezeigt, deren Risiko für die Organisation nicht akzeptabel ist. Daraus folgen die Notwendigkeit von Maßnahmen zur Behandlung der festgestellten Bedrohungen, Schwachstellen sowie die Einführung von Maßnahmen zur Prävention der Risiken. Dem Management bleiben in diesem Fall vier Möglichkeiten die sich einzeln ausführen oder kombinieren lassen.

- 4.2.1.f.1 Ergreifung geeigneter Maßnahmen
- 4.2.1.f.2 bewusste und objektive Akzeptanz der Risiken, sofern sie eindeutig der Politik der Organisation und den Kriterien der Risikoakzeptanz genügen, welche durch das Management festzulegen sind
- 4.2.1.f.3 Vermeiden von Risiken
- 4.2.1.f.4 Übertragen der entsprechenden Geschäftsrisiken auf andere Parteien wie Versicherung, Lieferanten oder andere

So ist eine denkbare Entscheidung, dass das Management Maßnahmen ergreift und bewusst das weitere Risiko akzeptiert. In Abbildung 5.16 ist diese Variante dargestellt. Es wurden sowohl eigene Maßnahmen als auch Maßnahmen aus dem Anhang A des Standards gewählt. Dies führt wiederum zu einer Akzeptanz des verbleibenden Risikos. Eine weitere Variante ist die Entscheidung, eigene Maßnahmen zu ergreifen und zusätzlich einen Teil des Risikos an Versicherungen abzugeben. Dies würde wiederum zur bewussten Akzeptanz des Restrisikos führen. In einer dritten Variante würde das Management die Risiken durch bestimmte Maßnahmen vermeiden und das Restrisiko bewusst akzeptieren.

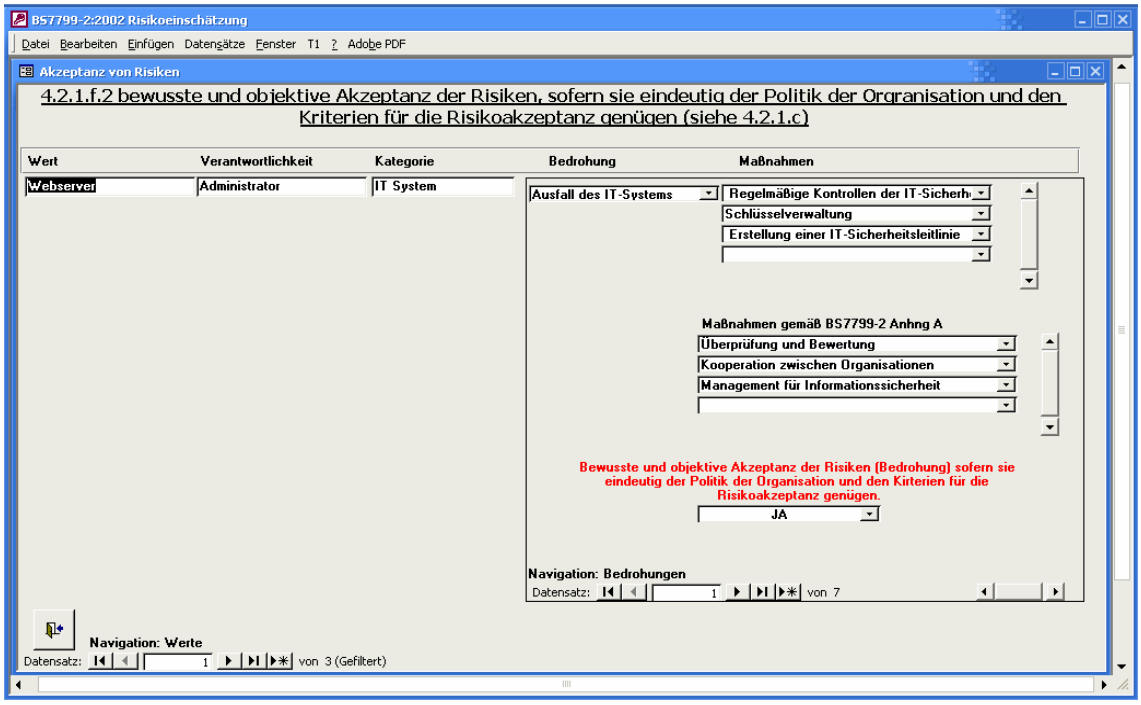


Abb. 5.16: Formular zur bewussten Akzeptanz der Risiken

Zu den drei aufgeführten Varianten sind weitere möglich. Dabei ist es dem Anwender der Software grundsätzlich möglich, zwischen den vorgegebenen Werten und eigenen Werte zu entscheiden, die er selbst hinzufügt.
Abschließend zur Risikobehandlung lässt sich wiederum ein Report, der die Werte, ihre Bedrohungen, Schwachstellen und der Behandlung ausgibt, erstellen.

Sicherheitsziele und Maßnahmen

Als weitere Funktion zur Risikoeinschätzung und Risikobehandlung lassen sich die Sicherheitsziele der Organisation und Maßnahmen gemäß Anhang A des Standards festlegen. Im Standard erfolgt die Beschreibung in Punkt 4.2.1.g und 4.2.1.h (siehe Abbildung 5.17). Die Software bietet hierbei die Sicherheitsziele gemäß Standard und die hierzu gegebenen Maßnahmen wiederum gemäß Standard zu wählen. Dabei sind die Sicherheitsziele und Maßnahmen, welche gewählt werden können, in der Datenbank hinterlegt. Dem Anwender obliegt es diese aus einer Liste auszuwählen. Der Auswahl folgt die Begründung der gewählten Sicherheitsziele und Maßnahmen, wie in Abbildung 5.17 zu erkennen. Diese ist wiederum laut Standard Punkt 4.2.1.h gefordert.

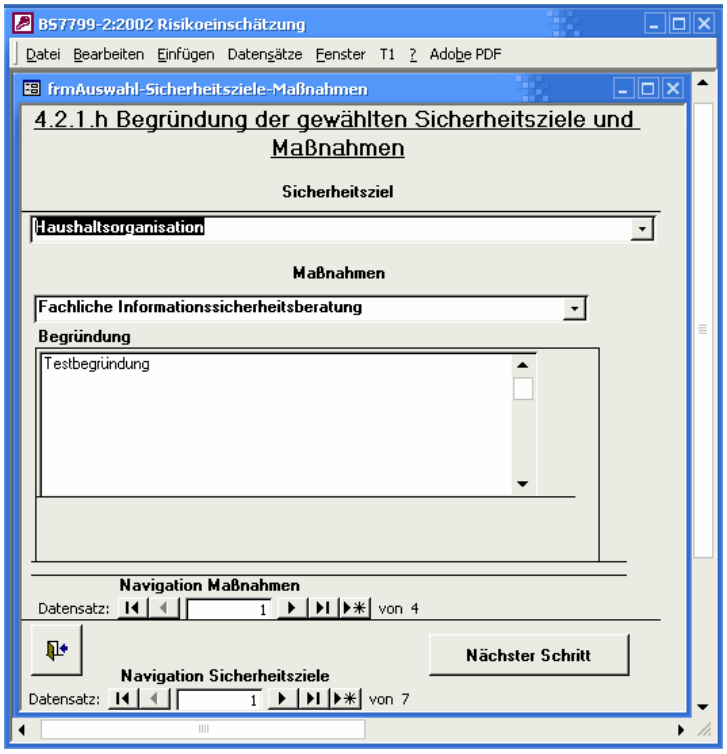


Abb. 5.17: Begründung der Sicherheitsziele und Maßnahmen

In einem weiteren Schritt werden dem Anwender alle nicht gewählten Sicherheitsziele und Maßnahmen angezeigt um diese zu dokumentieren.

Verwaltung der Vorgaben

Wie bereits in den vorherigen Abschnitten mehrfach erwähnt, lassen sich alle Vorgaben bearbeiten, anfügen oder löschen. Dazu bietet die Anwendung einerseits eine Übersicht der möglichen Vorgaben (siehe Abbildung 5.18) welche es dem Anwender erlaubt die gewünschten Änderungen vorzunehmen. Andererseits lassen sich in allen Formularen die wählbaren Vorgaben direkt bearbeiten.

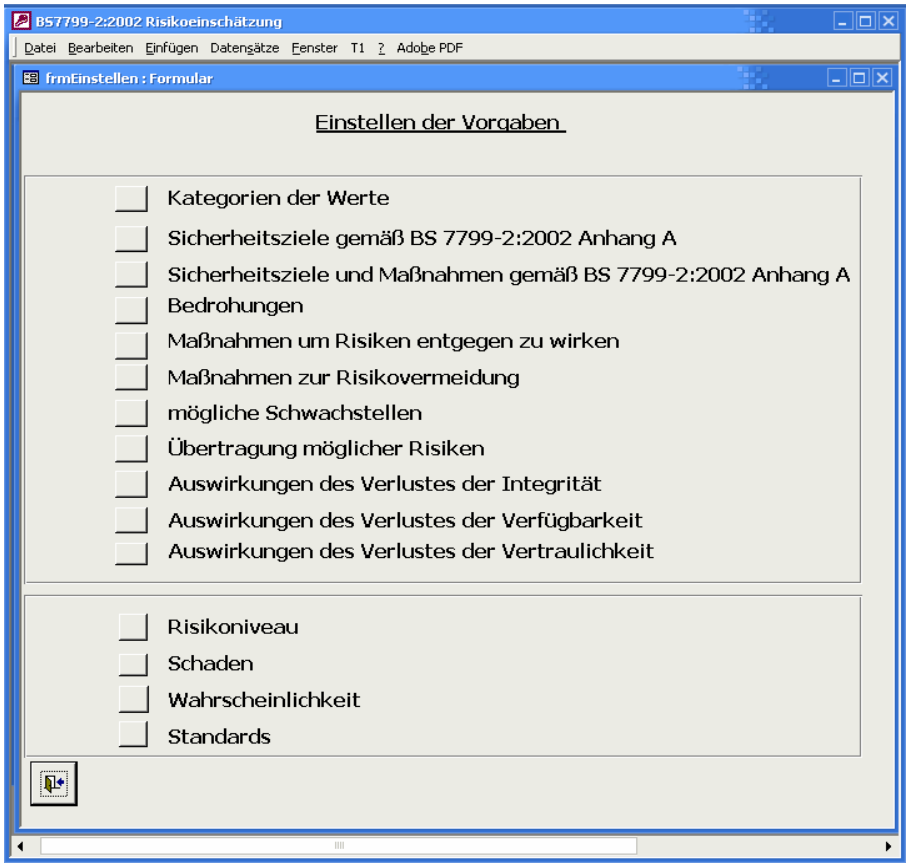


Abb. 5.18: Einstellen der Vorgaben

Weiterhin lassen sich in der Anwendung alle identifizierten Werte durch einen einfachen Dialog aus der Datenbank löschen. Von dieser Aktion bleiben alle Vorgaben unbeeinflusst.

5.2.4 Möglichkeiten der Erweiterung

Nachdem die Anwendung detailliert in den vielfältigen Möglichkeiten und Funktionen beschrieben wurde, bleiben aber auch mögliche Erweiterungen, welche in diesem Abschnitt benannt werden sollen. Angesichts der Kürze der Bearbeitungszeit sind einige dieser Funktionen als Wünschfunktionen offen geblieben. Sie können bei einer Erweiterung der Software leicht integriert werden. Sowohl die Struktur der Datenbank als auch die grafische Oberfläche lassen dies zu.

ISMS Audit

Eine denkbare Möglichkeit der Erweiterung ist die Unterstützung der ISMS-Audits. Dabei ließe sich der Auditierungsprozess durch die Vorgabe von Auditfragebögen sowie die Möglichkeit diese selbst zu erstellen, unterstützen. Darüber hinaus wäre in diesem Zusammenhang die Möglichkeit des Ausfüllens und der Auswertung durch Reports eine wünschenswerte Funktion.

Offizielle Dokumentation

Zurzeit bietet die Software die Möglichkeit Reports zur Risikoeinschätzung und –behandlung zu erstellen, welche jedoch nicht als offizielle Dokumentationen dienen können. In diesem Zusammenhang wäre die Ausgabe von Reports, welche die Spezifikation einer offizielle Dokumentation erfüllen, wünschenswert.

Priorität der Risiken

Bei der Risikoeinschätzung lassen sich u. a. Eintrittswahrscheinlichkeiten für Bedrohungen festlegen. Hier wäre die Möglichkeit quantitative Aussagen, wie beispielsweise die Priorität von Risiken, treffen zu können.

Überwachung beschlossener Maßnahmen

Ähnlich wie es das ARIS-PPM bietet wäre eine Unterstützung der Überwachung beschlossener Maßnahmen denkbar. Dabei könnten die Überwachung Werte liefern, die den Prozess der kontinuierlichen Verbesserung unterstützen.

Vorschläge für Maßnahmen

Zur Unterstützung der Risikobehandlung wäre eine System, welches Maßnahmen bei bestimmten Gütern zur Behandlung der Risiken vorschlagen könnte, wünschenswert.

6 Zusammenfassung und Ausblick

In der vorliegend Diplomarbeit wurde anhand eines fünfphasigen Vorgehensmodells die Erstellung des Referenzmodells zum BS7799-2:2002 Standard für Informationssicherheits-Managementsysteme erläutert und umgesetzt. Unterstützt wurde die Modellierung dabei durch das ARIS-Toolset zur Prozessmodellierung. Die ARIS-Architektur bot dabei die notwendige Unterstützung um eine konsistente Modellierung zu erreichen. Eingegrenzt wurden die umfangreichen Möglichkeiten des ARIS-Toolsets durch die Konventionen der Modellierung, welche detailliert die Anwendung u. a. der Modelltypen und Symbole festlegten. Kern der Modellierung war dabei der Bereich der Risikoeinschätzung und –behandlung, welcher besonders detailliert beleuchtet wurde. Diese Betrachtung ermöglichte es im Anschluss an die Modellierung den Bereich der Risikoeinschätzung und –behandlung in einer eigens zu diesem Zweck entwickelten Software abzubilden und somit die Anwendung des Referenzmodells gezielt unterstützen zu können. Neben dieser Umsetzung wurde der ARIS-Value-Engineering-Ansatz der IDS Scheer AG vorgestellt, welcher im Zusammenhang mit dem Referenzmodell einen möglichen Einsatz erläutert und die Integration der entwickelten Software ermöglicht.

Im Ergebnis zeigt sich der Nutzen der Referenzmodellierung. Dabei stellt sich der Bereich des Informationssicherheitsmanagements als bedeutend und in Zukunft stärker denn je gefragt heraus. Somit kann ein solches Referenzmodell als Schablone für eine organisationsweite Einführung eines Informationssicherheits-Managementsystems nach BS7799-2:2002 dienen. Dabei kann diese Einführung und der Betrieb durch Softwarelösungen, wie die hier vorgestellte, und deren Weiterentwicklung entscheidend unterstützt werden.

7 Anhang

Im Anhang dieser Arbeit werden alle Modelle aus der ARIS-Datenbank „ISMSRef“ zum Referenzmodell des BS7799-2:2002 Standards dargestellt.

Die Modelle werden nach folgendem Schema beschriftet.
Oberhalb der Abbildungen befinden sich die Bezeichnung des Diagrammtyps getrennt durch einen Doppelpunkt von der Modellbezeichnung. Darunter findet sich der Pfad der Gruppenstruktur des Referenzmodells im ARIS-Explorer, in welchen sich das jeweilige Modell einordnet. Pfade der Gruppenstruktur, die keine Modelle enthalten werden ebenfalls aufgeführt.

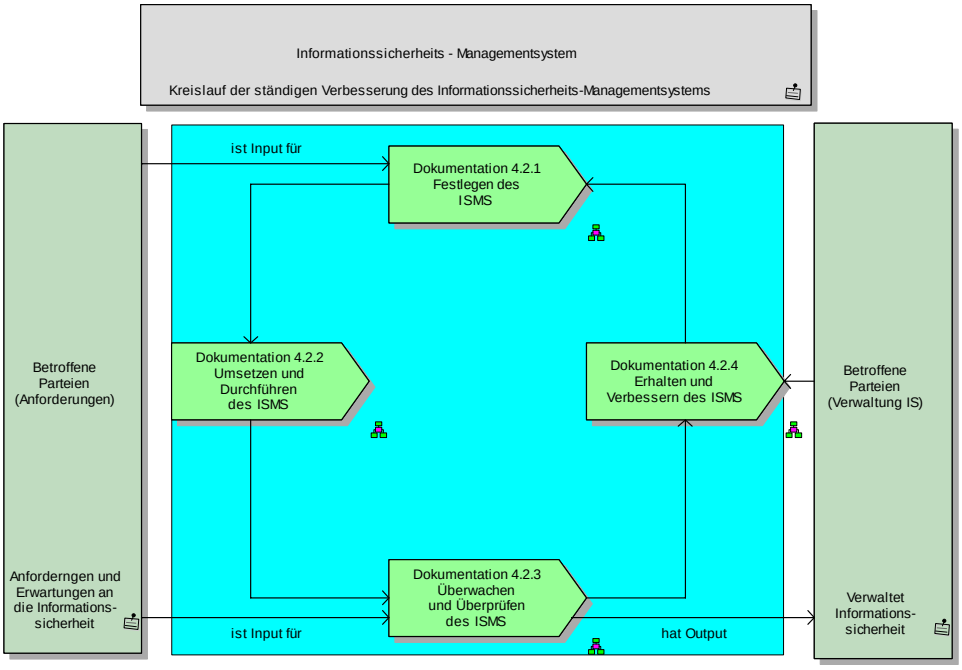
Modelle der ARIS-Datenbank „ISMSRef“

Gruppenpfadverzeichnis des ISMS-Referenzmodells

Referenzmodell

Wertschöpfungskettendiagramm: 0.2 BS 7799-2:2002

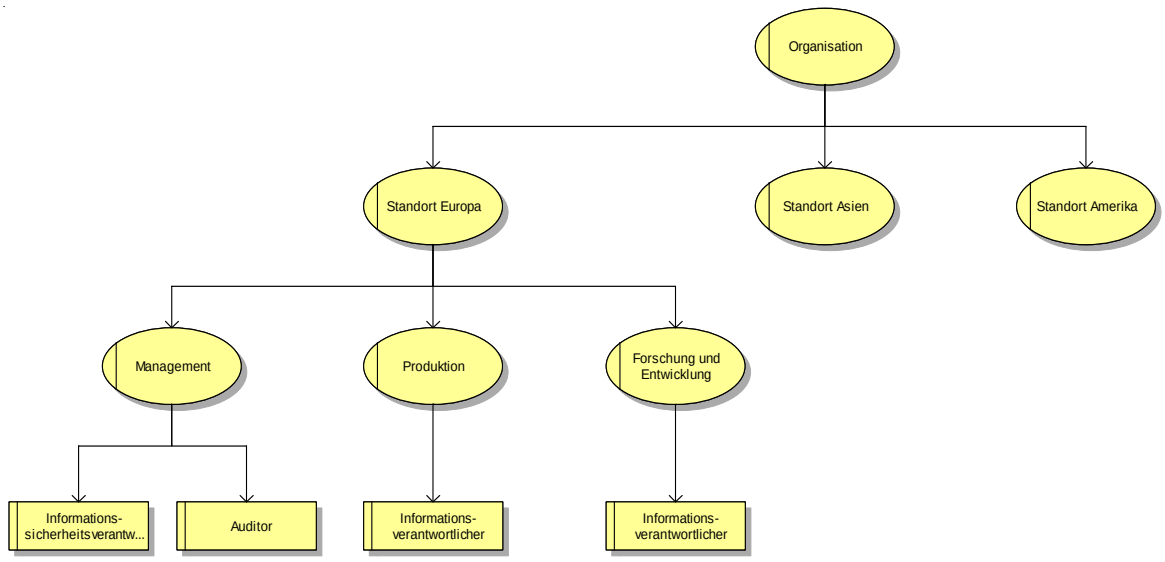
Gruppenpfad:\\Referenzmodell



0 Ebenenübergreifende Modelle

Organigramm: Organisation

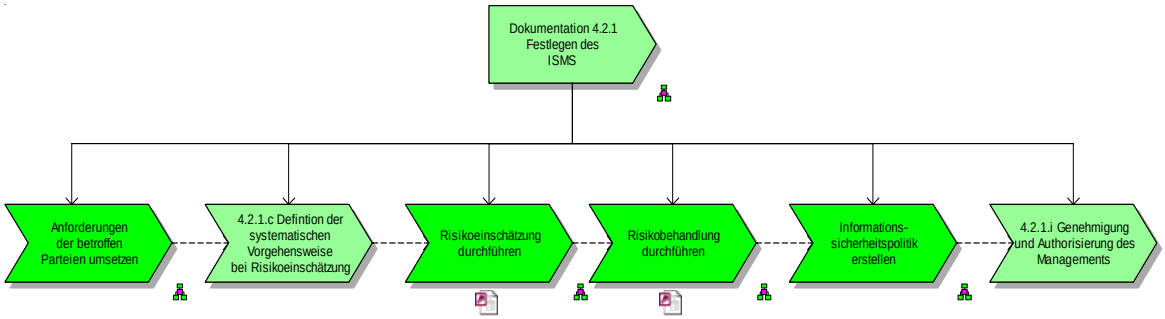
Gruppenpfad:\\Referenzmodell\0 Ebenenübergreifende Modelle



4.2.1 Festlegen des ISMS

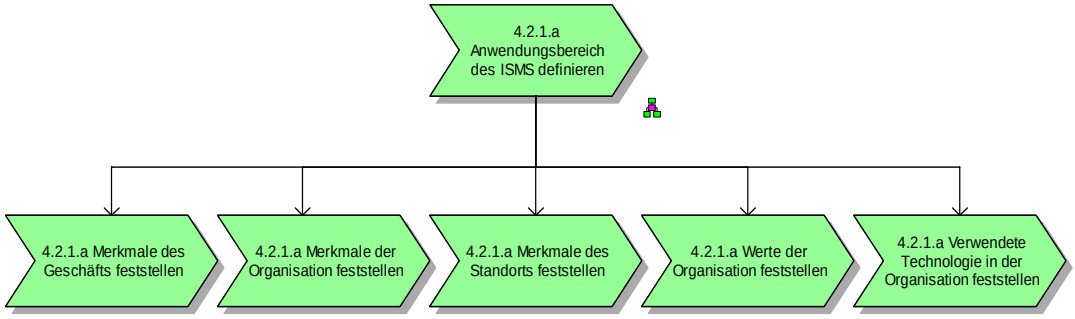
Wertschöpfungskettendiagramm: 4.2.1 Festlegen des ISMS

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS



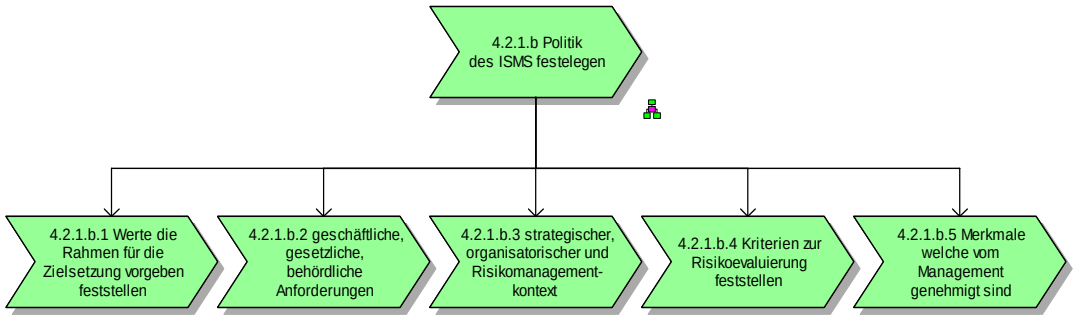
Wertschöpfungskettendiagramm: 4.2.1.a Anwendungsbereich des ISMS definieren

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Managementsicht



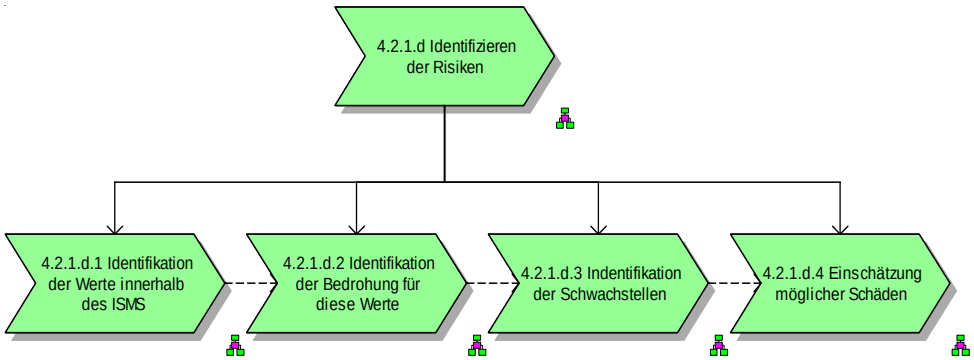
Wertschöpfungskettendiagramm: 4.2.1.b Politik des ISMS festelegen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Managementsicht



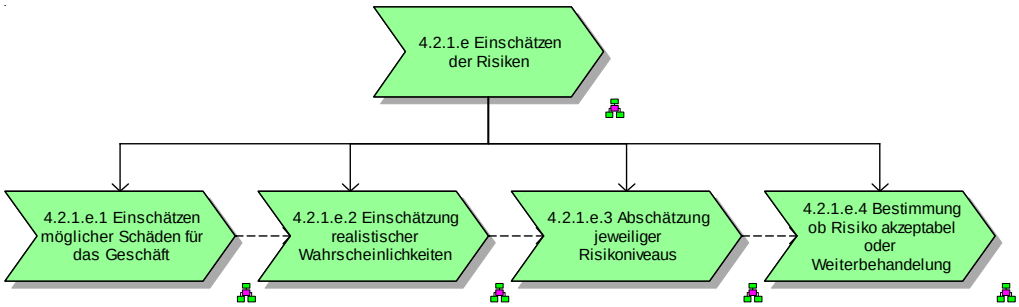
Wertschöpfungskettendiagramm: 4.2.1.d Identifizieren der Risiken

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Managementsicht



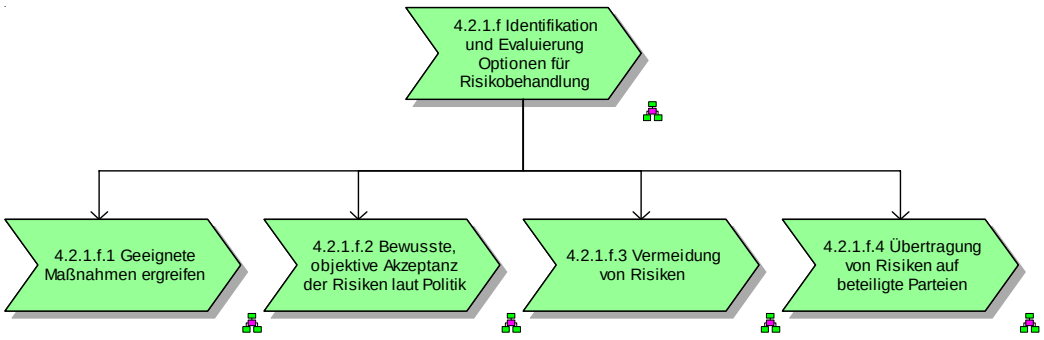
Wertschöpfungskettendiagramm: 4.2.1.e Einschätzen der Risiken

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Managementsicht

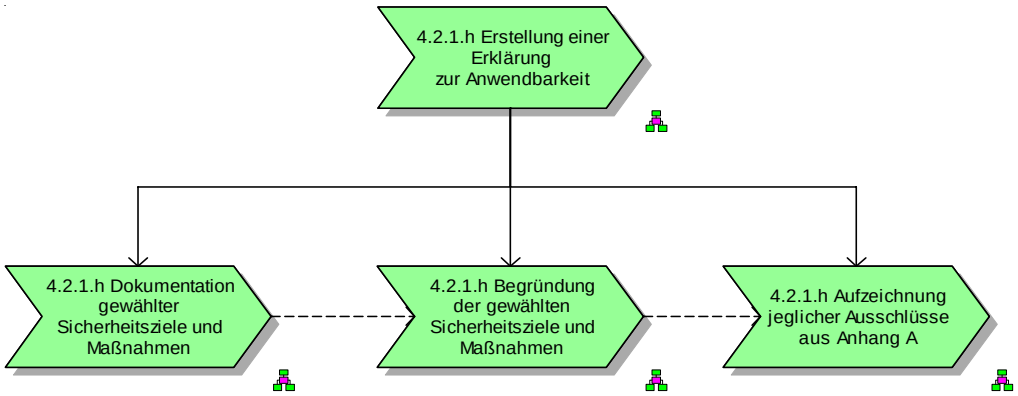


Wertschöpfungskettendiagramm: 4.2.1.f Identifikation und Evaluierung Optionen für Risikobehandlung

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Managementsicht

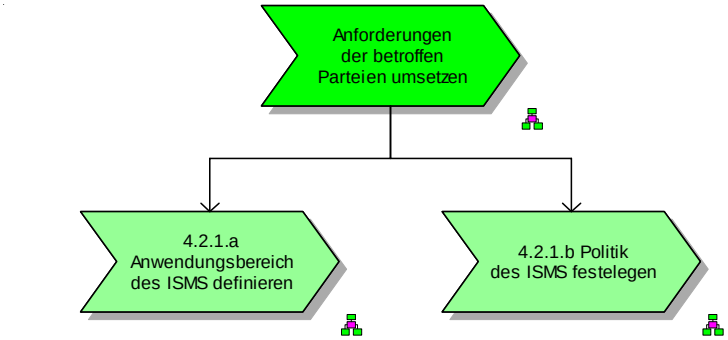


Wertschöpfungskettendiagramm: 4.2.1.h Erstellung einer Erklärung zur Anwendbarkeit
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Managementsicht



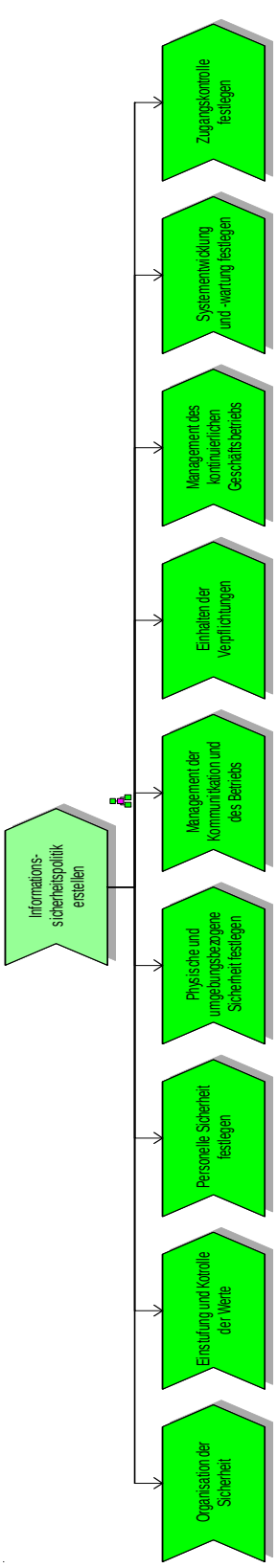
Wertschöpfungskettendiagramm: Anforderungen der betroffen Parteien

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Managementsicht



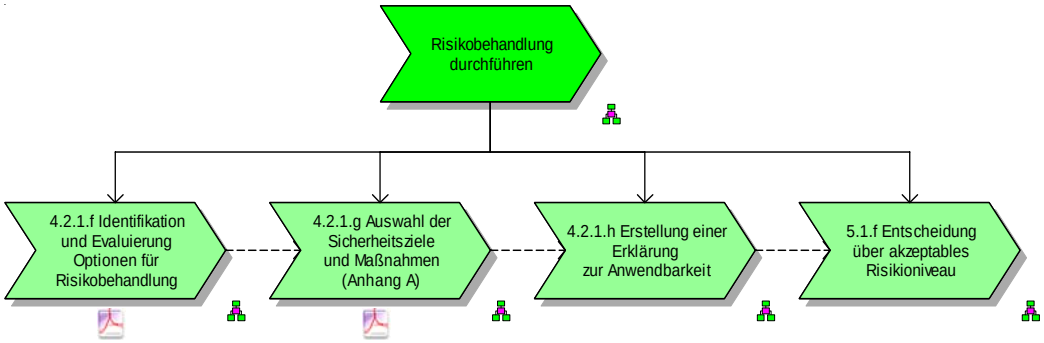
Wertschöpfungskettendiagramm: Festlegen der Sicherheitspolitk

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Managementsicht



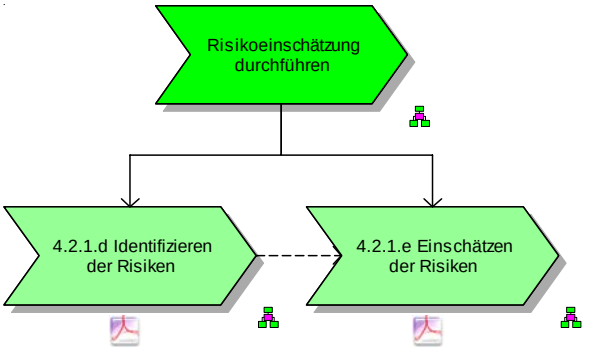
Wertschöpfungskettendiagramm: Risikobehandlung

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Managementsicht



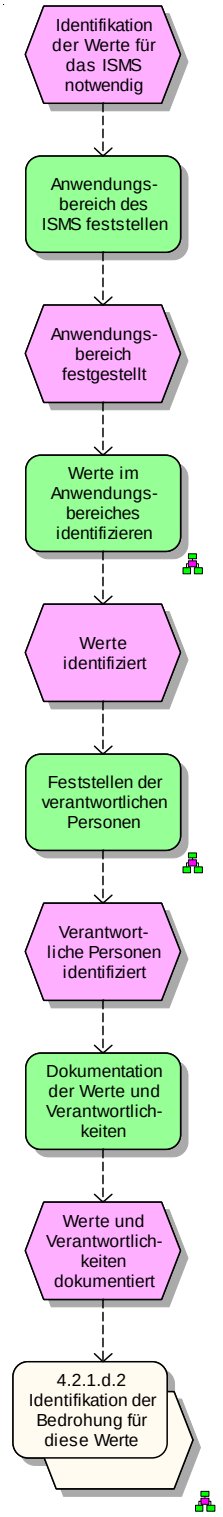
Wertschöpfungskettendiagramm: Risikoeinschätzung

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Managementsicht



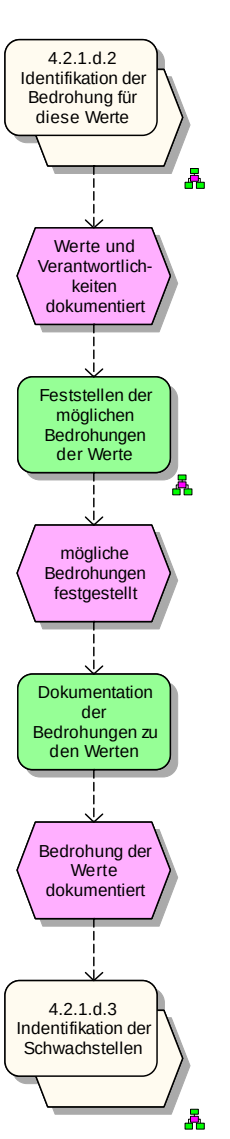
EPK: 4.2.1.d.1 Identifikation der Werte innerhalb des ISMS

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



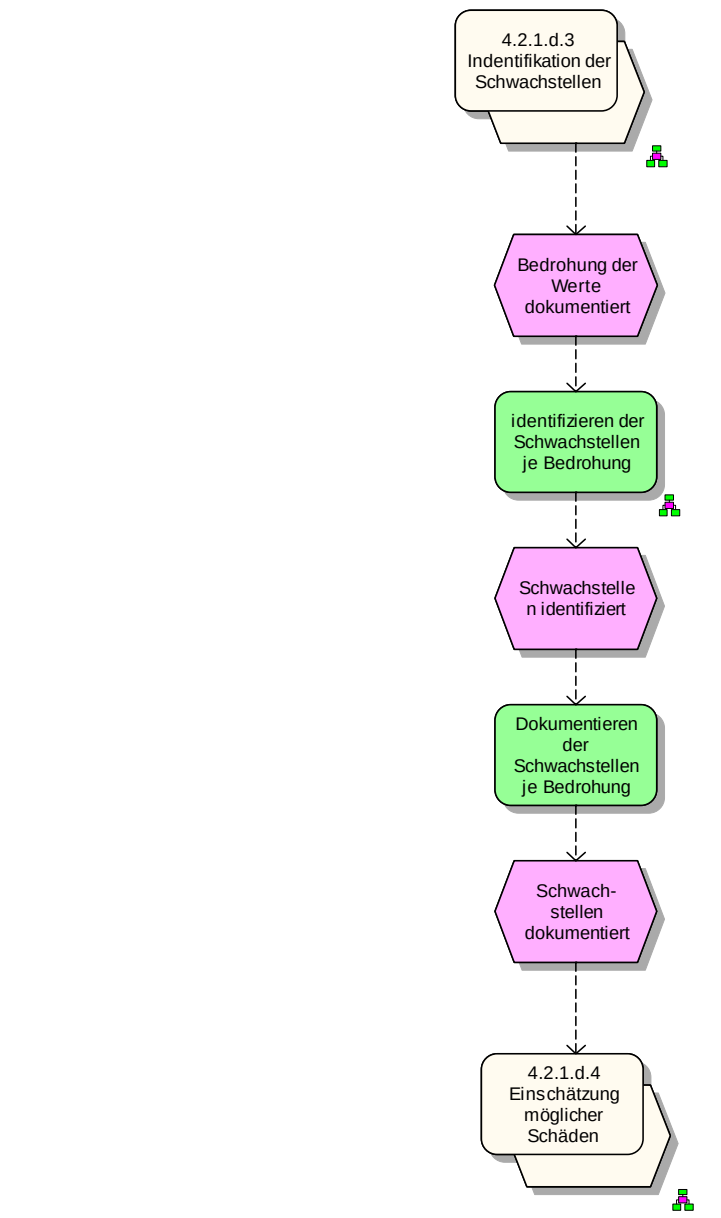
EPK: 4.2.1.d.2 Identifikation der Bedrohung für diese Werte

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



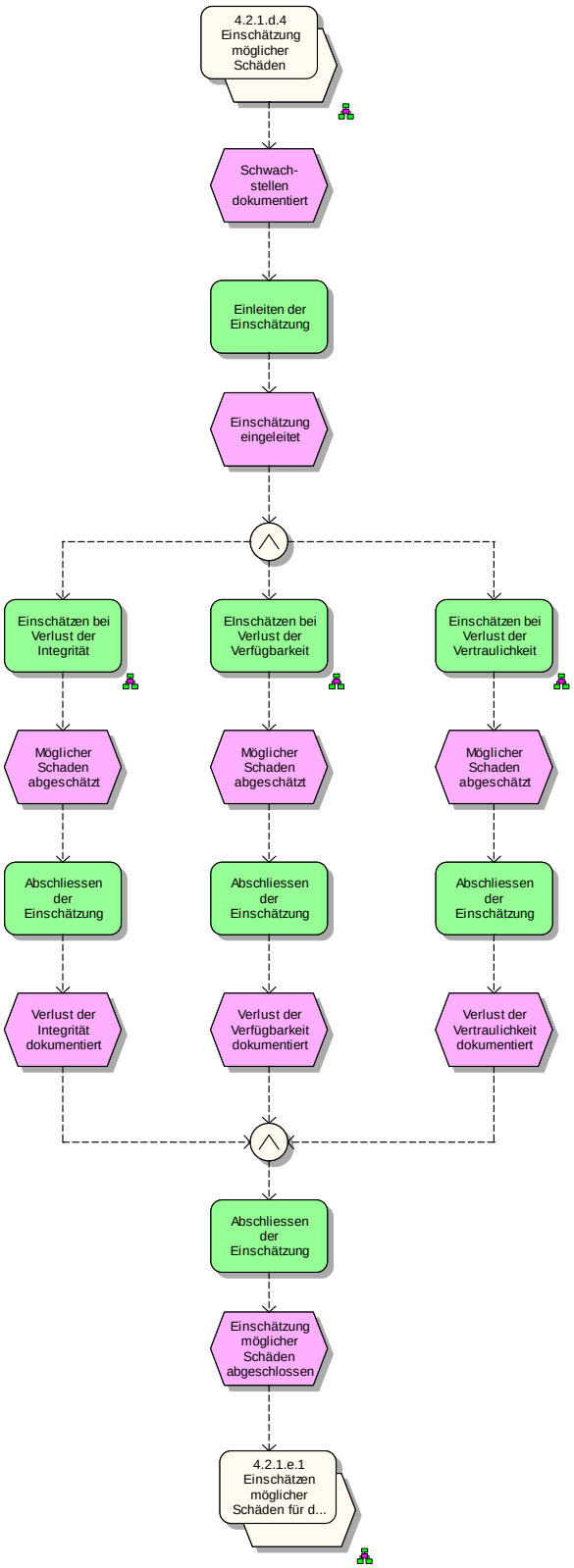
EPK: 4.2.1.d.3 Indentifikation der Schwachstellen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



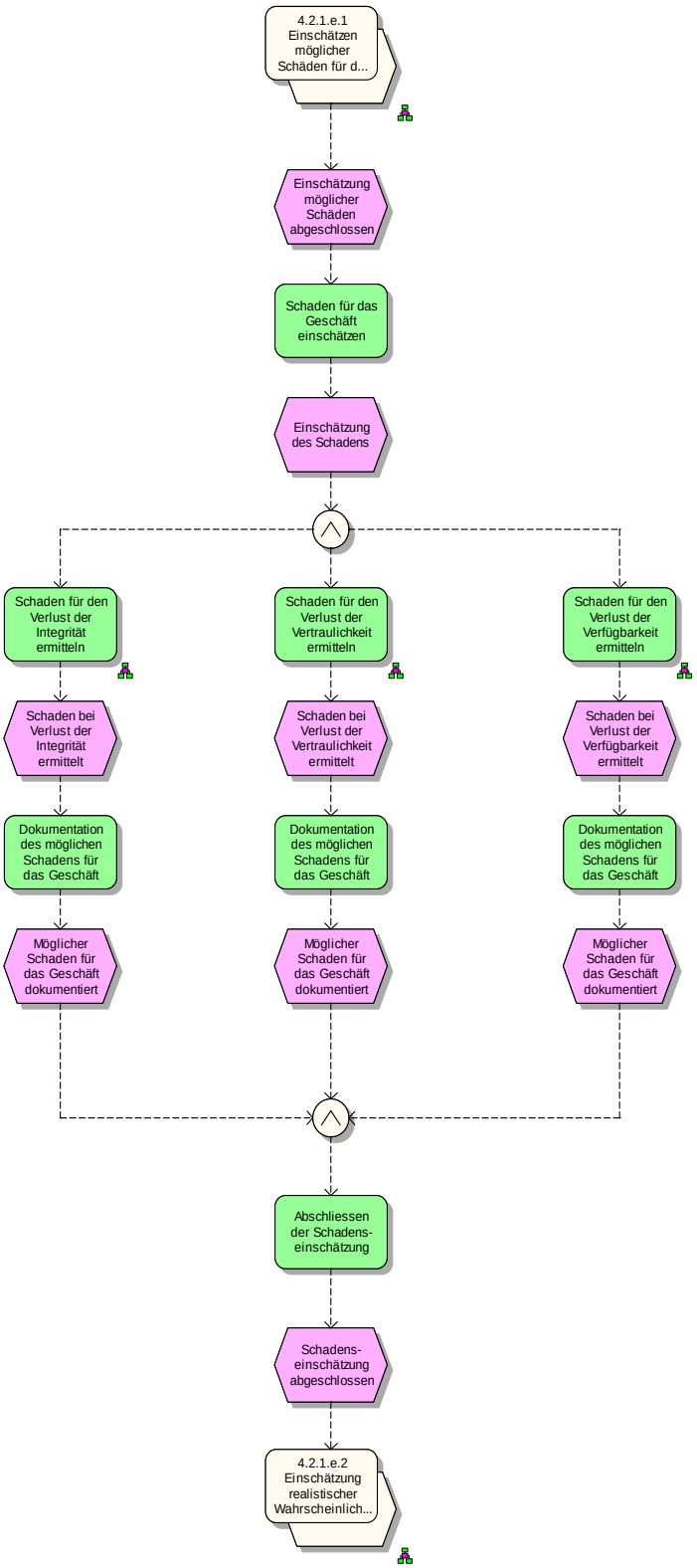
EPK: 4.2.1.d.4 Einschätzung möglicher Schäden

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



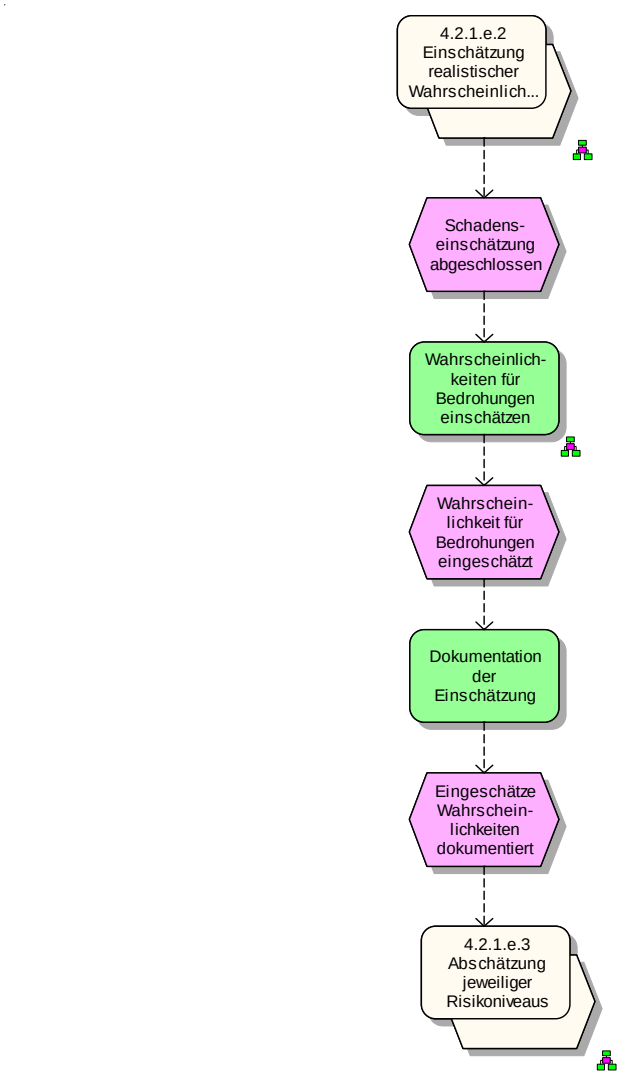
EPK: 4.2.1.e.1 Einschätzen möglicher Schäden für das Geschäft

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



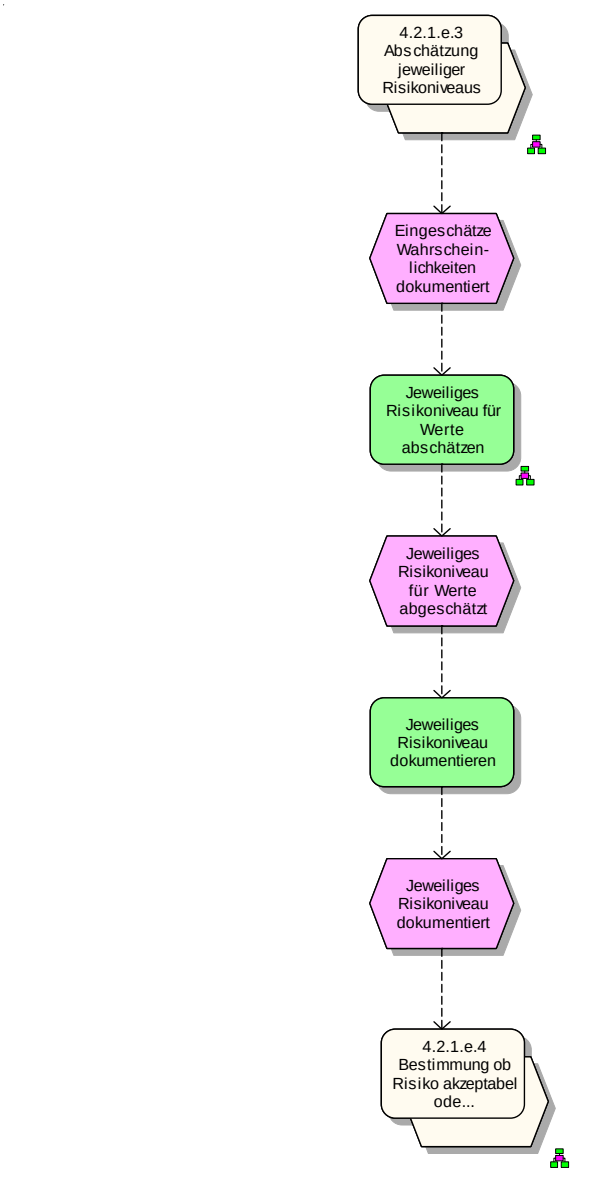
EPK: 4.2.1.e.2 Einschätzung realistischer Wahrscheinlichkeiten

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



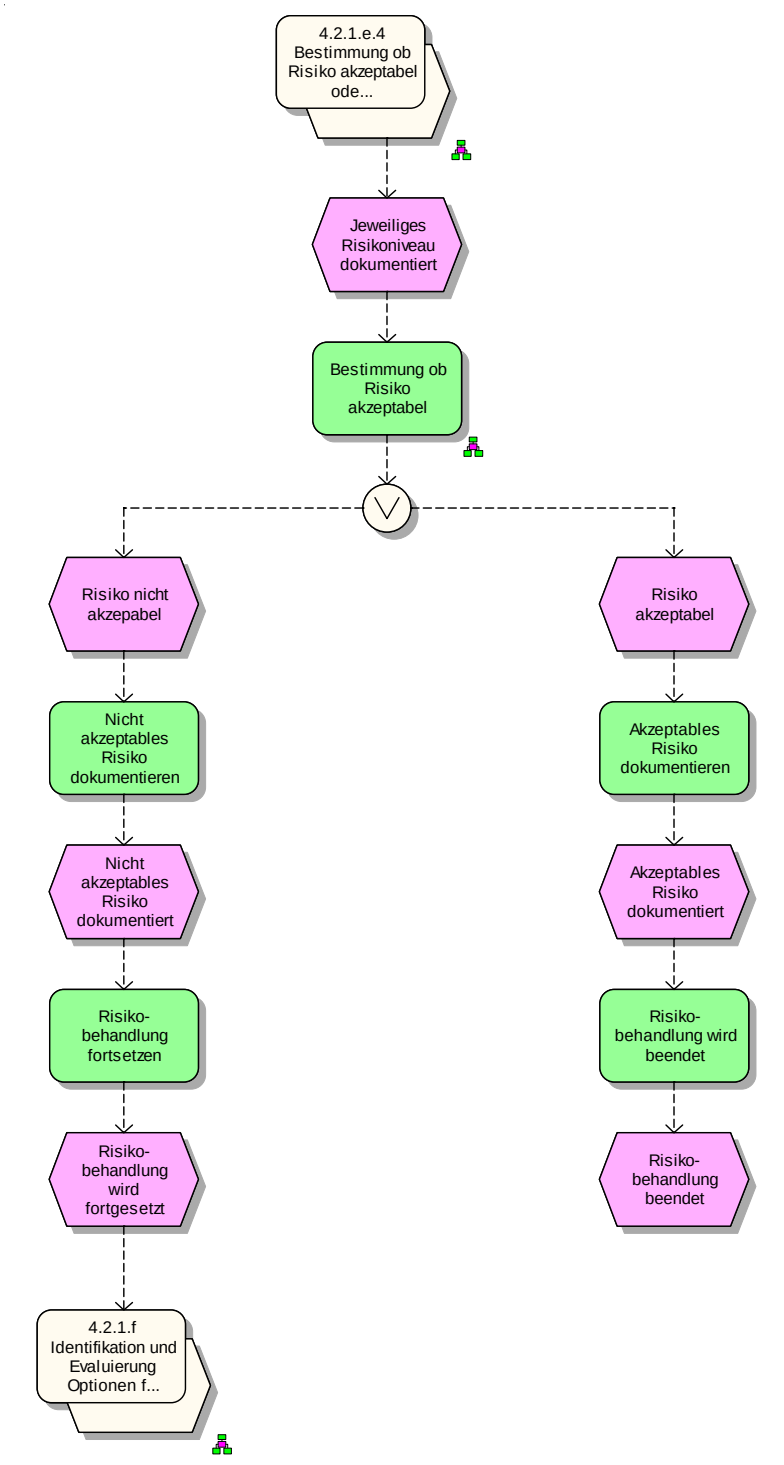
EPK: 4.2.1.e.3 Abschätzung jeweiliger Risikoniveaus

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



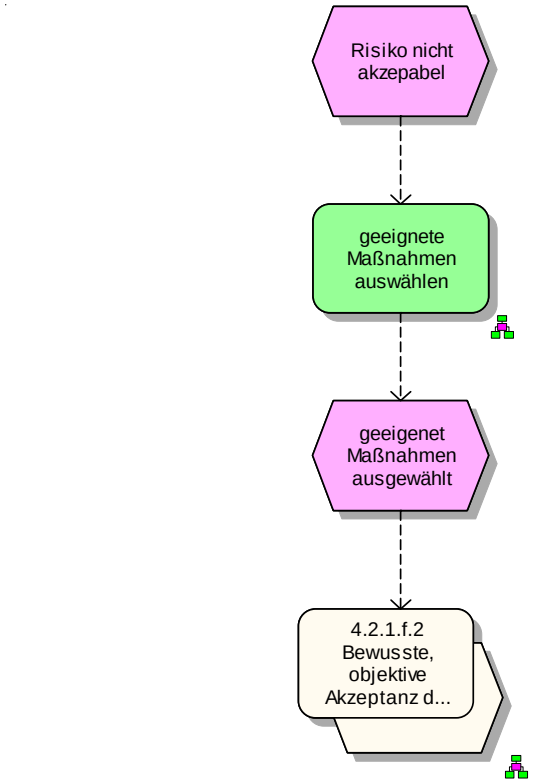
EPK: 4.2.1.e.4 Bestimmung ob Risiko akzeptabel oder Weiterbehandelung

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



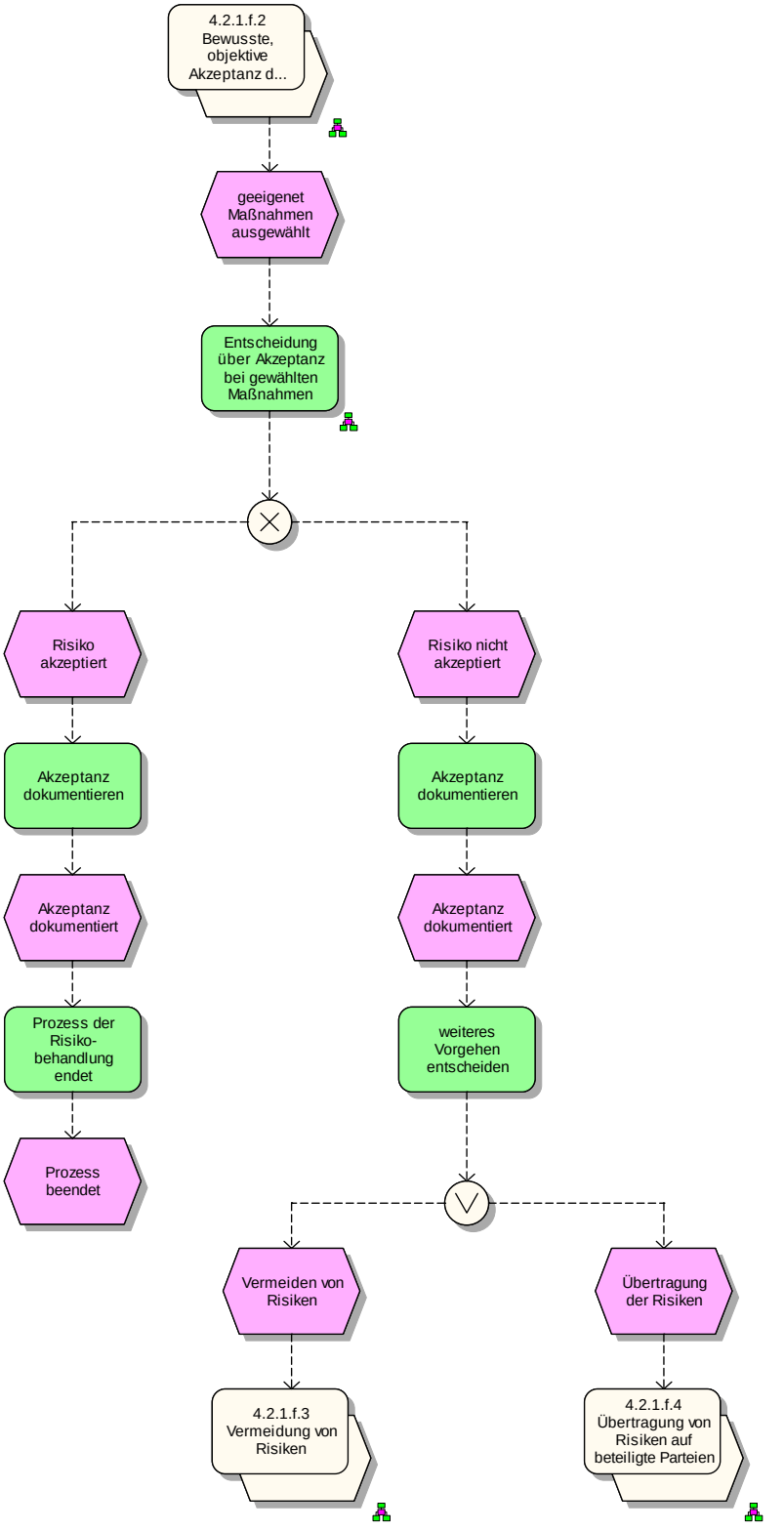
EPK: 4.2.1.f.1 Geeignete Maßnahmen ergreifen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



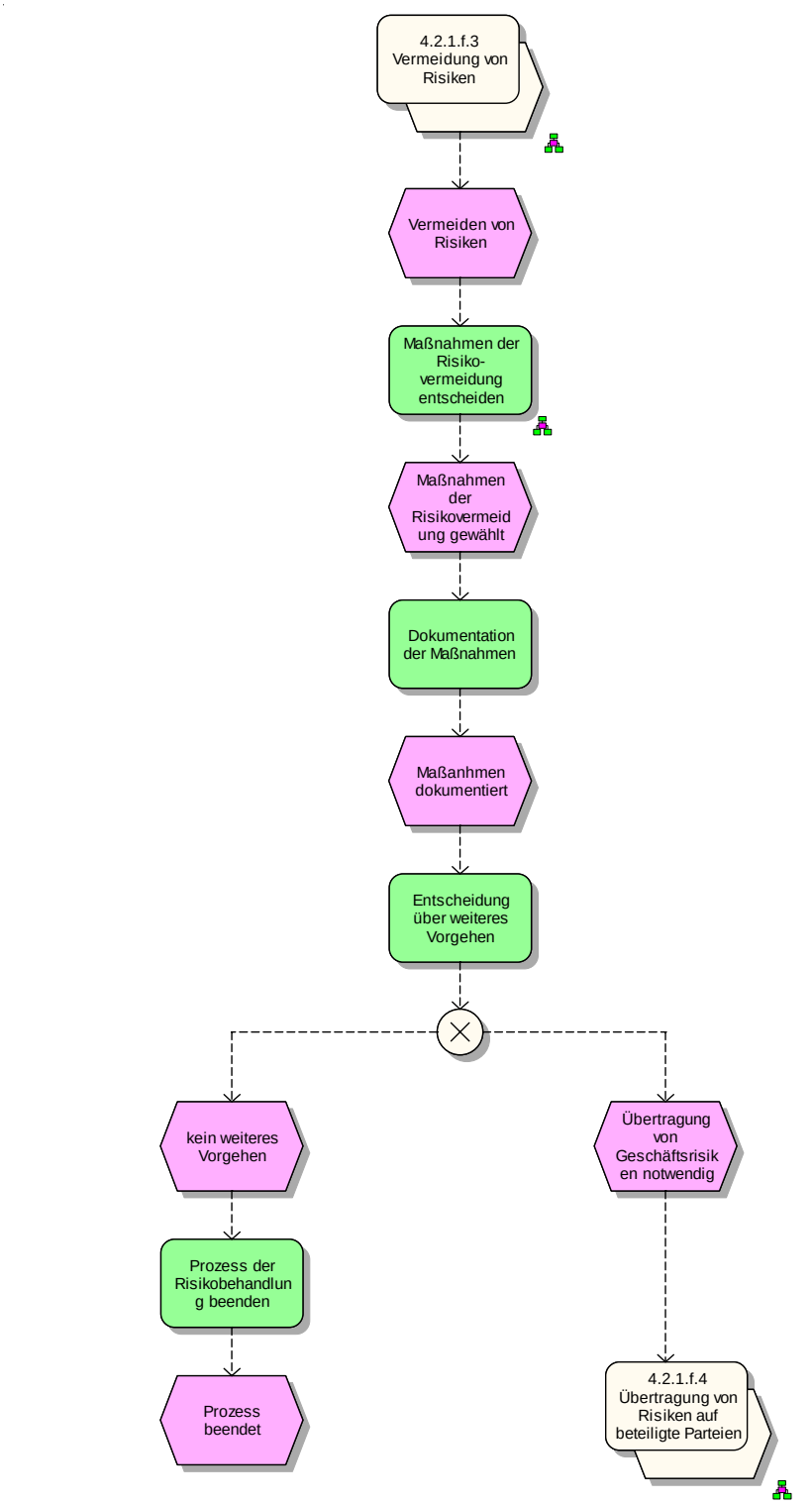
EPK: 4.2.1.f.2 Bewusste, objektive Akzeptanz der Risiken laut Politik

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



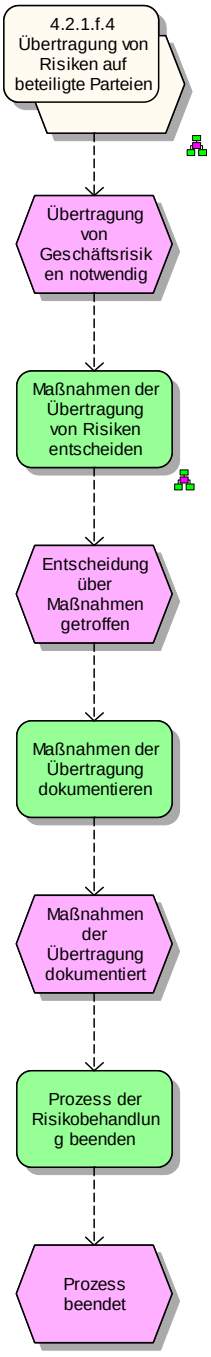
EPK: 4.2.1.f.3 Vermeidung von Risiken

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



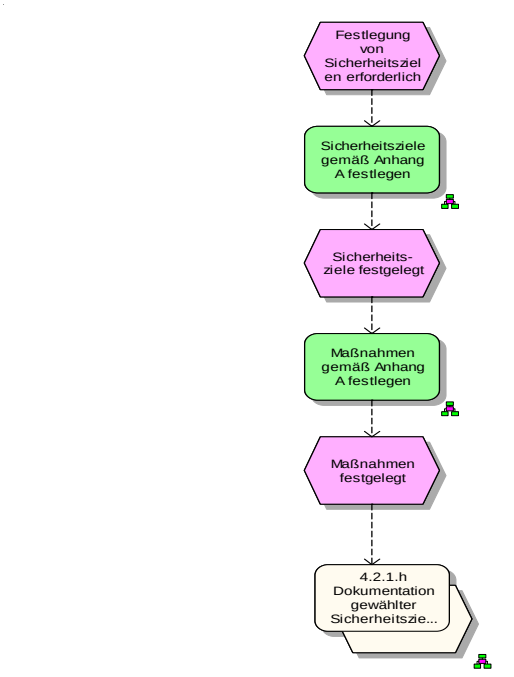
EPK: 4.2.1.f.4 Übertragung von Risiken auf beteiligte Parteien

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



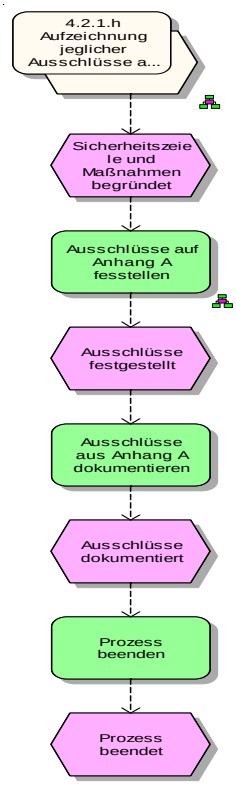
EPK: 4.2.1.g Auswahl der Sicherheitsziele und Maßnahmen (Anhang A)

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht

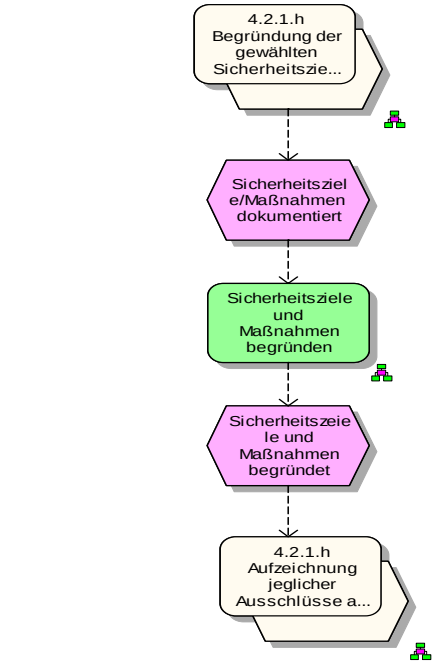


EPK: 4.2.1.h Aufzeichnung jeglicher Ausschlüsse aus Anhang A

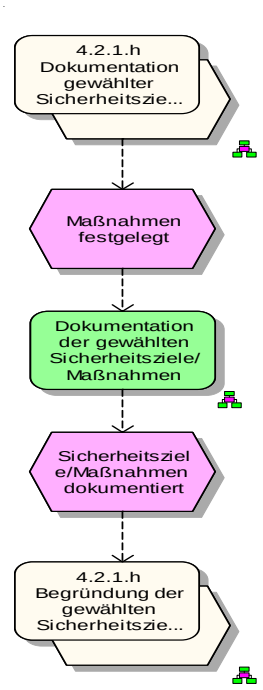
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



EPK: 4.2.1.h Begründung der gewählten Sicherheitsziele und Maßnahmen
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht

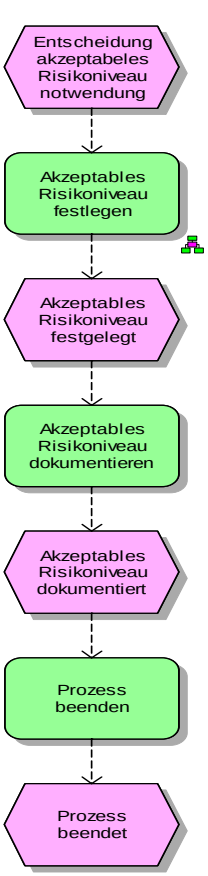


EPK: 4.2.1.h Dokumentation gewählter Sicherheitsziele und Maßnahmen
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



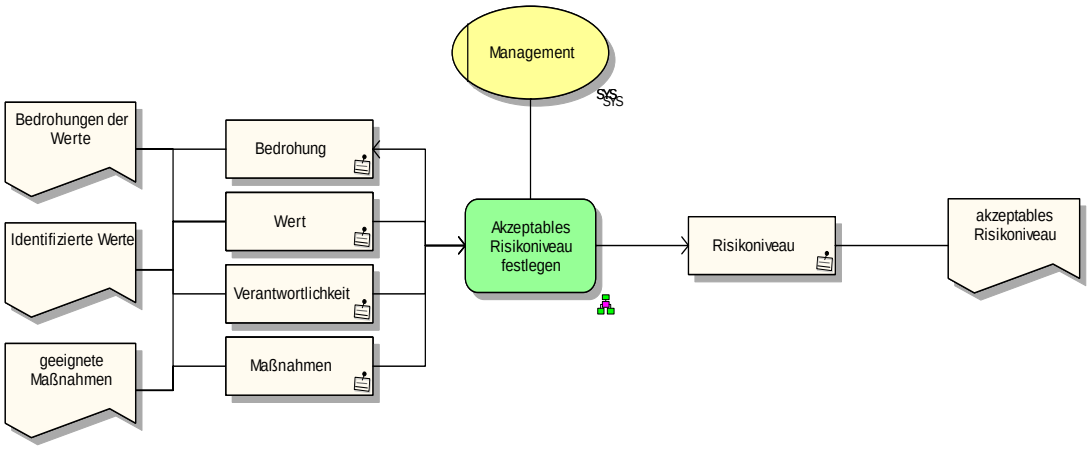
EPK: 5.1.f Entscheidung über akzeptables Risikioniveau

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



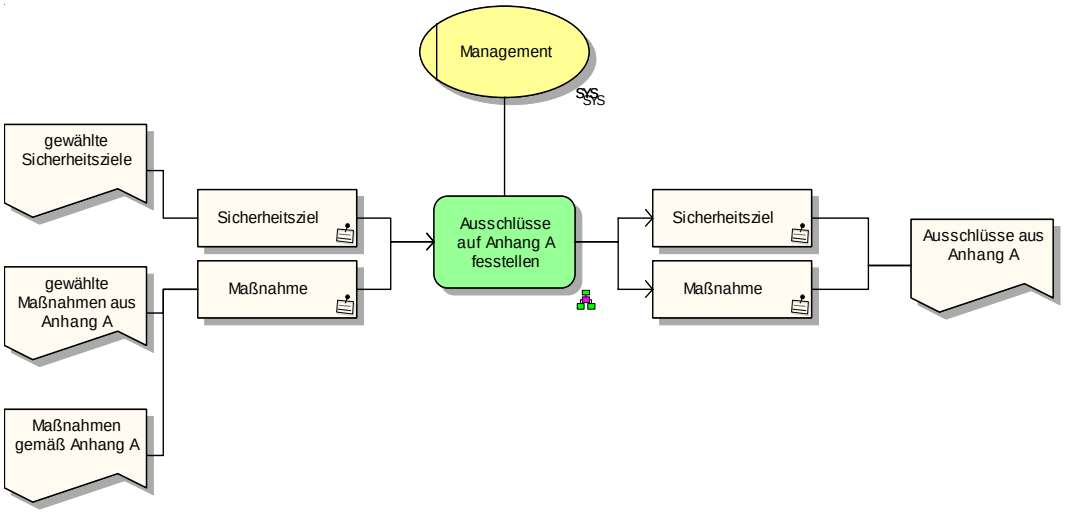
Funktionszuordnungsdiagramm: Akzeptables Risikoniveau festlegen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



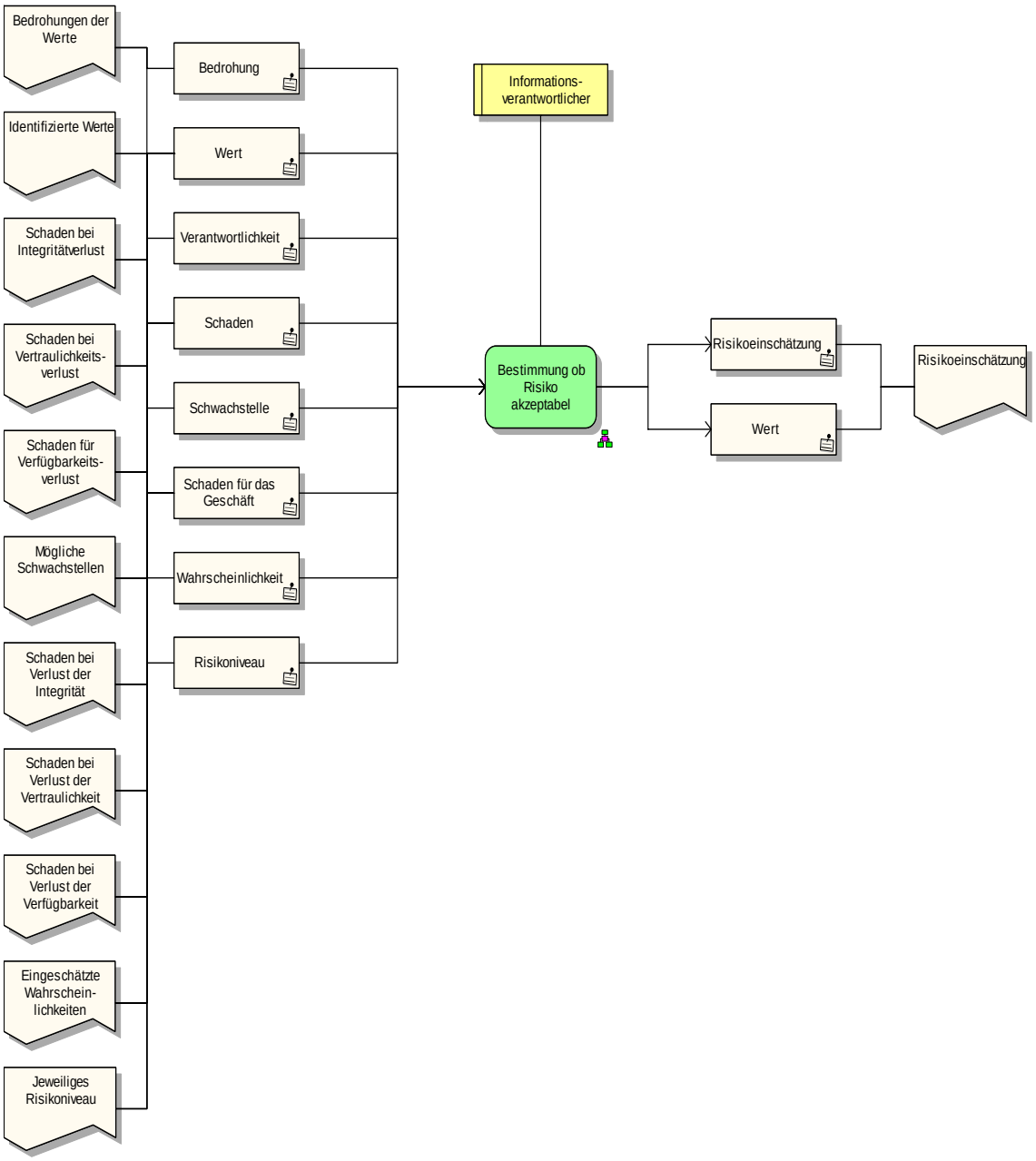
Funktionszuordnungsdiagramm: Ausschlüsse auf Anhang A fesstellen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



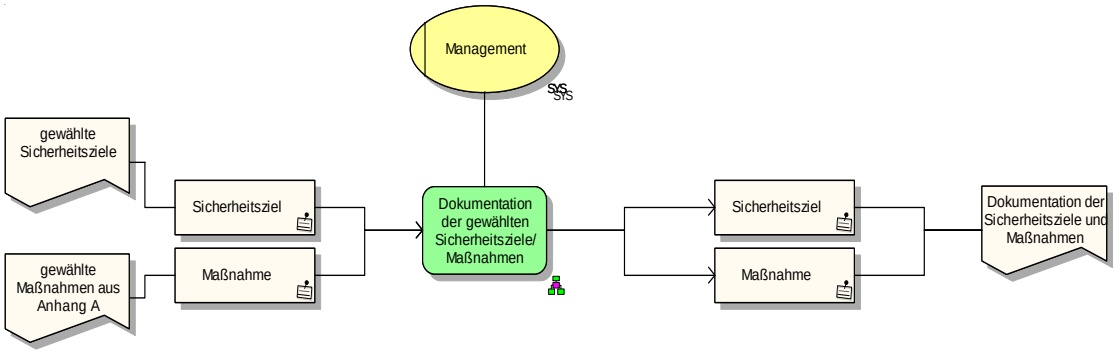
Funktionszuordnungsdiagramm: Bestimmung ob Risiko akzeptabel

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



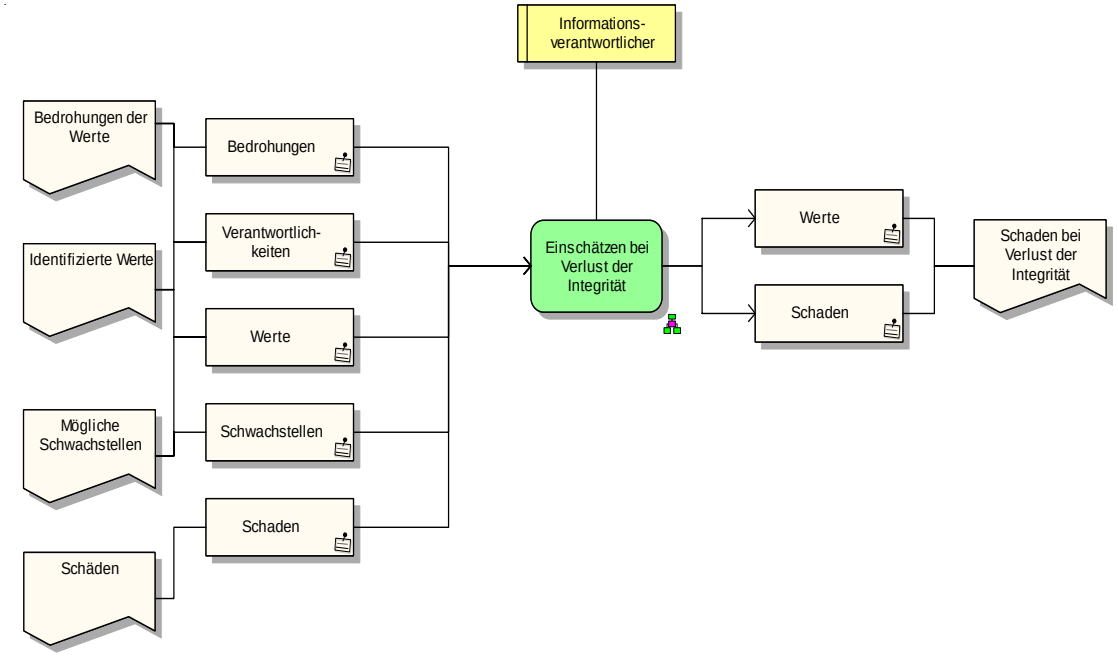
Funktionszuordnungsdiagramm: Dokumentation der gewählten Sicherheitsziele/Maßnahmen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht

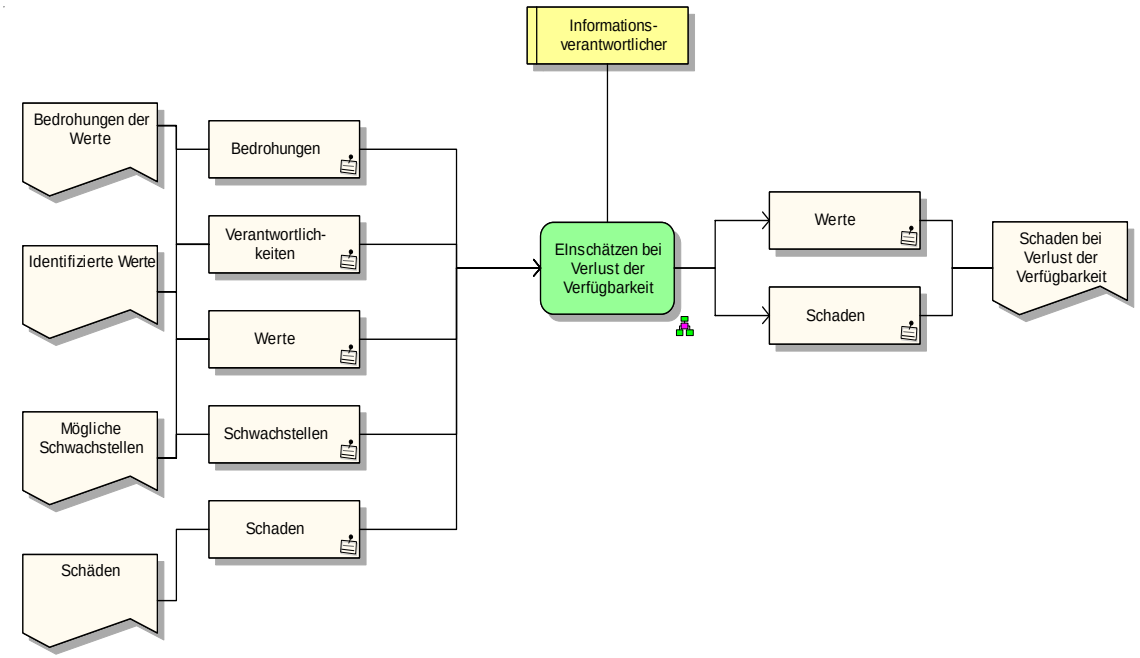


Funktionszuordnungsdiagramm: Einschätzen bei Verlust der Integrität

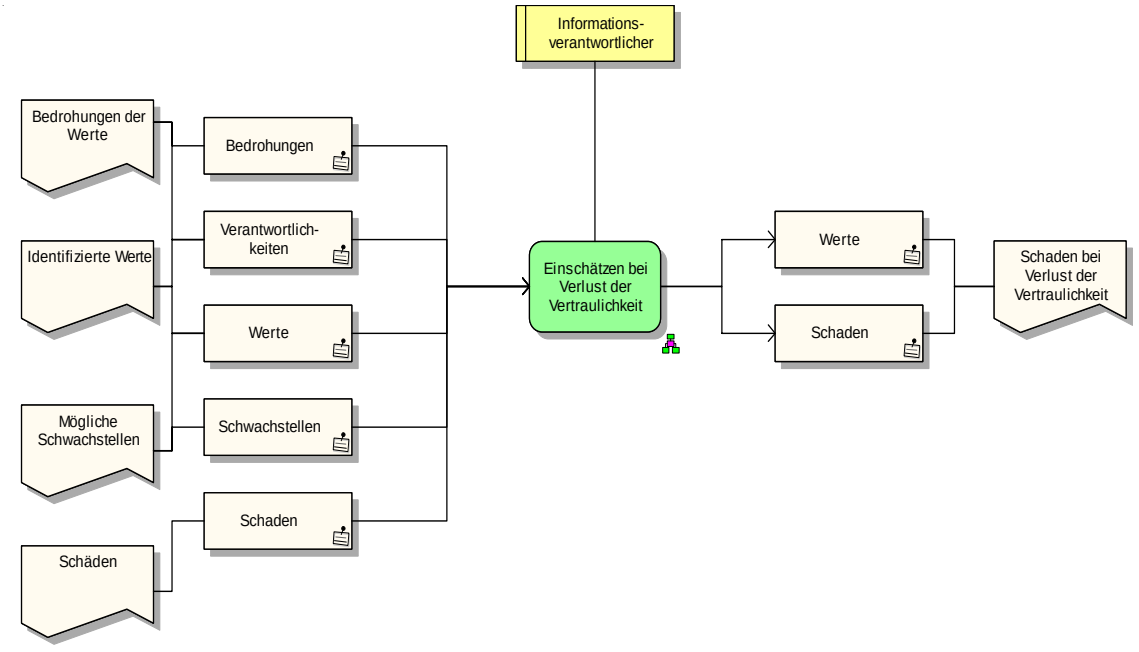
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



Funktionszuordnungsdiagramm: EInschätzen bei Verlust der Verfügbarkeit
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht

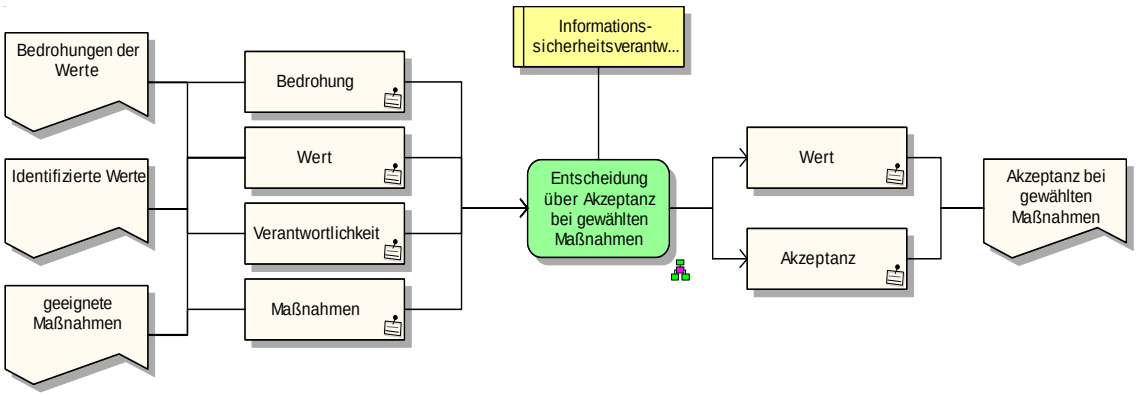


Funktionszuordnungsdiagramm: Einschätzen bei Verlust der Vertraulich-keit
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



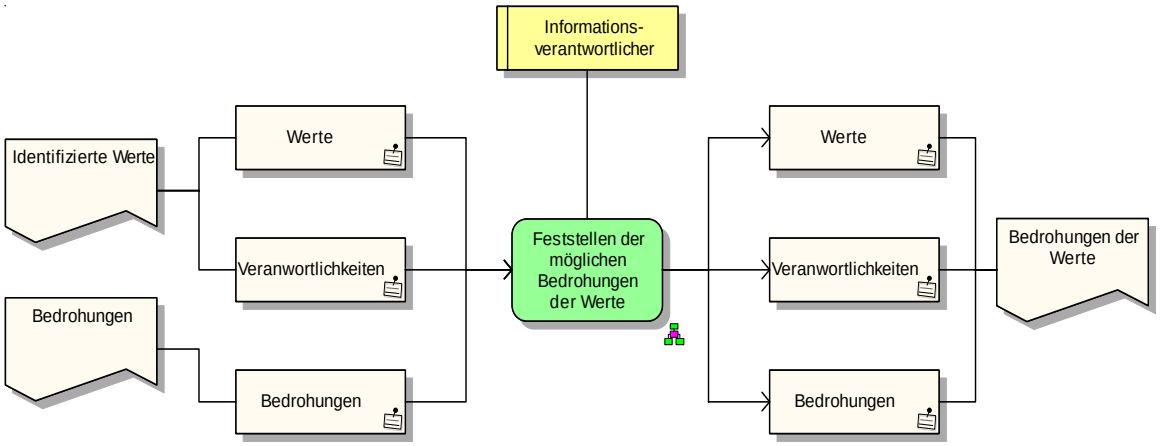
Funktionszuordnungsdiagramm: Entscheidung über Akzeptanz bei gewählten Maßnahmen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



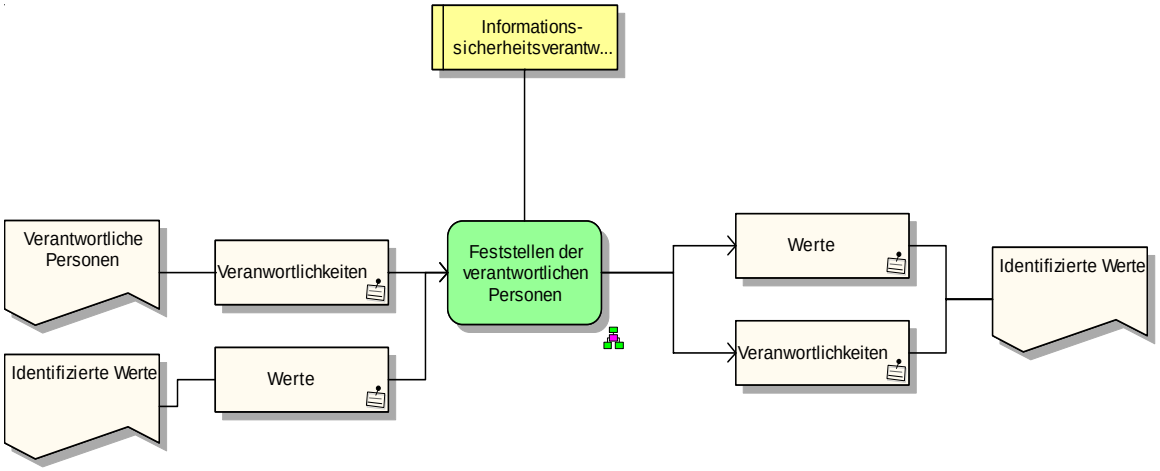
Funktionszuordnungsdiagramm: Feststellen der möglichen Bedrohungen der Werte

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



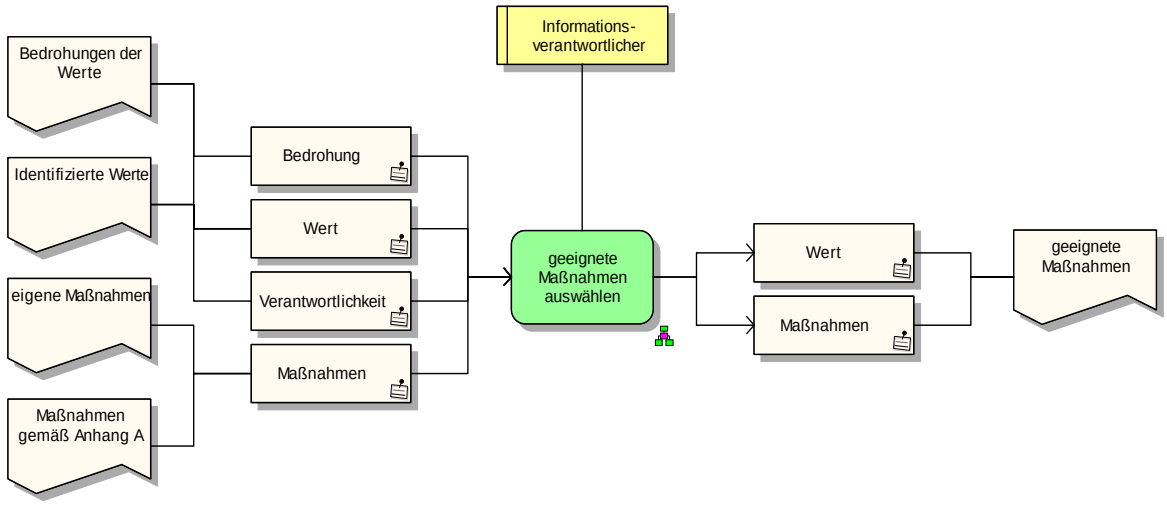
Funktionszuordnungsdiagramm: Feststellen der verantwortlichen Personen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



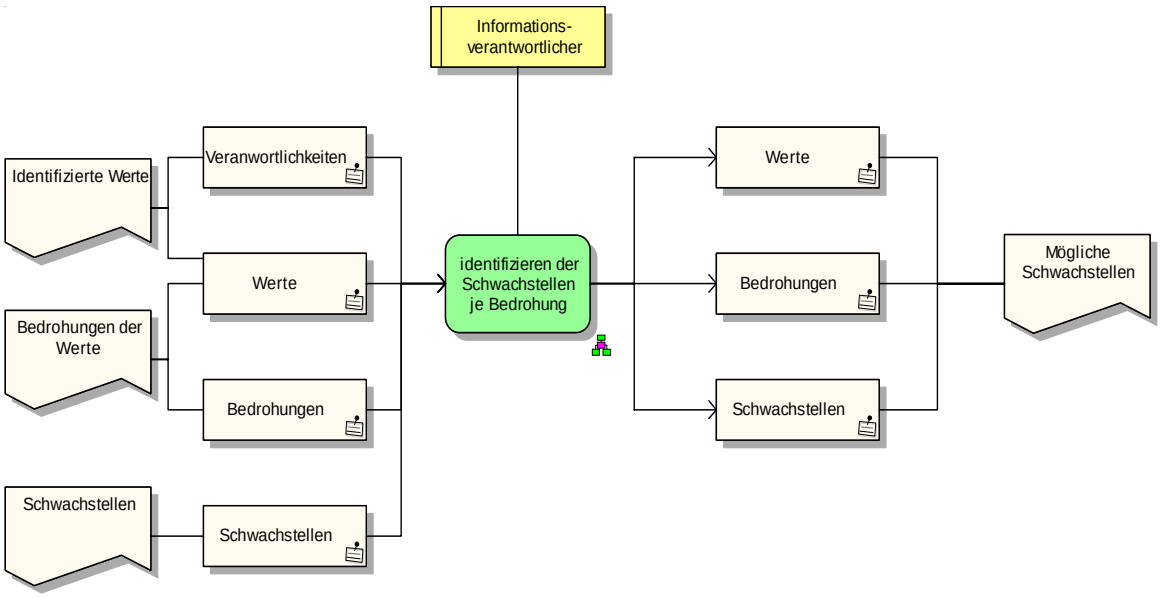
Funktionszuordnungsdiagramm: geeignete Maßnahmen auswählen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



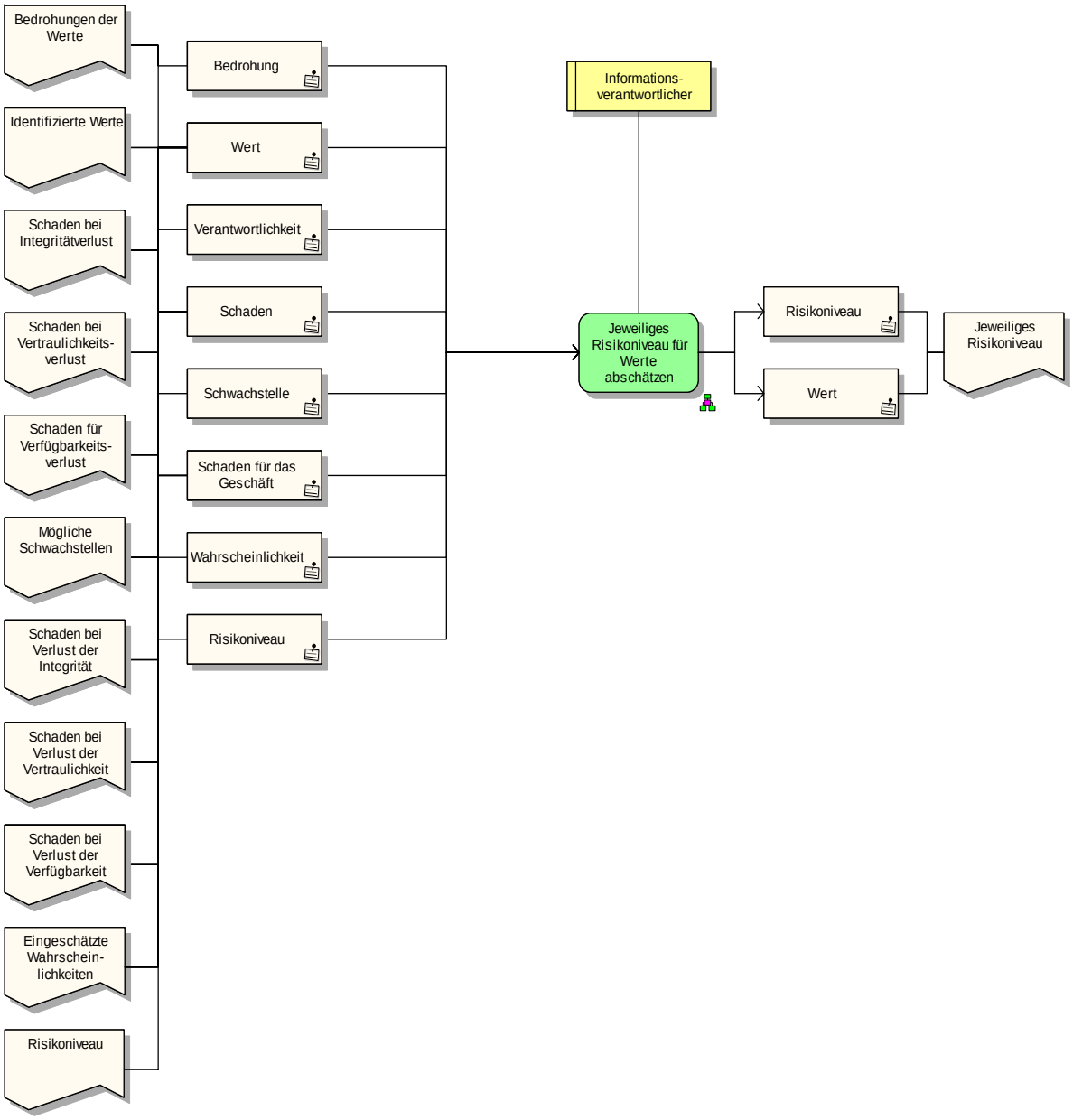
Funktionszuordnungsdiagramm: identifizieren der Schwachstellen je Bedrohung

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



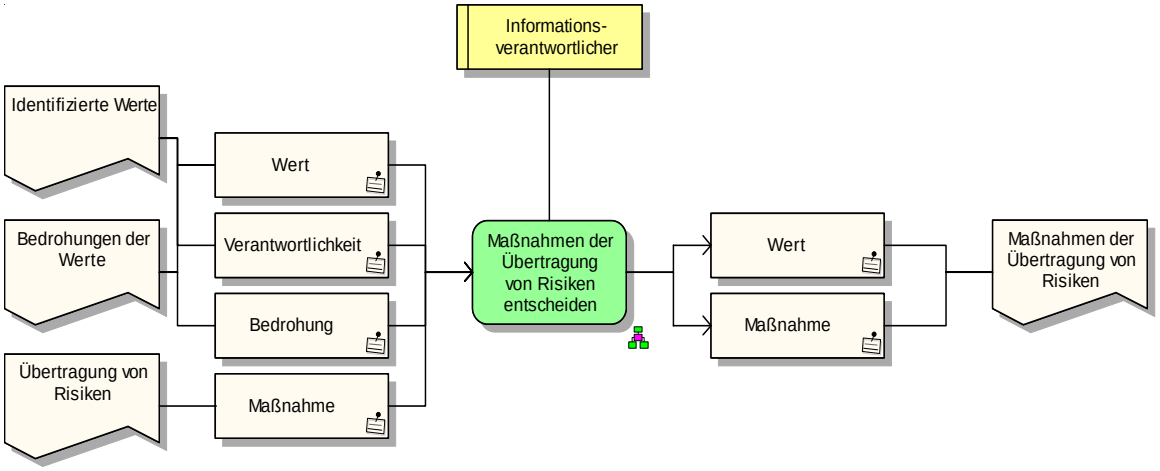
Funktionszuordnungsdiagramm: Jeweiliges Risikoniveau für Werte abschätzen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



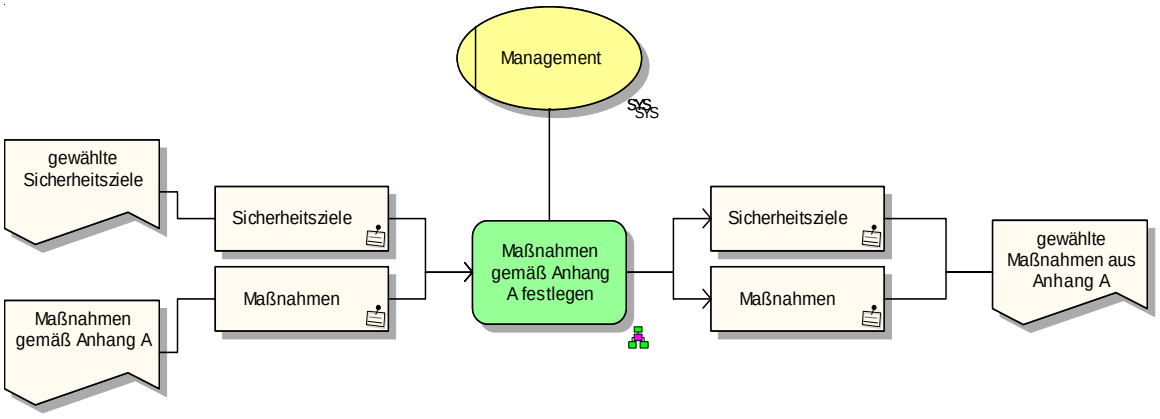
Funktionszuordnungsdiagramm: Maßnahmen der Übertragung von Risiken entscheiden

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



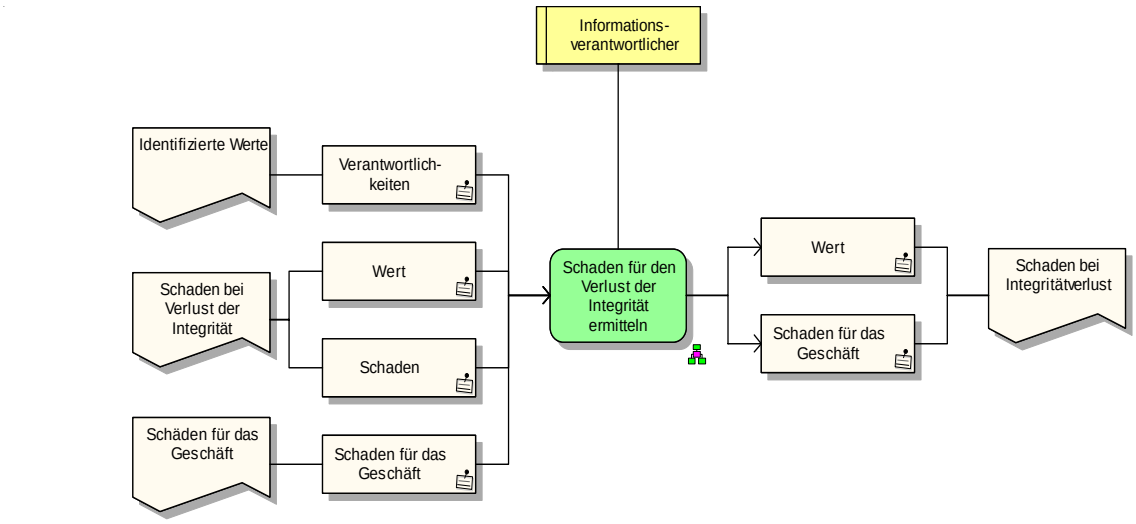
Funktionszuordnungsdiagramm: Maßnahmen gemäß Anhang A festlegen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



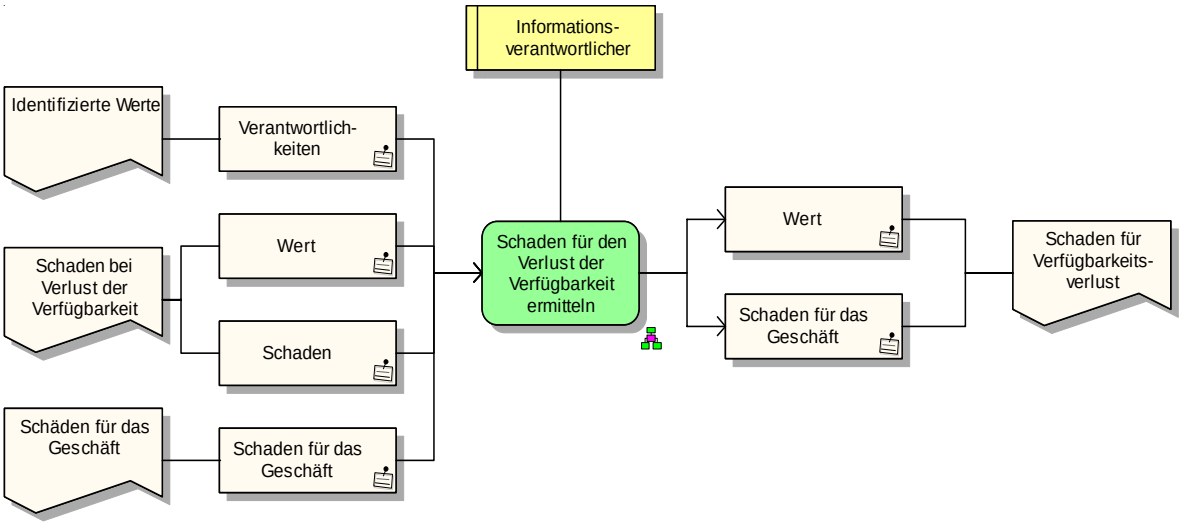
Funktionszuordnungsdiagramm: Schaden für den Verlust der Integrität ermitteln

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



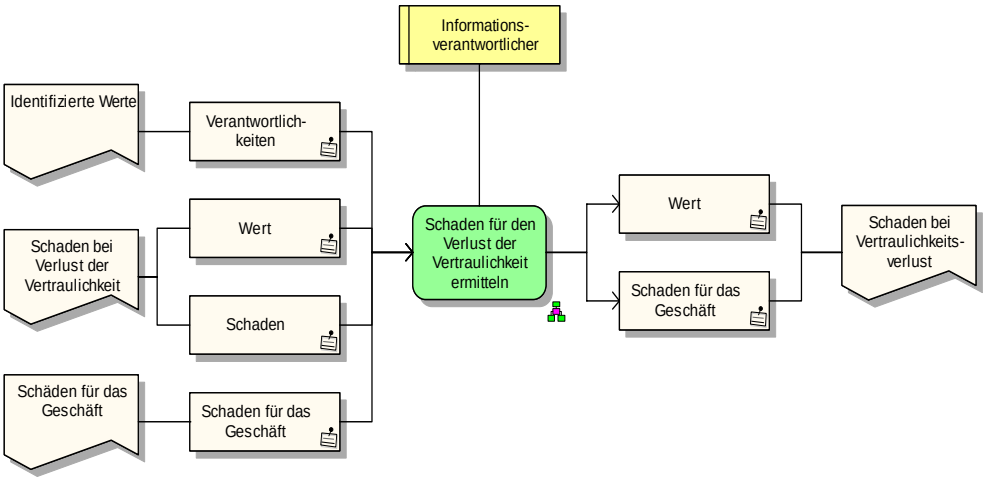
Funktionszuordnungsdiagramm: Schaden für den Verlust der Verfügbarkeit ermitteln

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



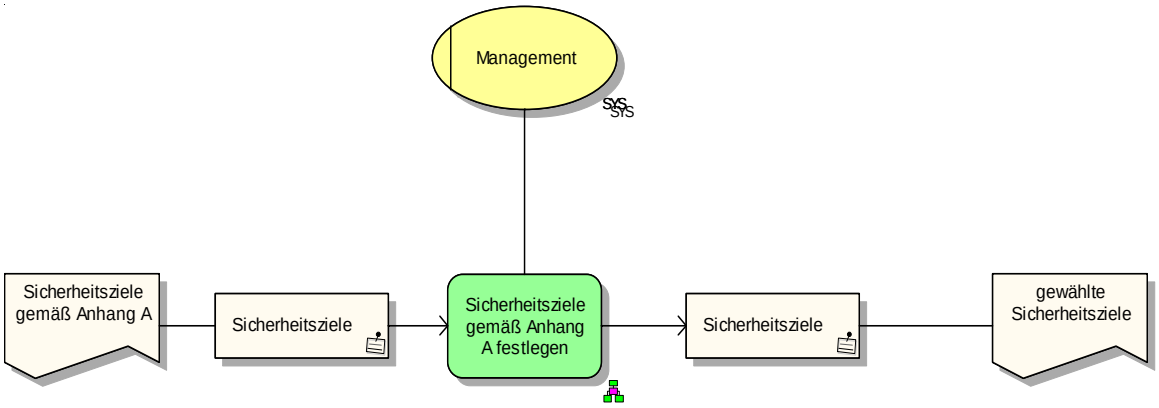
Funktionszuordnungsdiagramm: Schaden für den Verlust der Vertraulichkeit ermitteln

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



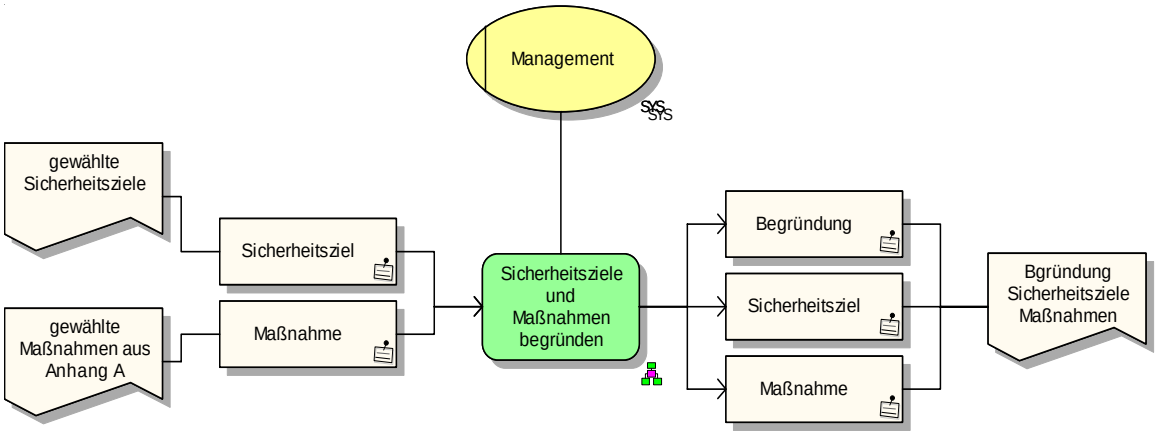
Funktionszuordnungsdiagramm: Sicherheitsziele gemäß Anhang A festlegen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



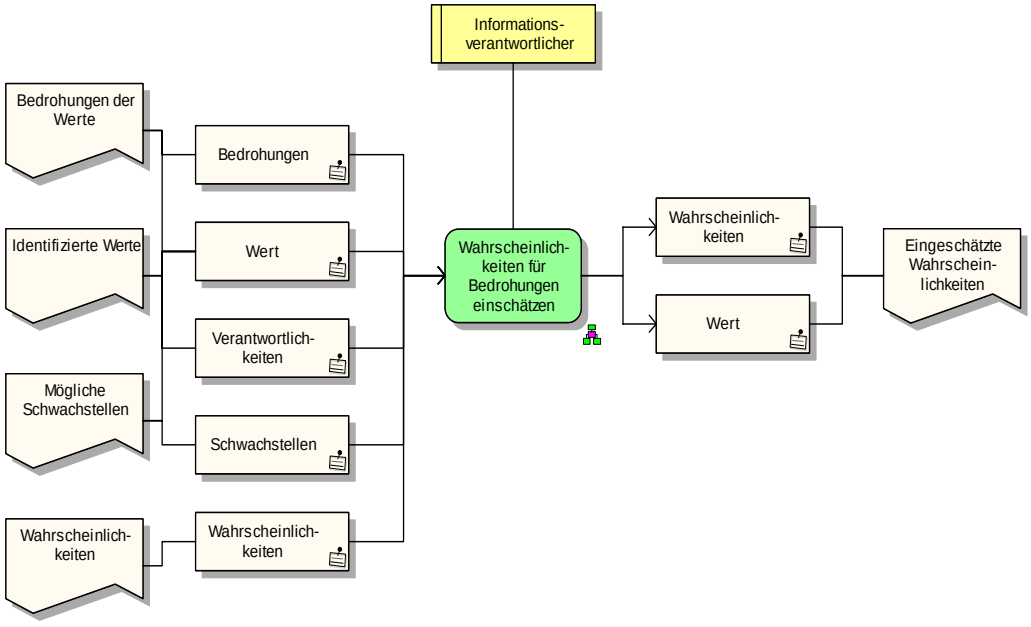
Funktionszuordnungsdiagramm: Sicherheitsziele und Maßnahmen begründen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



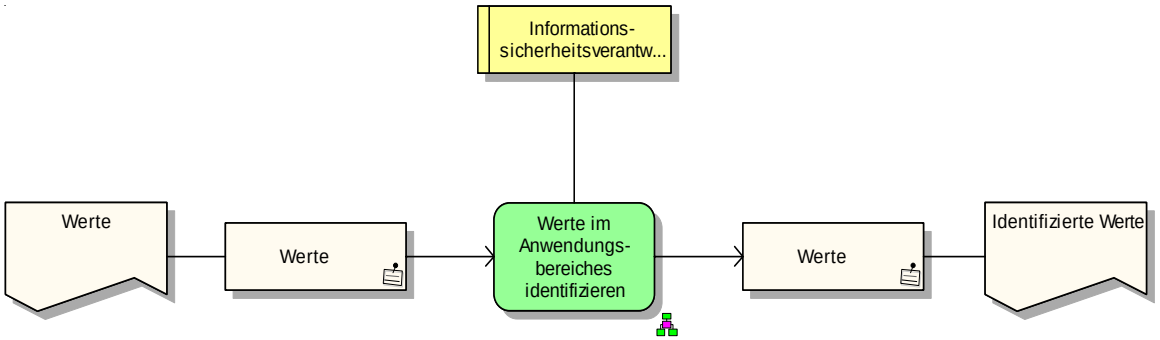
Funktionszuordnungsdiagramm: Wahrscheinlich-keiten für Bedrohungen einschätzen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



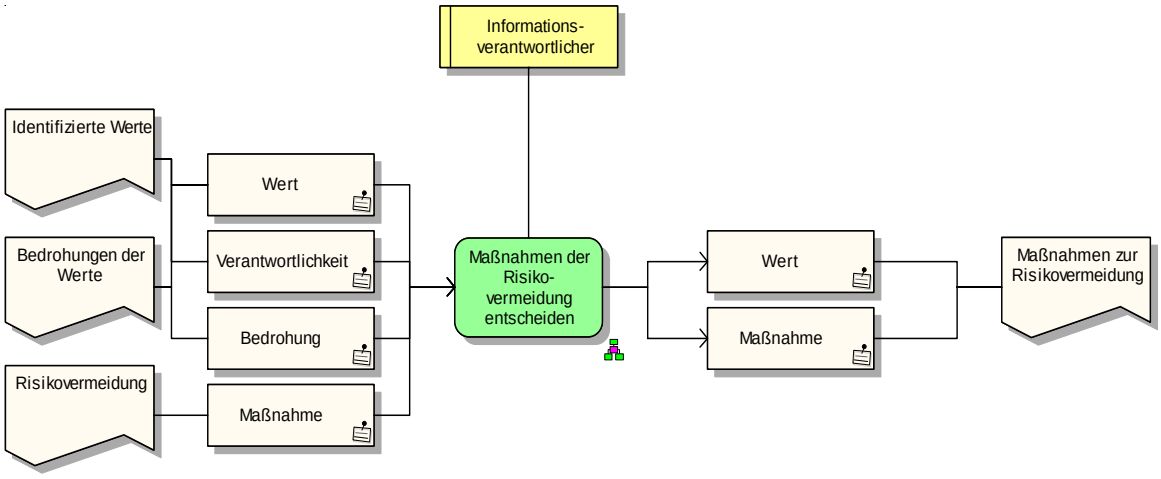
Funktionszuordnungsdiagramm: Werte innerhalb identifizieren

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht



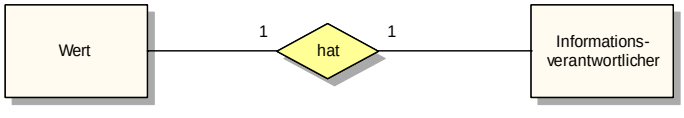
Funktionszuordnungsdiagramm: über Maßnahmen der Risikovermeidung entscheiden

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht

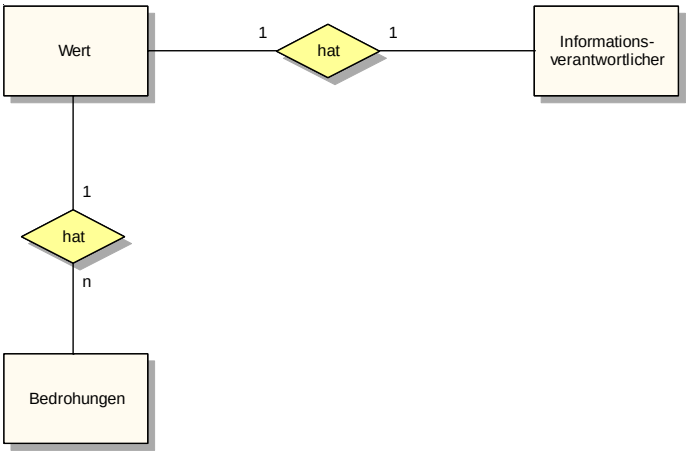


eERM: 4.2.1.d.1 Identifikation der Werte innerhalb des ISMS

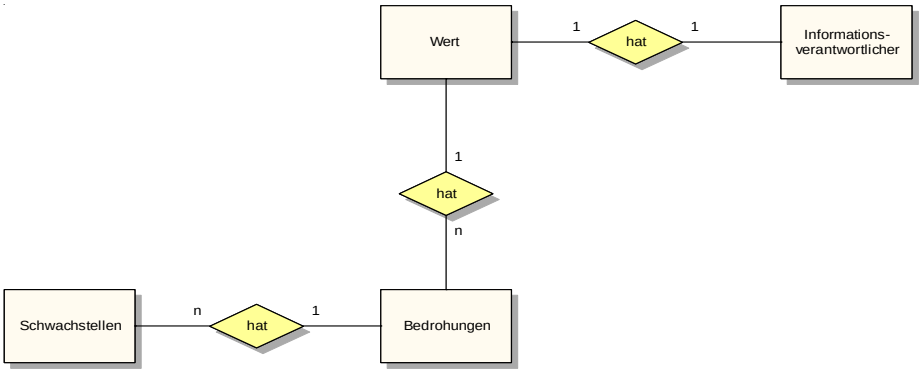
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



eERM: 4.2.1.d.2 Identifikation der Bedrohung für diese Werte
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung

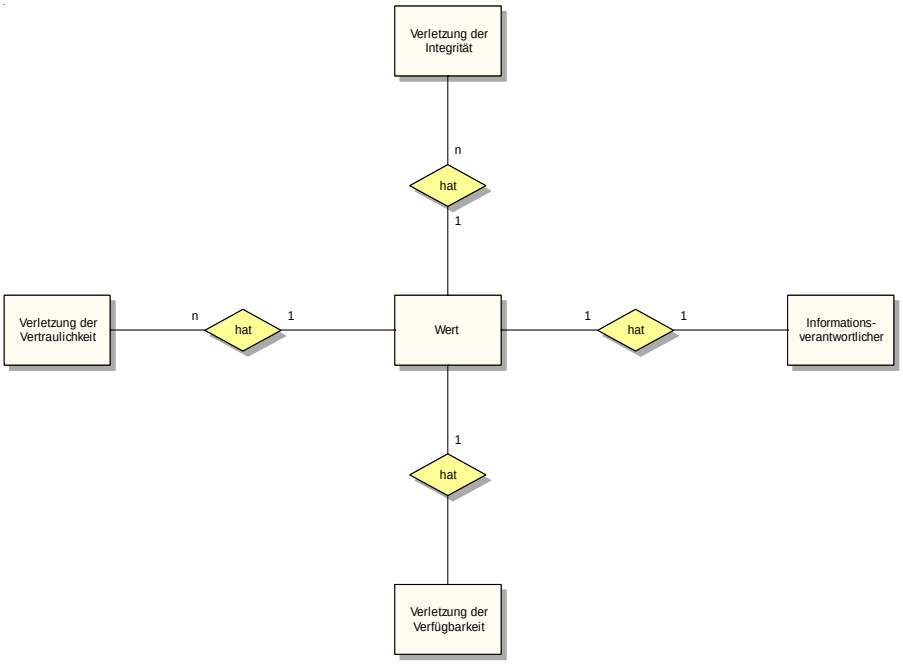


eERM: 4.2.1.d.3 Indentifikation der Schwachstellen
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



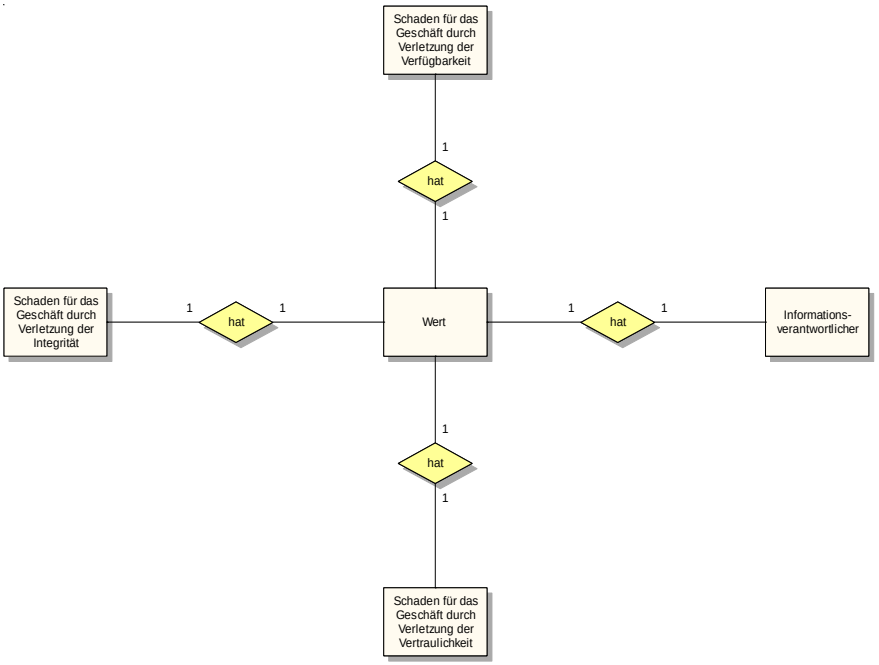
eERM: 4.2.1.d.4 Einschätzen der möglichen Schäden

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



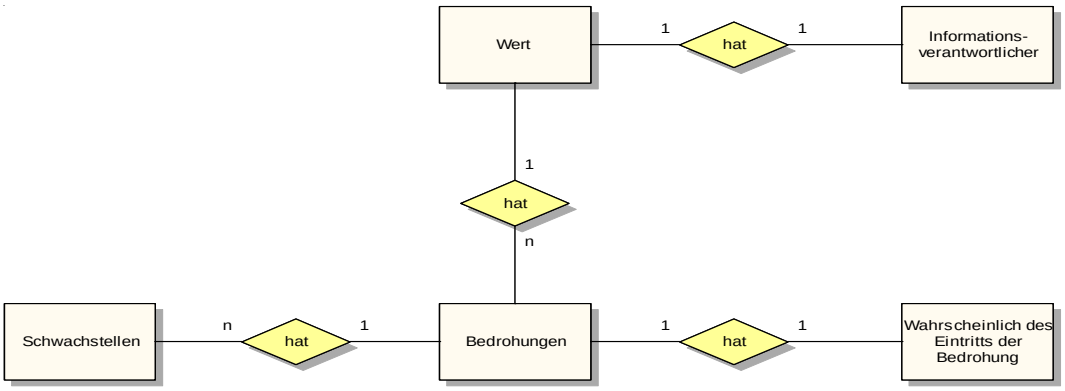
eERM: 4.2.1.e.1 Einschätzen möglicher Schäden für das Geschäft

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



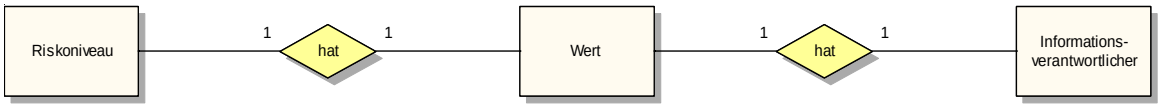
eERM: 4.2.1.e.2 Einschätzung realistischer Wahrscheinlichkeiten

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



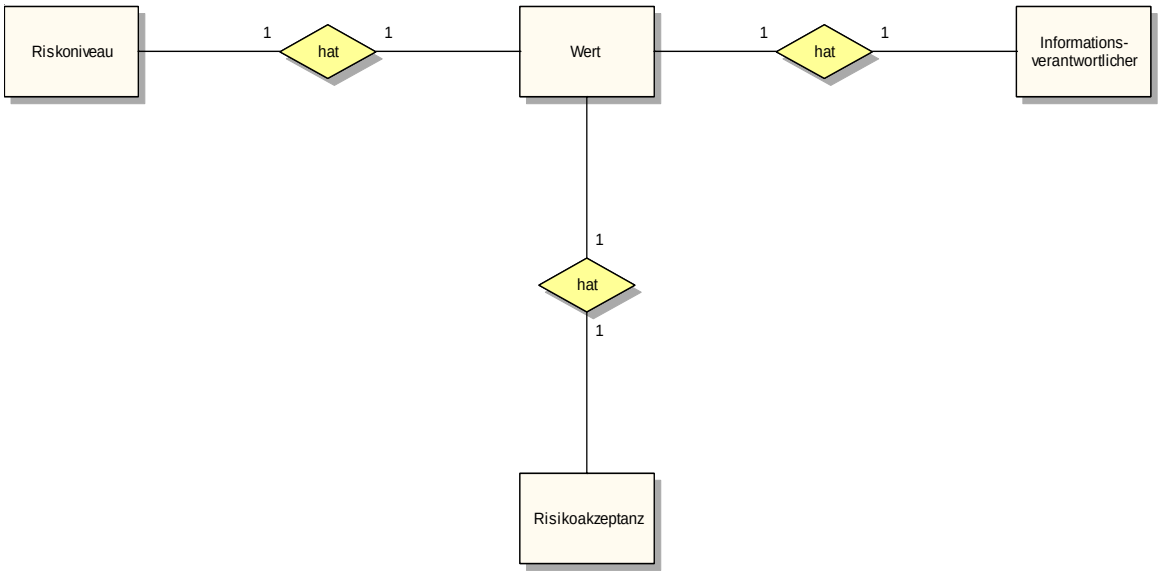
eERM: 4.2.1.e.3 Abschätzung jeweiliger Risikoniveaus

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



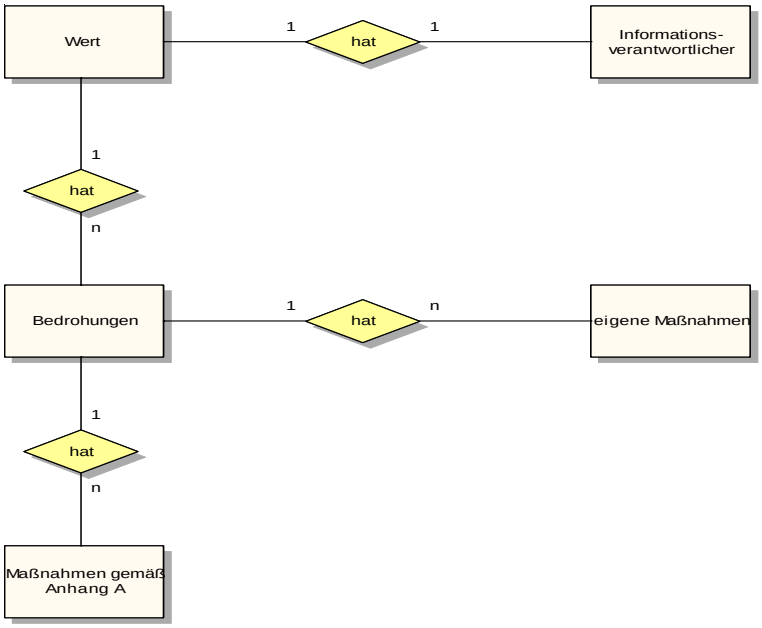
eERM: 4.2.1.e.4 Bestimmung ob Risiko akzeptabel oder Weiterbehandelung

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



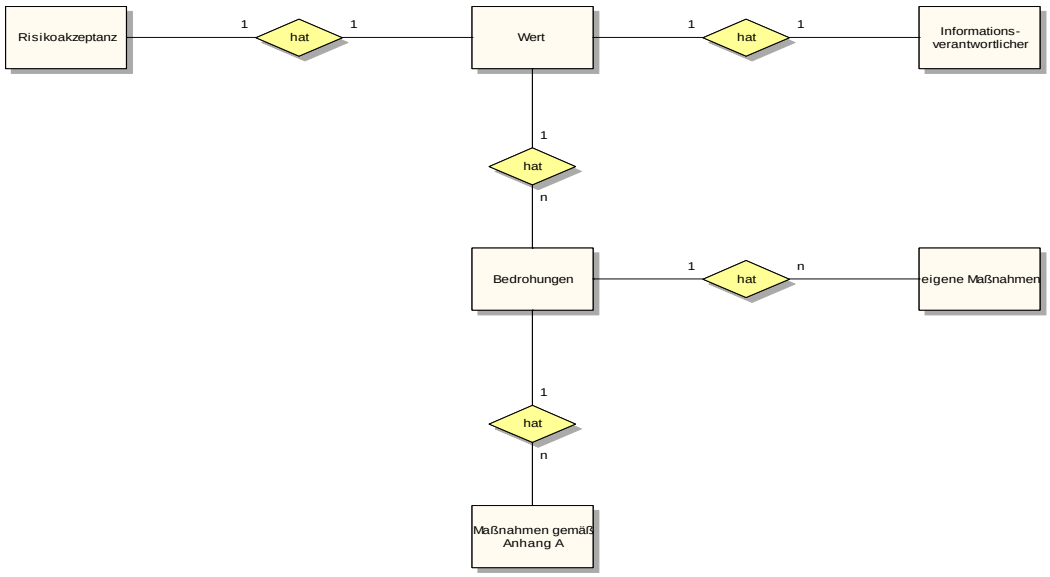
eERM: 4.2.1.f.1 Geeignete Maßnahmen ergreifen

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



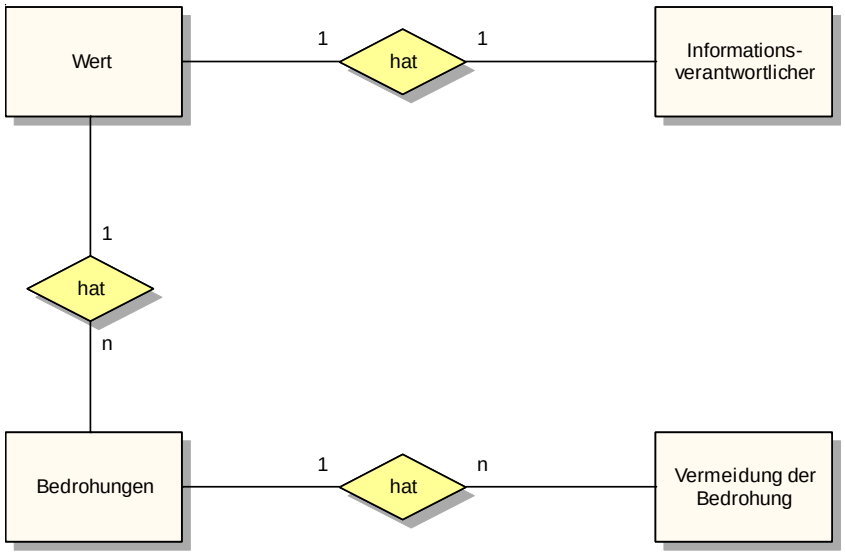
eERM: 4.2.1.f.2 Bewusste, objektive Akzeptanz der Risiken laut Politik

Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung

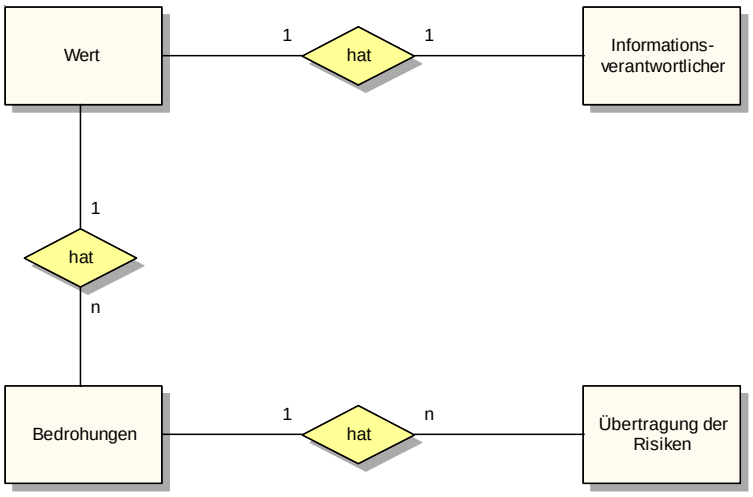


eERM: 4.2.1.f.3 Vermeidung von Risiken

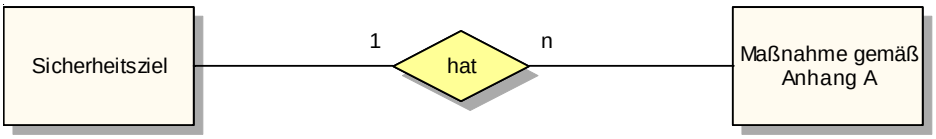
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



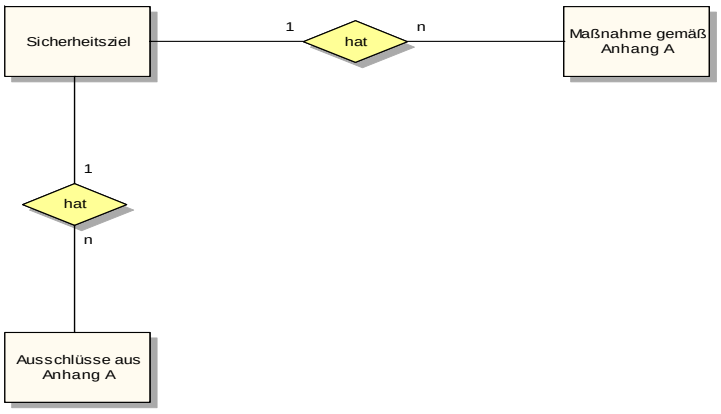
eERM: 4.2.1.f.4 Übertragung von Risiken auf beteiligte Parteien
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



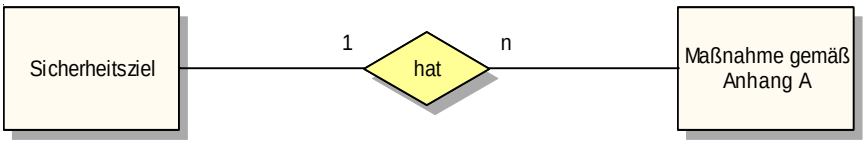
eERM: 4.2.1.g Auswahl der Sicherheitsziele und Maßnahmen (Anhang A)
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



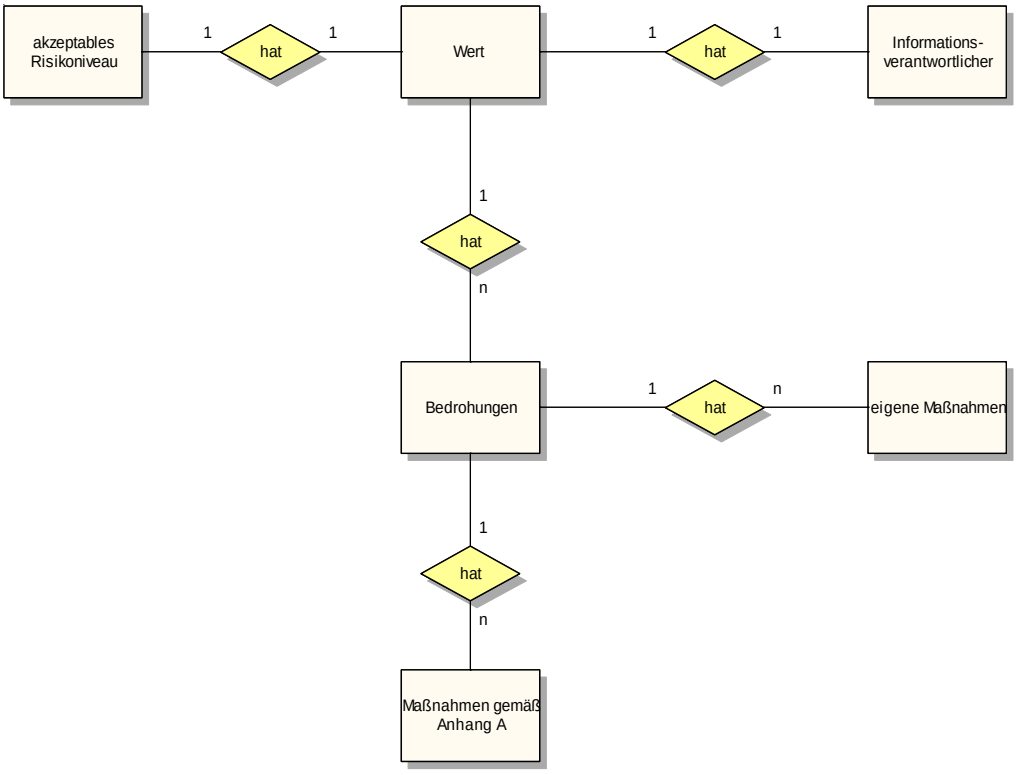
eERM: 4.2.1.h Aufzeichnung jeglicher Ausschlüsse aus Anhang A
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



eERM: 4.2.1.h Dokumentation gewählter Sicherheitsziele und Maßnahmen
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung

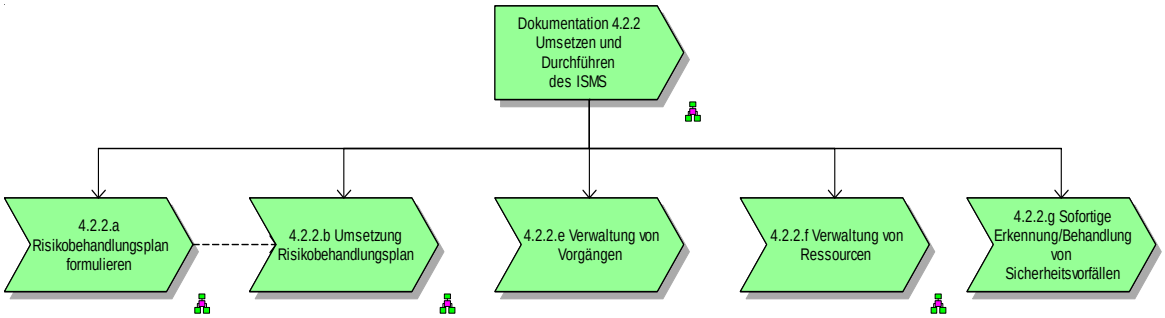


eERM: 5.1.f Entscheidung über akzeptables Risikioniveau
Gruppenpfad:\\Referenzmodell\4.2.1 Festlegen des ISMS\Arbeitssicht\DV-Konzept Risikoeinschätzung /-bewertung



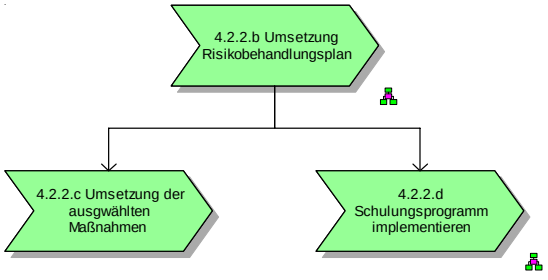
4.2.2 Umsetzen und Durchführen des ISMS

Wertschöpfungskettendiagramm: 4.2.2 Umsetzen und Durchführen des ISMS
Gruppenpfad:\\Referenzmodell\4.2.2 Umsetzen und Durchführen des ISMS

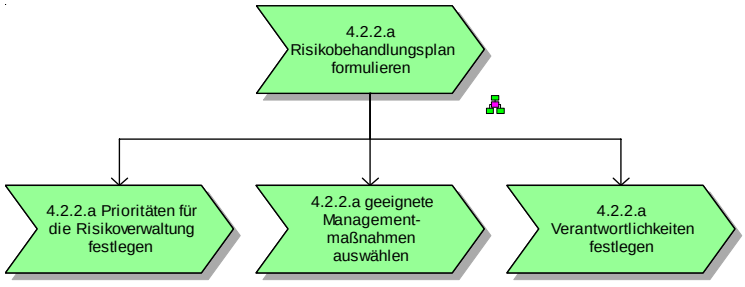


keine Modelle in Gruppe \Referenzmodell\4.2.2 Umsetzen und Durchführen des ISMS\Arbeitssicht

Wertschöpfungskettendiagramm: 4.2.2.b Umsetzung Risikobehandlungsplan
Gruppenpfad:\\Referenzmodell\4.2.2 Umsetzen und Durchführen des ISMS\Managementsicht

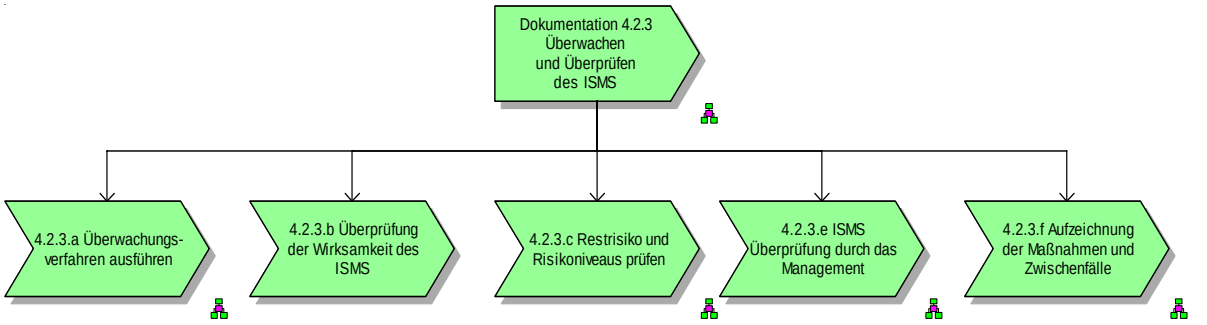


Wertschöpfungskettendiagramm: Risikobehandlungsplan formulieren
Gruppenpfad:\\Referenzmodell\4.2.2 Umsetzen und Durchführen des ISMS\ Managementsicht

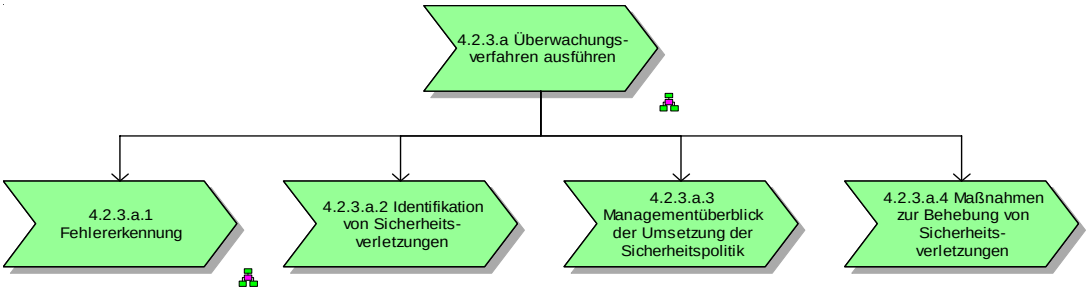


4.2.3 Überwachen und Überprüfen des ISMS

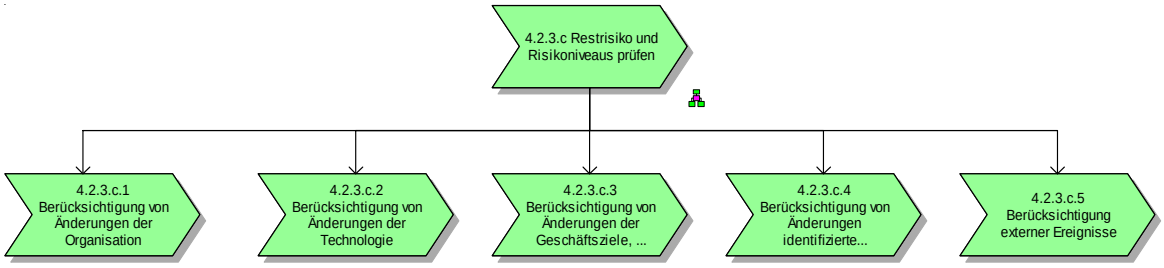
Wertschöpfungskettendiagramm: 4.2.3 Überwachen und Überprüfen des ISMS
Gruppenpfad:\\Referenzmodell\4.2.3 Überwachen und Überprüfen des ISMS



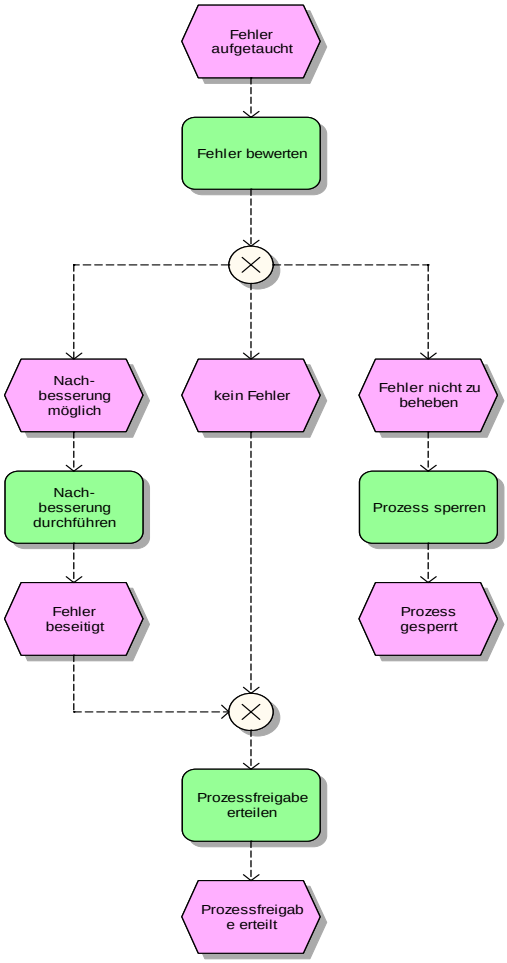
Wertschöpfungskettendiagramm: 4.2.3.a Überwachungsverfahren ausführen
Gruppenpfad:\\Referenzmodell\4.2.3 Überwachen und Überprüfen des ISMS\ Managmentsicht



Wertschöpfungskettendiagramm: 4.2.3.c Restrisiko und Risikoniveaus prüfen
Gruppenpfad:\\Referenzmodell\4.2.3 Überwachen und Überprüfen des ISMS\Managmentsicht

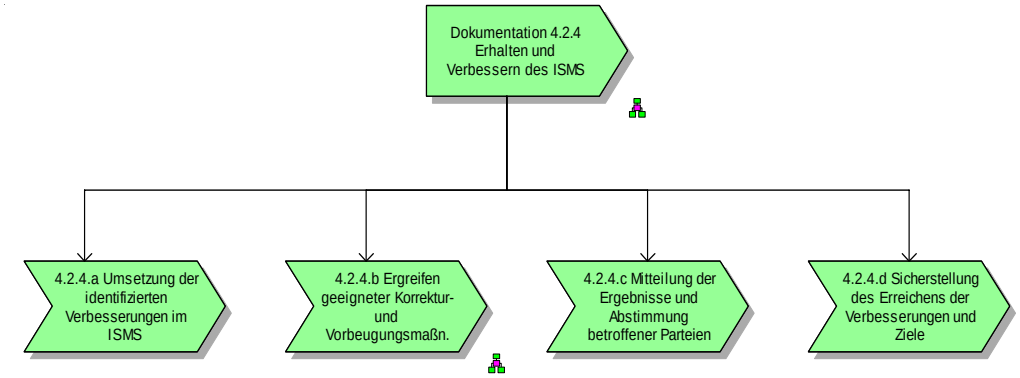


EPK: Fehler erkennen und behandeln
Gruppenpfad:\\Referenzmodell\4.2.3 Überwachen und Überprüfen des ISMS\Arbeitssicht



4.2.4 Aufrechterhalten und Verbessern des ISMS

Wertschöpfungskettendiagramm: 4.2.4 Aufrechterhalten und Verbessern des ISMS
Gruppenpfad:\\Referenzmodell\4.2.4 Aufrechterhalten und Verbessern des ISMS

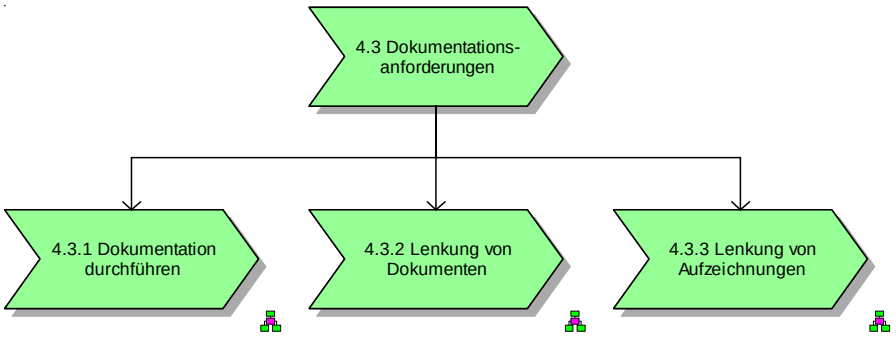


keine Modelle in Gruppe \Referenzmodell\4.2.4 Aufrechterhalten und Verbessern des ISMS\Arbeitssicht

keine Modelle in Gruppe \Referenzmodell\4.2.4 Aufrechterhalten und Verbessern des ISMS\Managementsicht

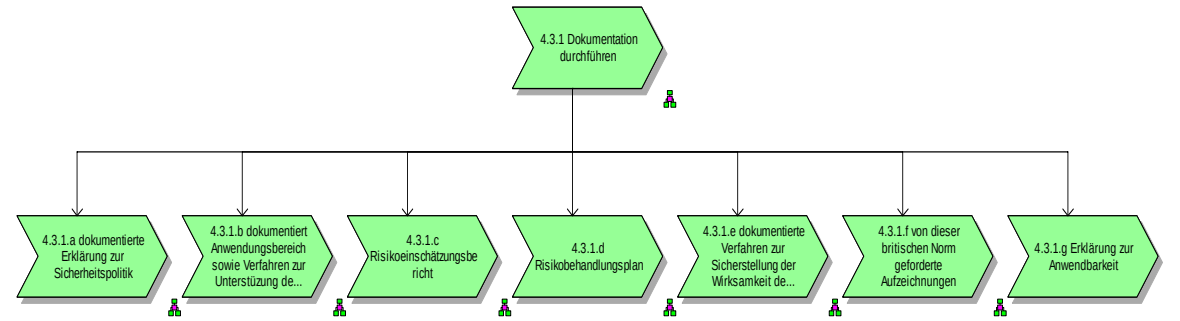
4.3 Dokumentationsanforderungen

Wertschöpfungskettendiagramm: 4.3 Dokumentationsanforderungen
Gruppenpfad:\\Referenzmodell\4.3 Dokumentationsanforderungen



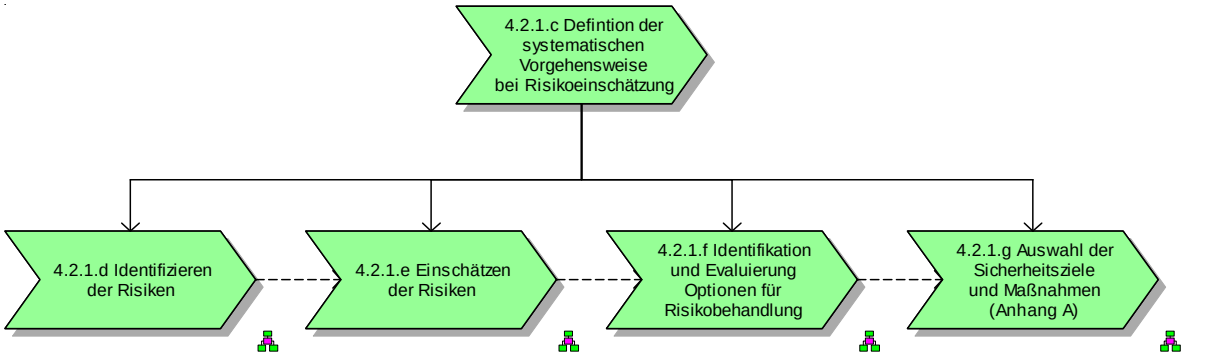
Wertschöpfungskettendiagramm: 4.3.1 Dokumentation

Gruppenpfad:\\Referenzmodell\4.3 Dokumentationsanforderungen\Managementsicht



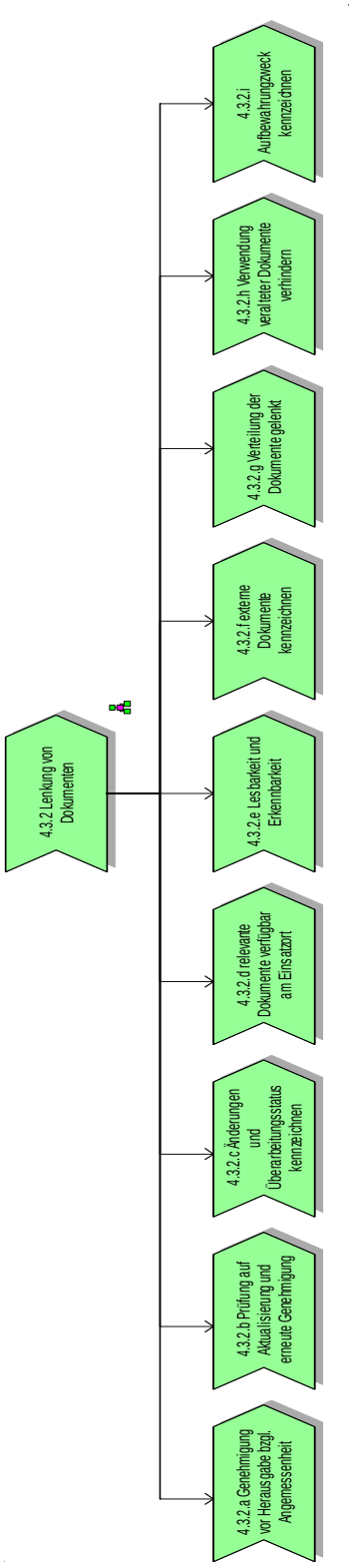
Wertschöpfungskettendiagramm: 4.3.1.c Risikoeinschätzungsbericht

Gruppenpfad:\\Referenzmodell\4.3 Dokumentationsanforderungen\Managementsicht

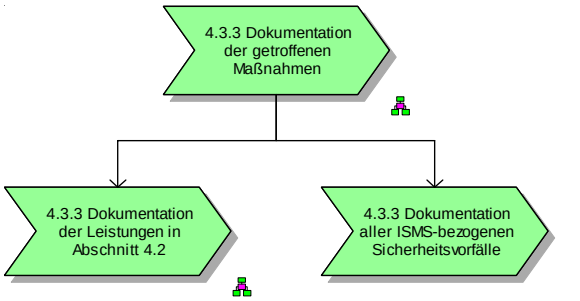


Wertschöpfungskettendiagramm: 4.3.2 Lenkung von Dokumenten

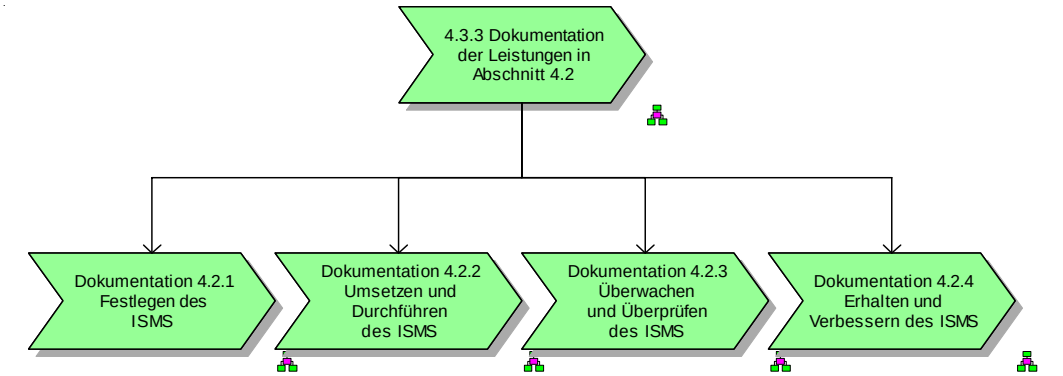
Gruppenpfad:\\Referenzmodell\4.3 Dokumentationsanforderungen\Managementsicht



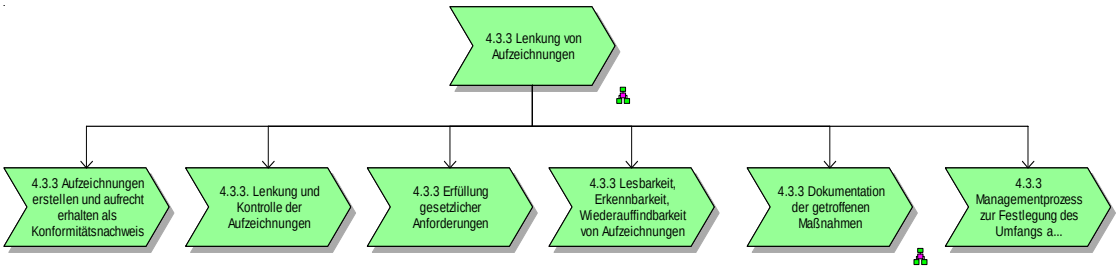
Wertschöpfungskettendiagramm: 4.3.3 Dokumentation der getroffenen Maßnahmen
Gruppenpfad:\\Referenzmodell\4.3 Dokumentationsanforderungen\Managementsicht



Wertschöpfungskettendiagramm: 4.3.3 Dokumentation der Leistungen in Abschnitt 4.2
Gruppenpfad:\\Referenzmodell\4.3 Dokumentationsanforderungen\Managementsicht



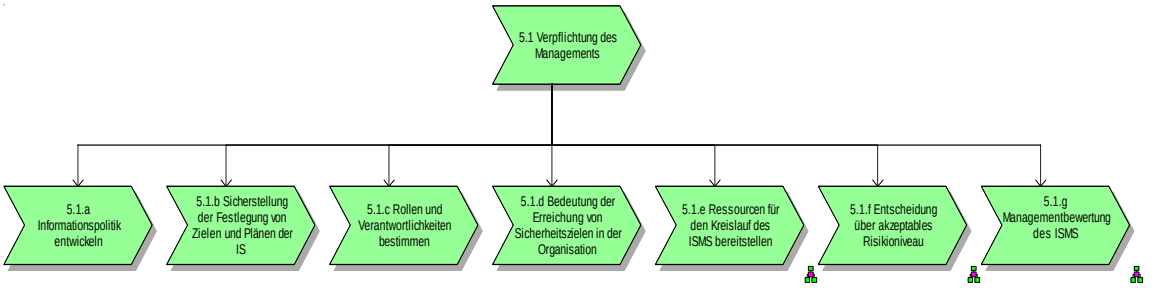
Wertschöpfungskettendiagramm: 4.3.3 Lenkung von Aufzeichnungen
Gruppenpfad:\\Referenzmodell\4.3 Dokumentationsanforderungen\Managementsicht



keine Modelle in Gruppe \Referenzmodell\4.3 Dokumentationsanforderungen\Arbeitssicht

5.1 Verpflichtung des Managements

Wertschöpfungskettendiagramm: 5.1. Verpflichtung des Managements
Gruppenpfad:\\Referenzmodell\5.1 Verpflichtung des Managements

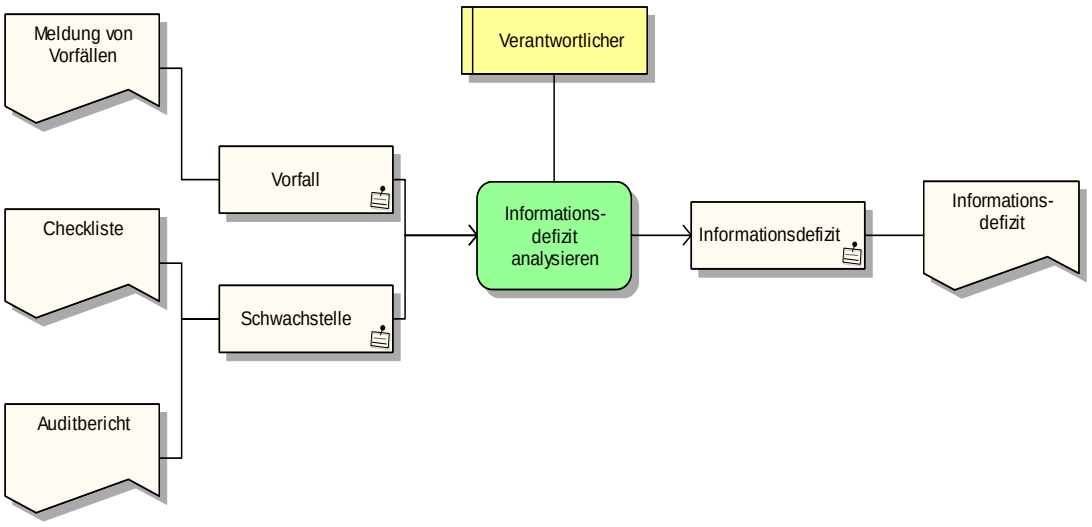


keine Modelle in Gruppe \Referenzmodell\5.1 Verpflichtung des Managements\Managementsicht

keine Modelle in Gruppe \Referenzmodell\5.1 Verpflichtung des Managements\Arbeitssicht

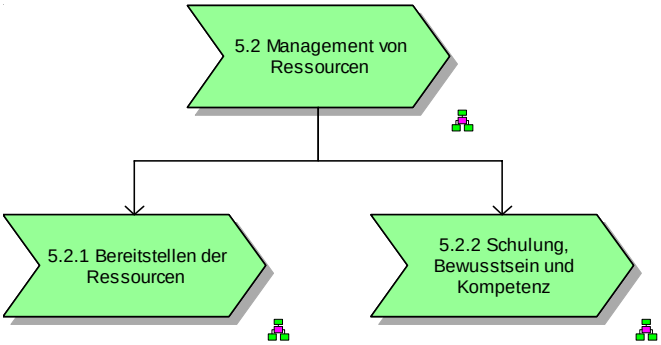
5.2 Ressourcenmanagementprozesse

Funktionszuordnungsdiagramm: Informationsdefizit analysieren
Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



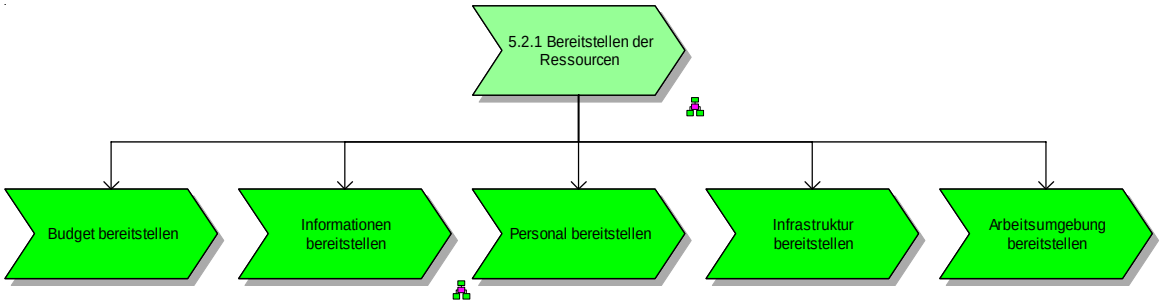
Wertschöpfungskettendiagramm: 5.2 Management von Ressourcen

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse



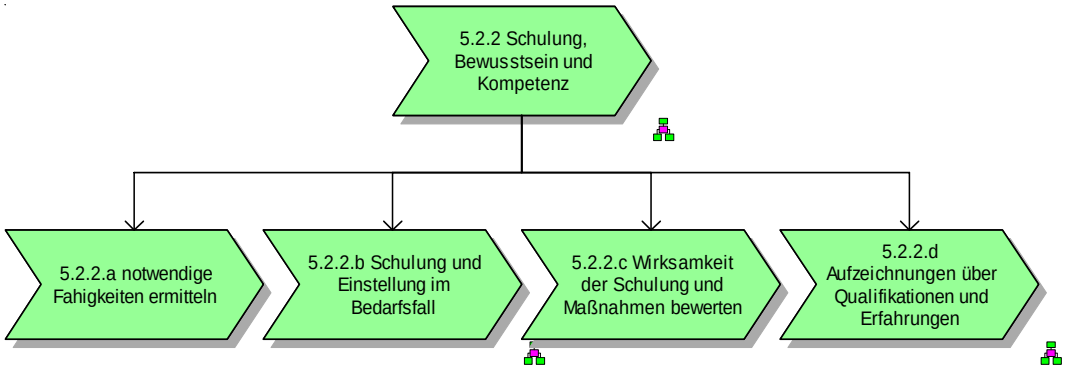
Wertschöpfungskettendiagramm: 5.2.1 Bereitstellen der Ressourcen

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Managmentsicht



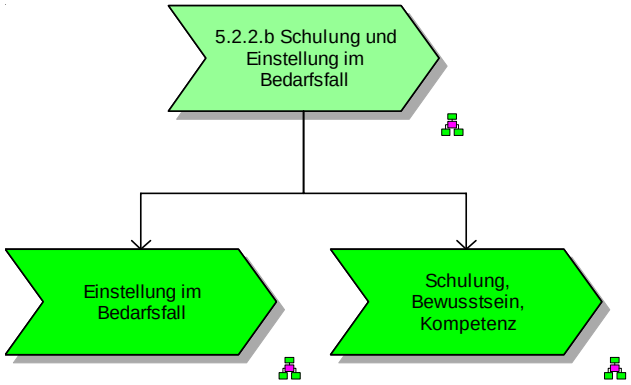
Wertschöpfungskettendiagramm: 5.2.2 Schulung, Bewusstsein und Kompetenz

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Managmentsicht



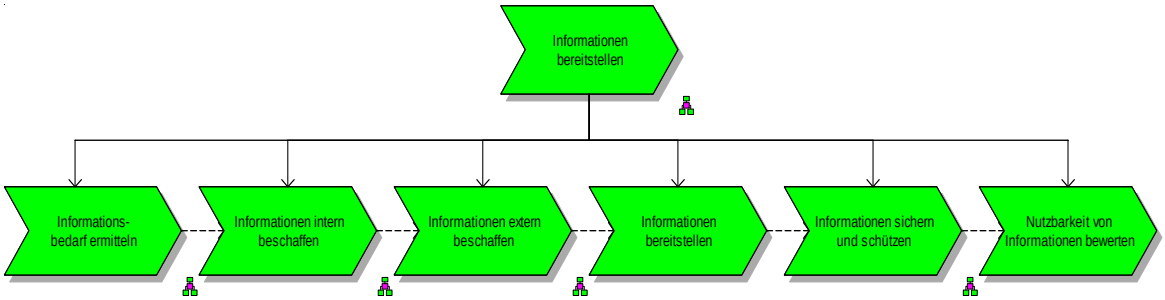
Wertschöpfungskettendiagramm: 5.2.2.b Schulung und Einstellung im Bedarfsfall

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Managmentsicht



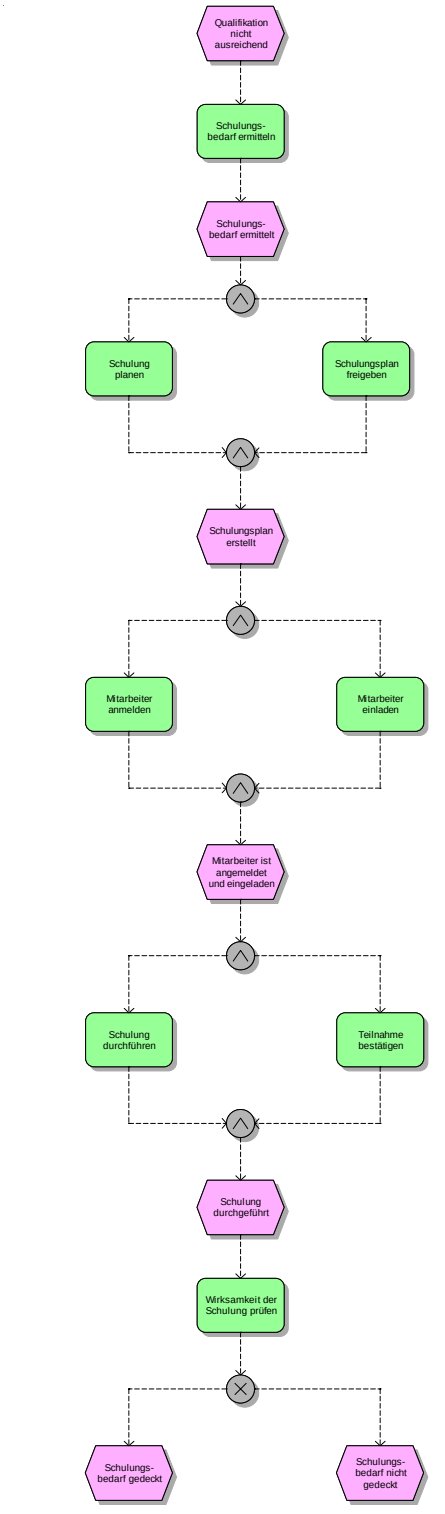
Wertschöpfungskettendiagramm: Informationen

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Managmentsicht



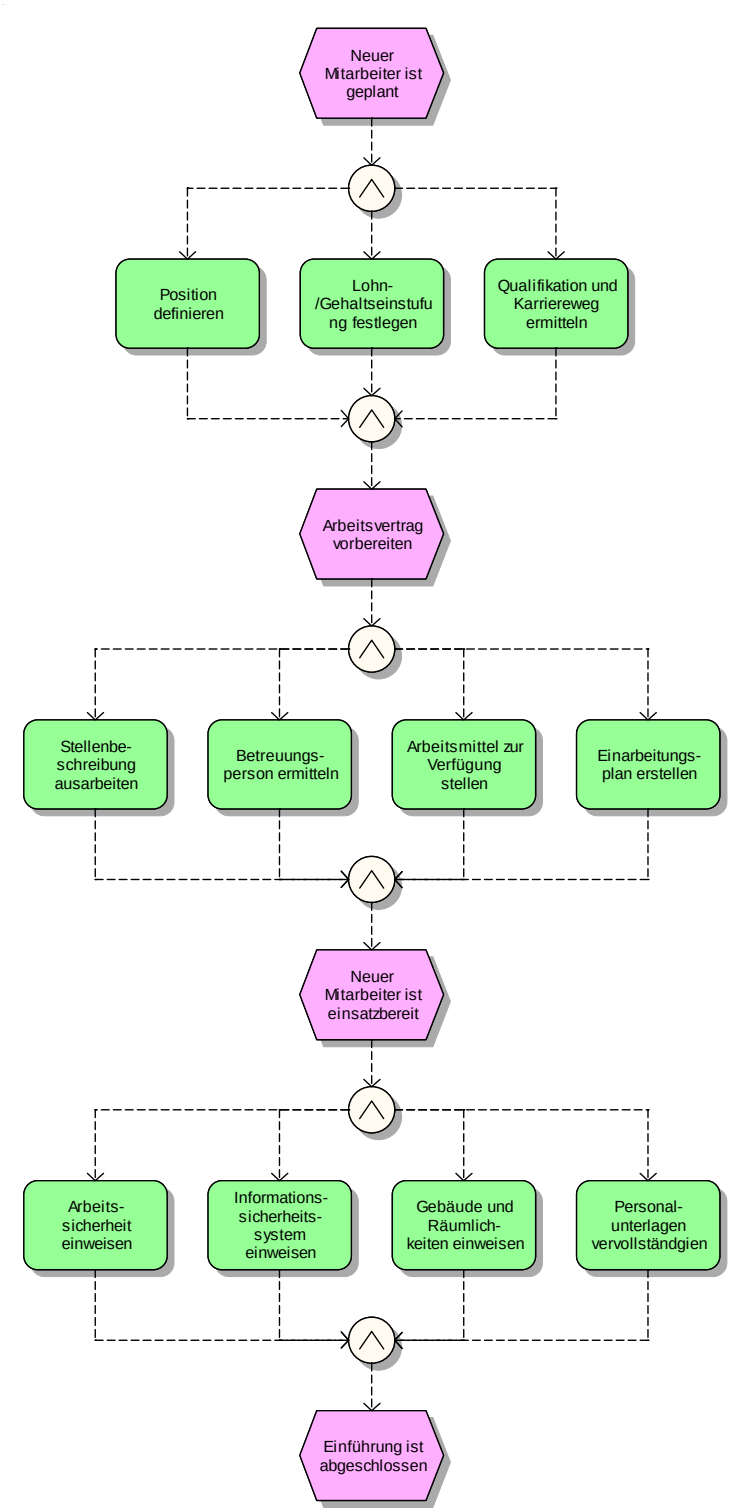
EPK: 5.2.2 Schulung, Bewusstsein, Kompetenz

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



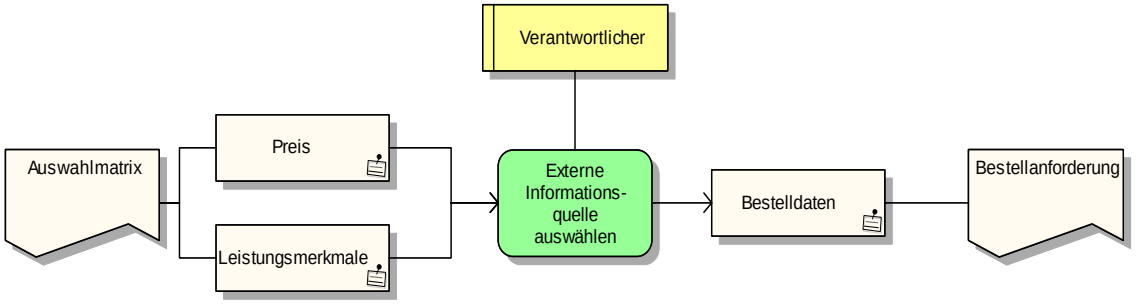
EPK: Einstellung im Bedarfsfall

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



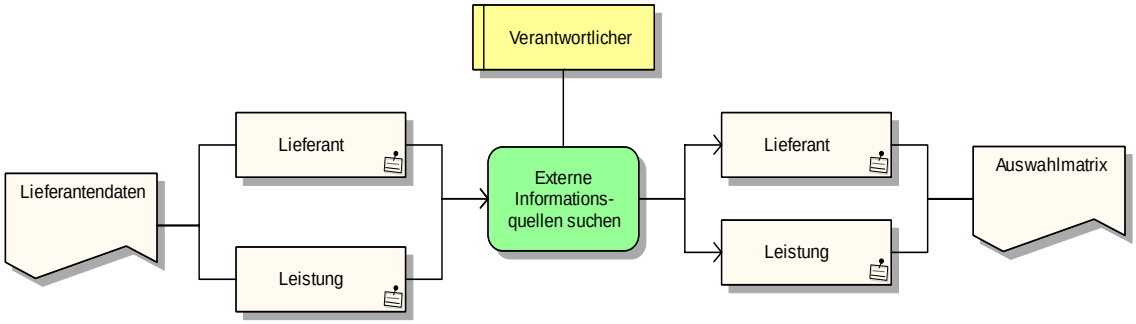
Funktionszuordnungsdiagramm: Externe Informationsquelle auswählen

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



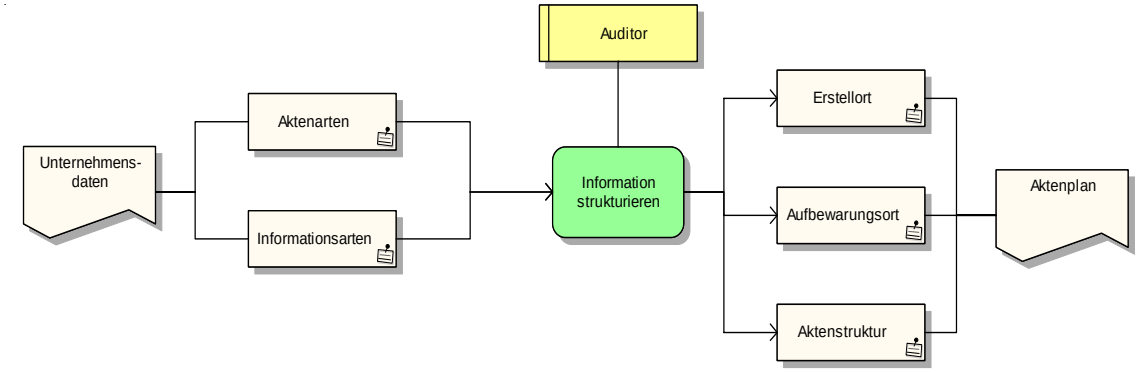
Funktionszuordnungsdiagramm: Externe Informationsquellen suchen

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



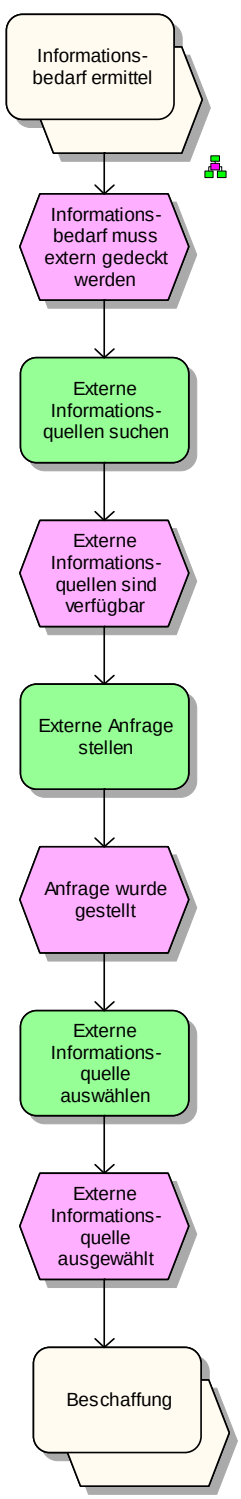
Funktionszuordnungsdiagramm: Information strukturieren

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



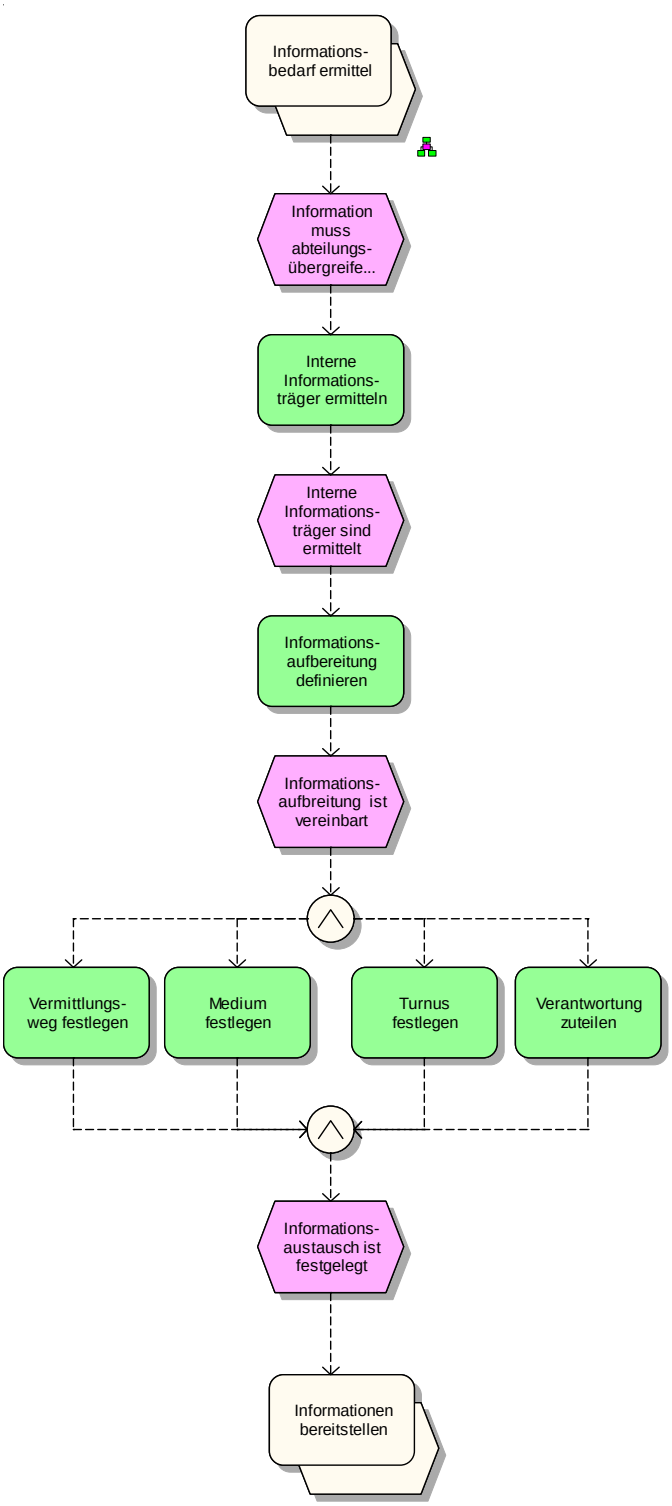
EPK: Informationen extern beschaffen

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



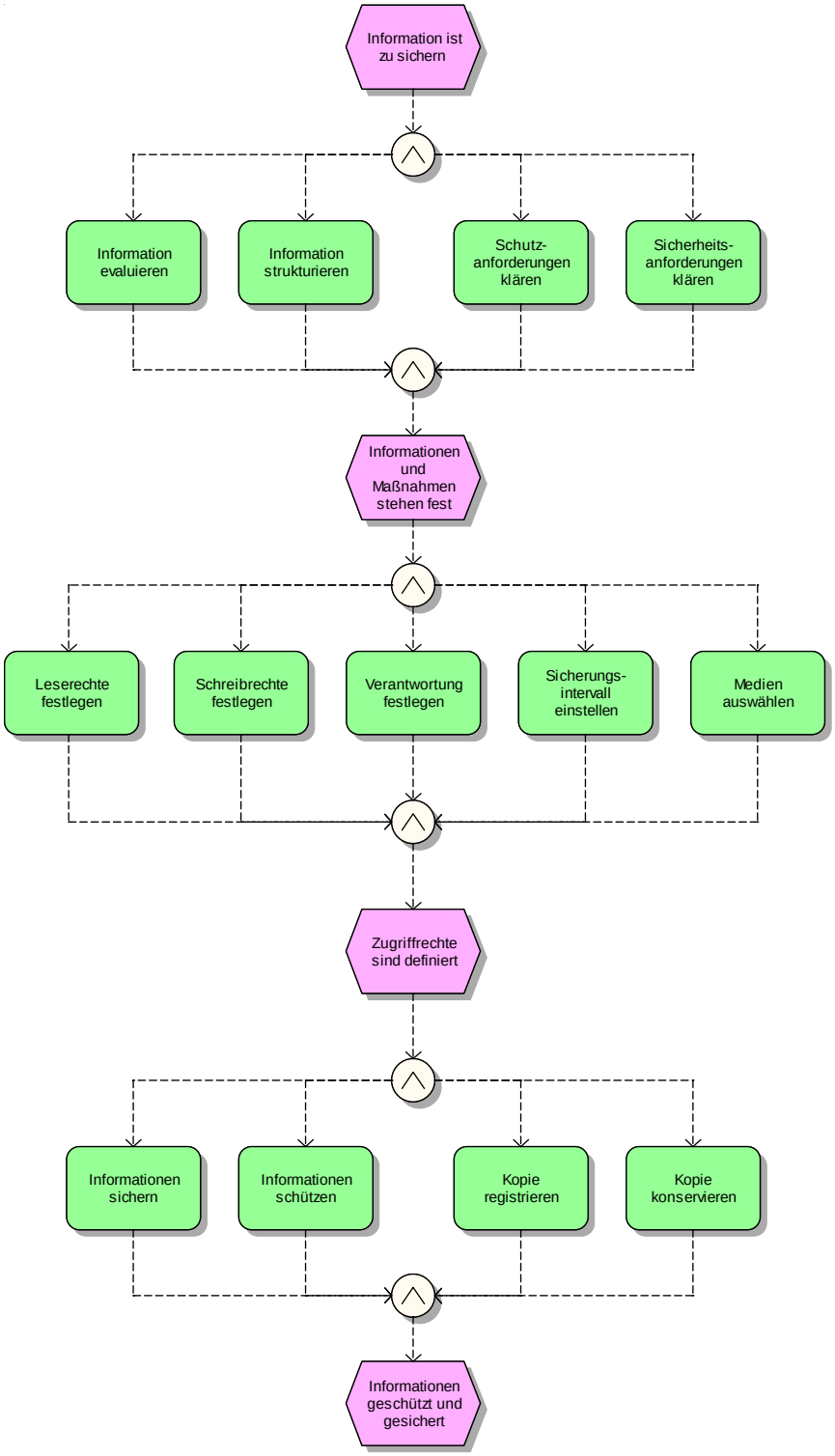
EPK: Informationen intern beschaffen

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



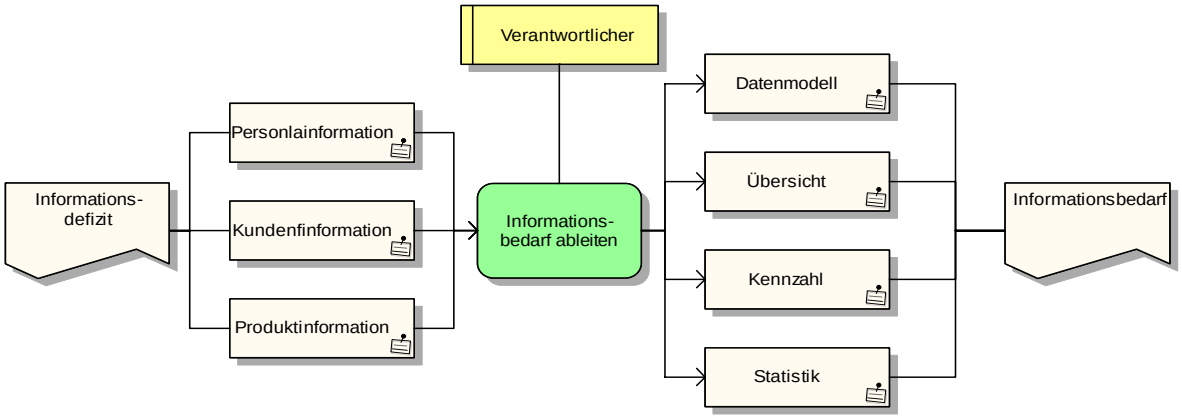
EPK: Informationen sichern und schützen

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



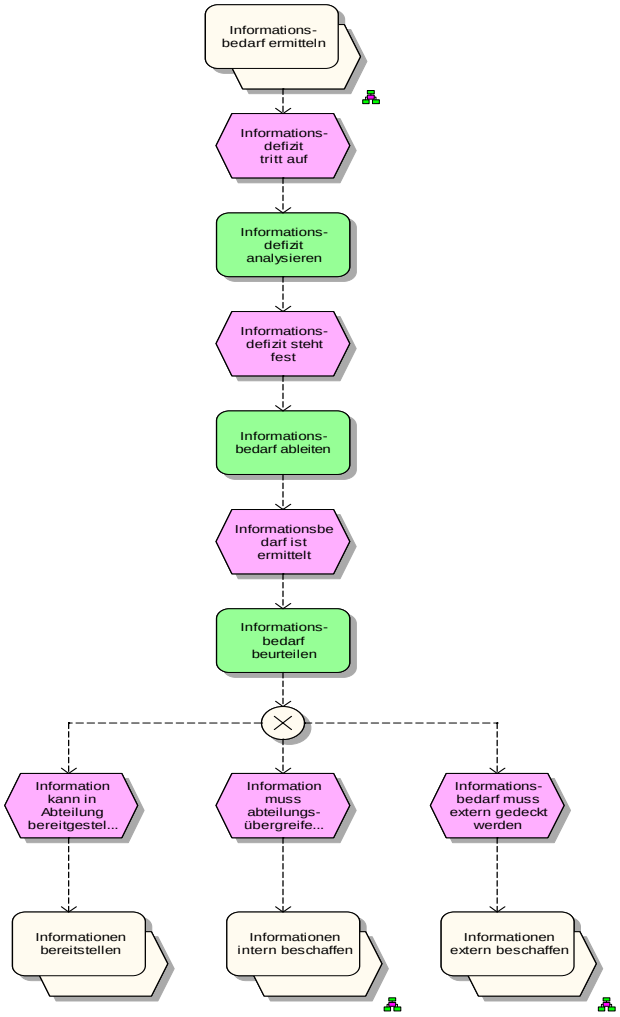
Funktionszuordnungsdiagramm: Informationsbedarf ableiten

Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



EPK: Informationsbedarf ermitteln

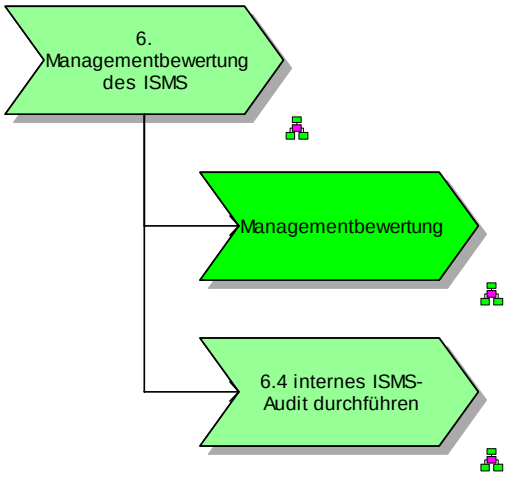
Gruppenpfad:\\Referenzmodell\5.2 Ressourcenmanagementprozesse\Arbeitssicht



6. Managementbewertung des ISMS

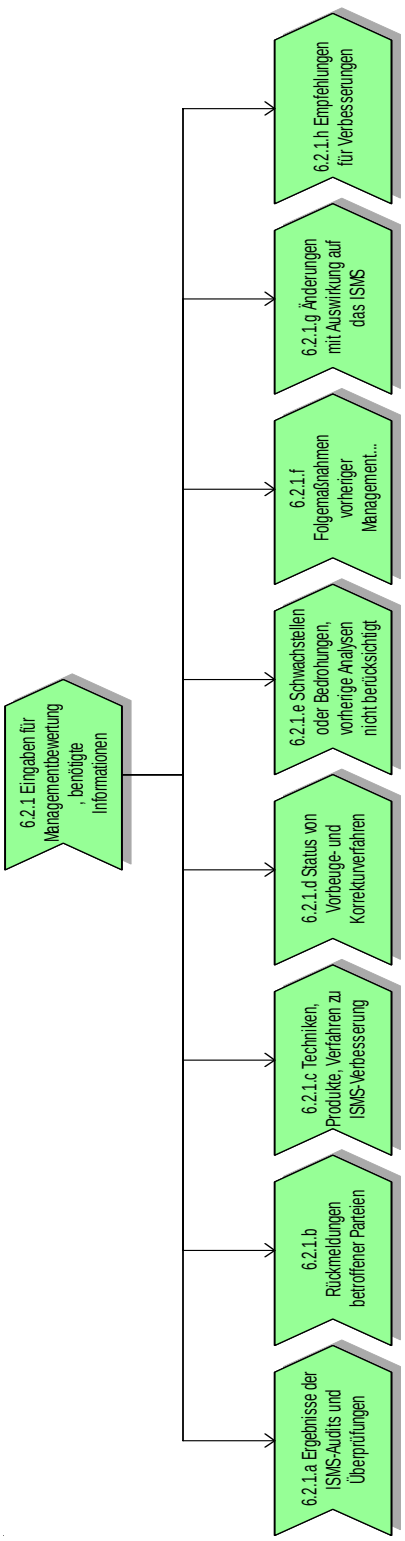
Wertschöpfungskettendiagramm: 6. Managementbewertung des ISMS

Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS

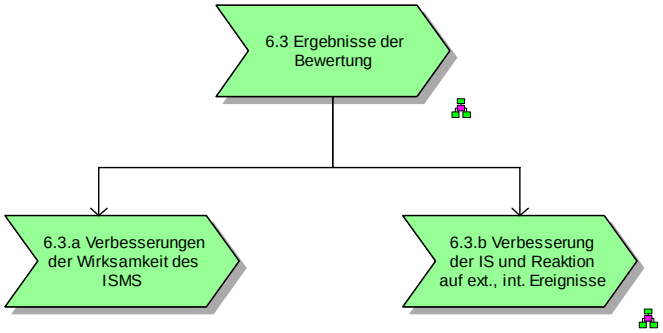


Wertschöpfungskettendiagramm: 6.2 Informationsbedarf

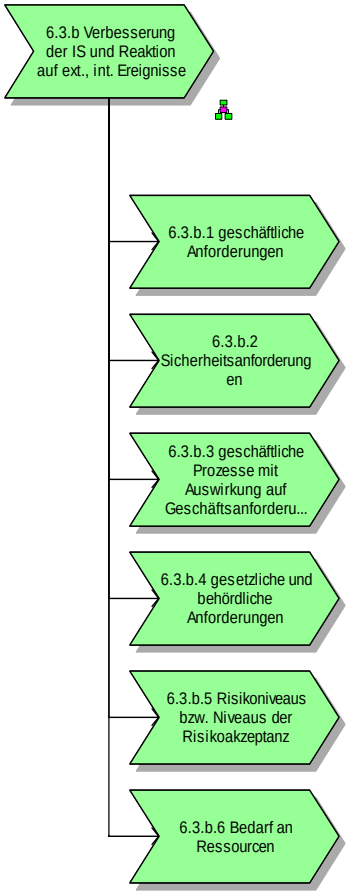
Gruppenpfad:\\Referenzmodell\6.Managementbewertung des ISMS\ Managementsicht



Wertschöpfungskettendiagramm: 6.3 Ergebnisse der Bewertung
Gruppenpfad:\\Referenzmodell\6.Managementbewertung des ISMS\ Managementsicht

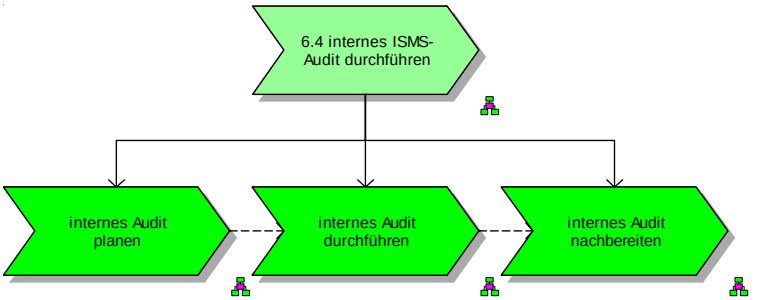


Wertschöpfungskettendiagramm: 6.3.b Verbesserung der IS und Reaktion auf ext., int. Ereignisse
Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Managementsicht



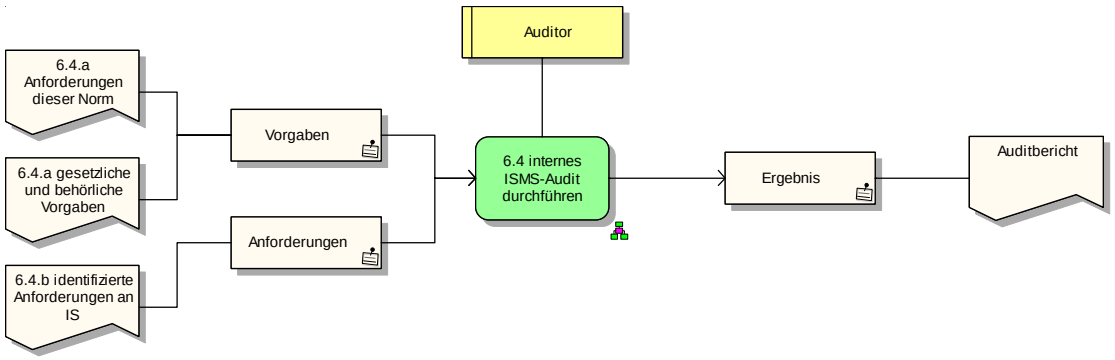
Wertschöpfungskettendiagramm: 6.4 internes ISMS-Audit

Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Managementsicht



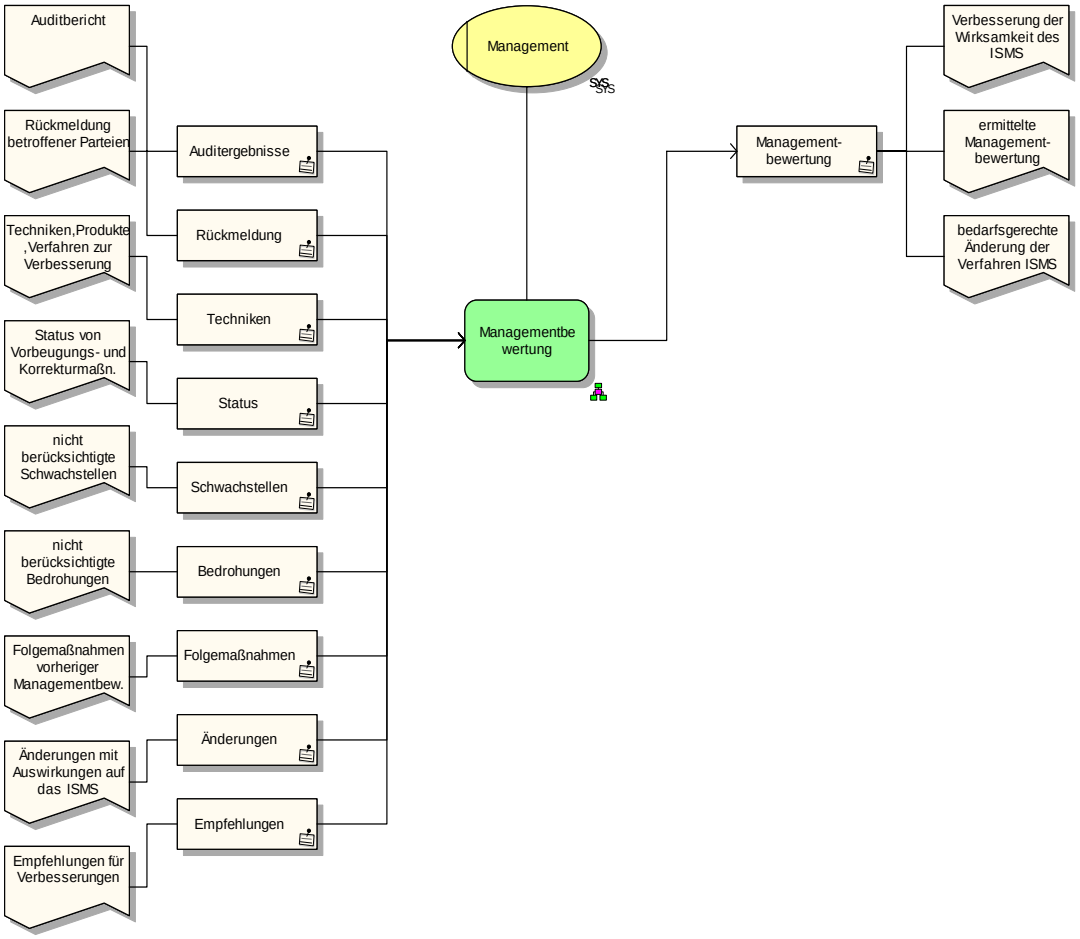
Funktionszuordnungsdiagramm: 6.4 internes ISMS-Audit

Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Managementsicht



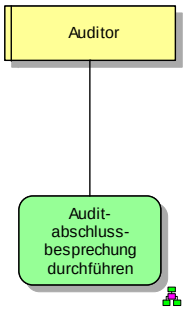
Funktionszuordnungsdiagramm: Managementbewertung

Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Managementsicht

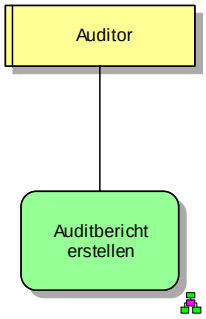


Funktionszuordnungsdiagramm: Auditabschlussbesprechung durchführen

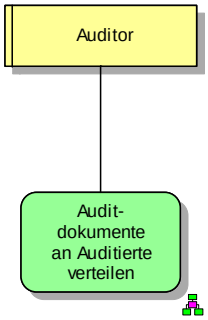
Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Arbeitssicht



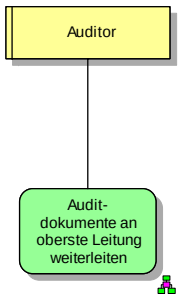
Funktionszuordnungsdiagramm: Auditbericht erstellen
Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Arbeitssicht



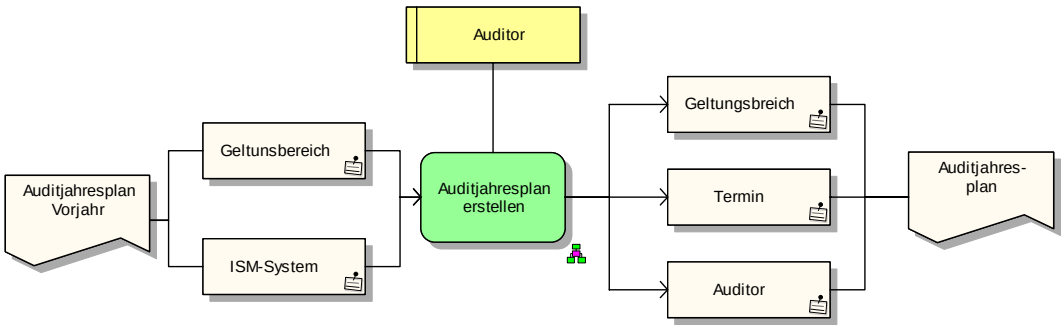
Funktionszuordnungsdiagramm: Auditdokumente an Auditierte verteilen
Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Arbeitssicht



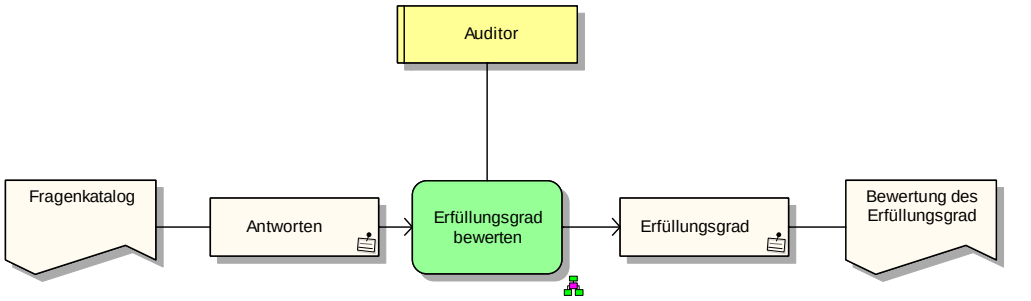
Funktionszuordnungsdiagramm: Auditdokumente an oberste Leitung weiterleiten
Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Arbeitssicht



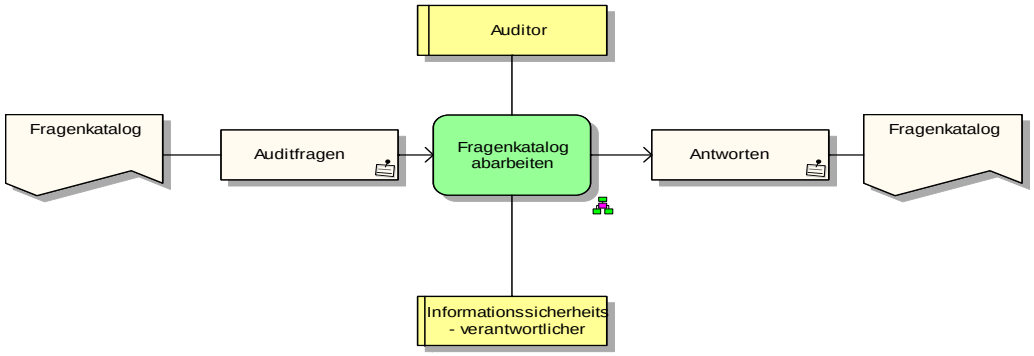
Funktionszuordnungsdiagramm: Auditjahresplan erstellen
Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Arbeitssicht



Funktionszuordnungsdiagramm: Erfüllungsgrad bewerten
Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Arbeitssicht

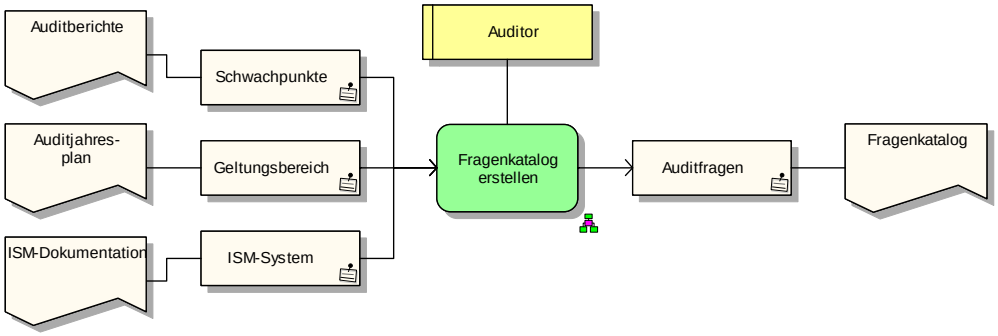


Funktionszuordnungsdiagramm: Fragenkatalog abarbeiten
Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Arbeitssicht



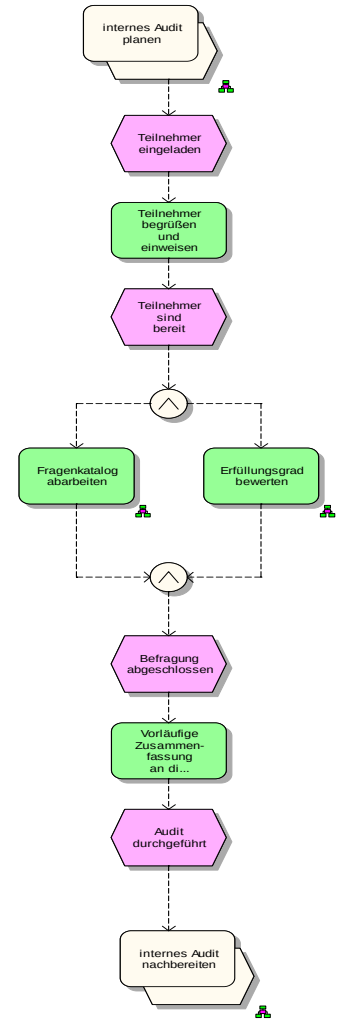
Funktionszuordnungsdiagramm: Fragenkatalog erstellen

Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Arbeitssicht



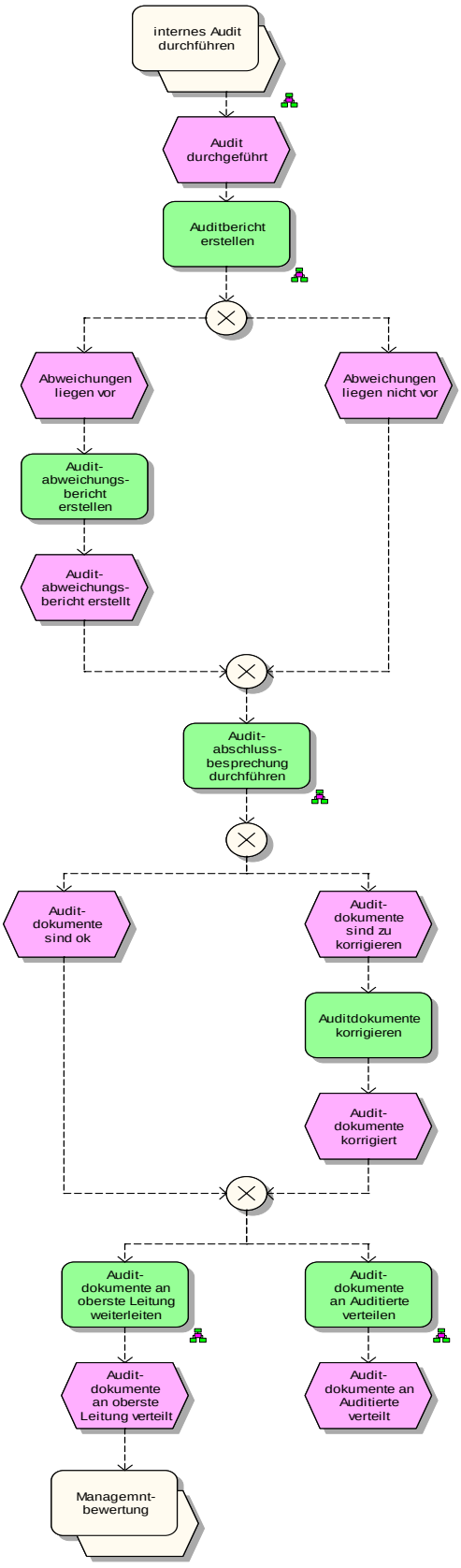
EPK: internes Audit durchführen

Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\Arbeitssicht



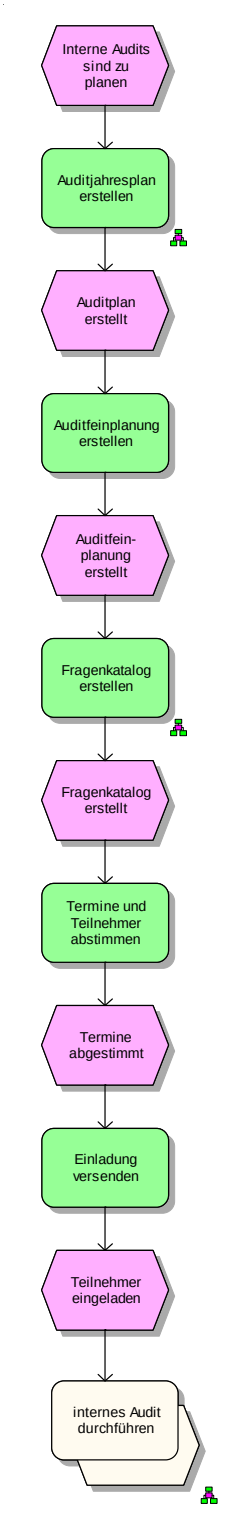
EPK: internes Audit nachbereiten

Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\Arbeitssicht



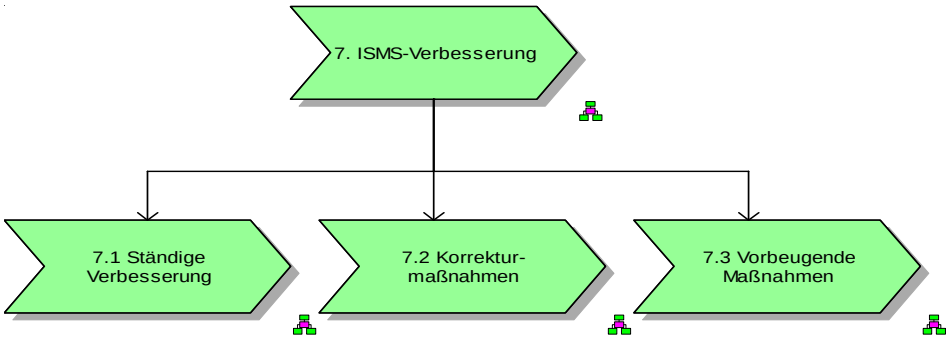
EPK: internes Audit planen

Gruppenpfad:\\Referenzmodell\6. Managementbewertung des ISMS\ Arbeitssicht



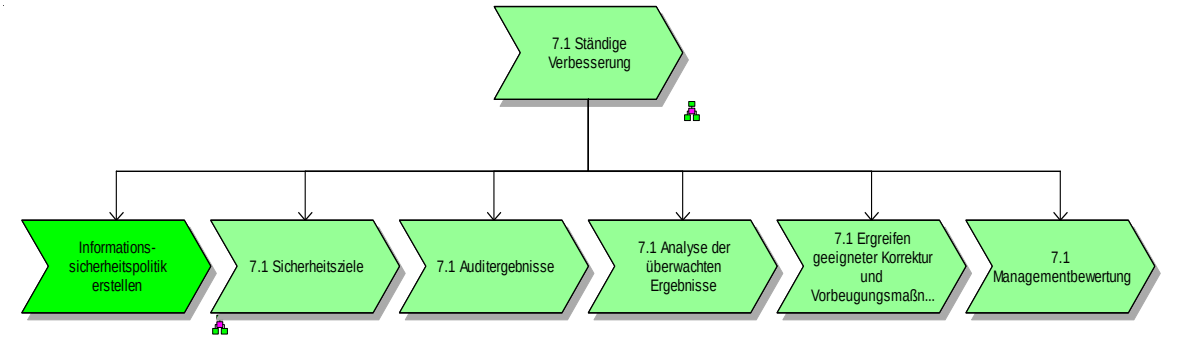
7. ISMS Verbesserung

Gruppenpfad:\\Referenzmodell\7. ISMS-Verbesserung



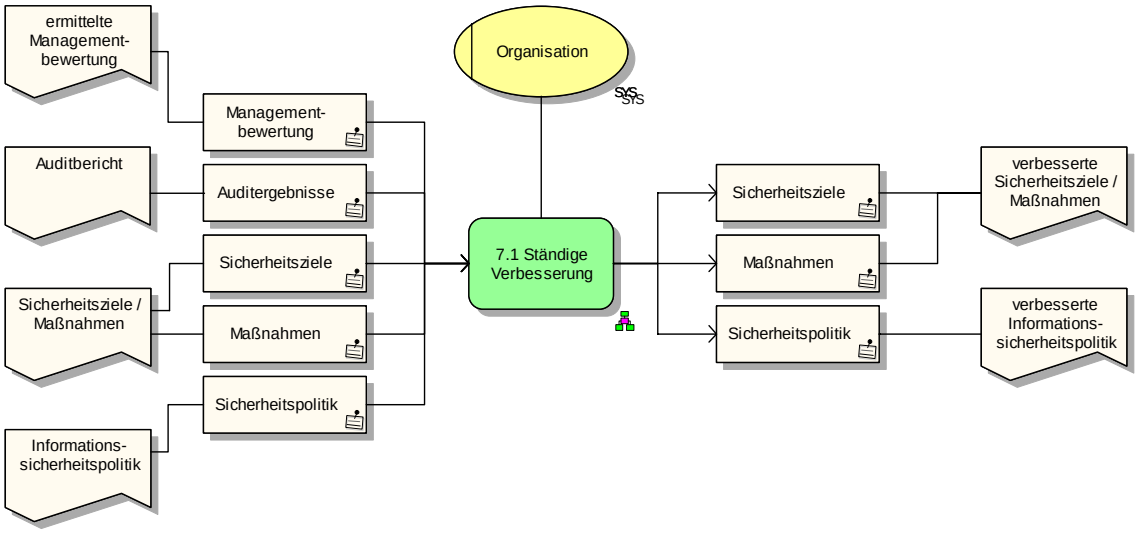
Wertschöpfungskettendiagramm: 7.1 Ständige Verbesserung

Gruppenpfad:\\Referenzmodell\7. ISMS-Verbesserung\Managementsicht



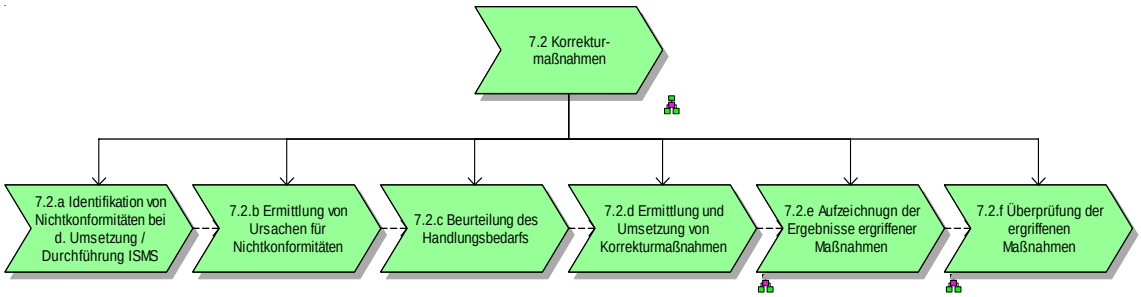
Funktionszuordnungsdiagramm: 7.1 Ständige Verbesserung

Gruppenpfad:\\Referenzmodell\7. ISMS-Verbesserung\Managementsicht



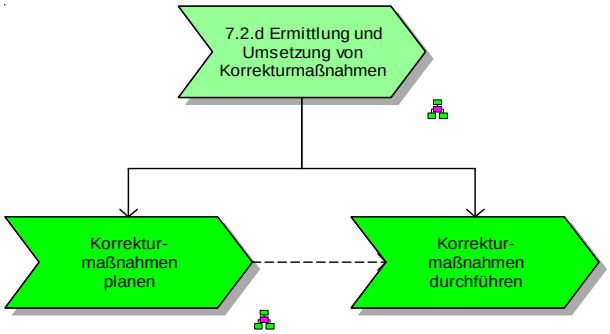
Wertschöpfungskettendiagramm: 7.2 Korrekturmaßnahmen

Gruppenpfad:\\Referenzmodell\7. ISMS-Verbesserung\Managementsicht



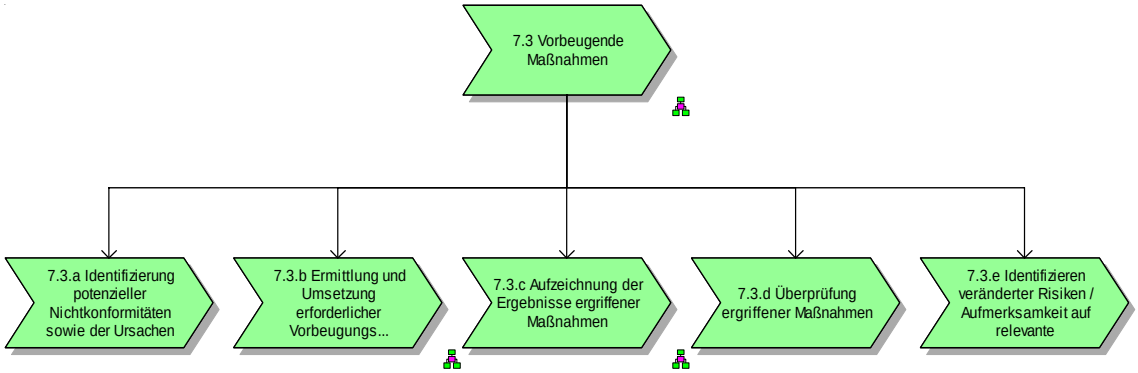
Wertschöpfungskettendiagramm: 7.2.d Ermittlung und Umsetzung von Korrekturmaßnahmen

Gruppenpfad:\\Referenzmodell\7. ISMS-Verbesserung\Managementsicht



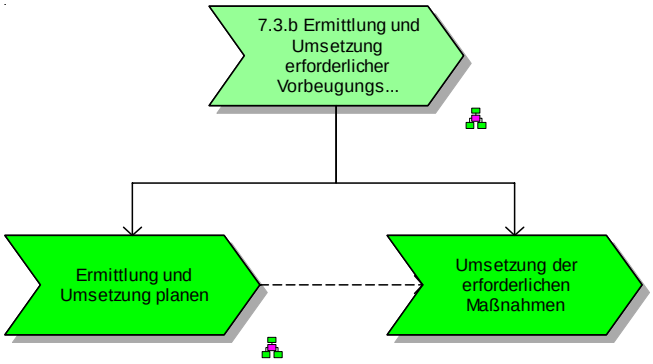
Wertschöpfungskettendiagramm: 7.3 Vorbeugende Maßnahmen

Gruppenpfad:\\Referenzmodell\7. ISMS-Verbesserung\Managementsicht



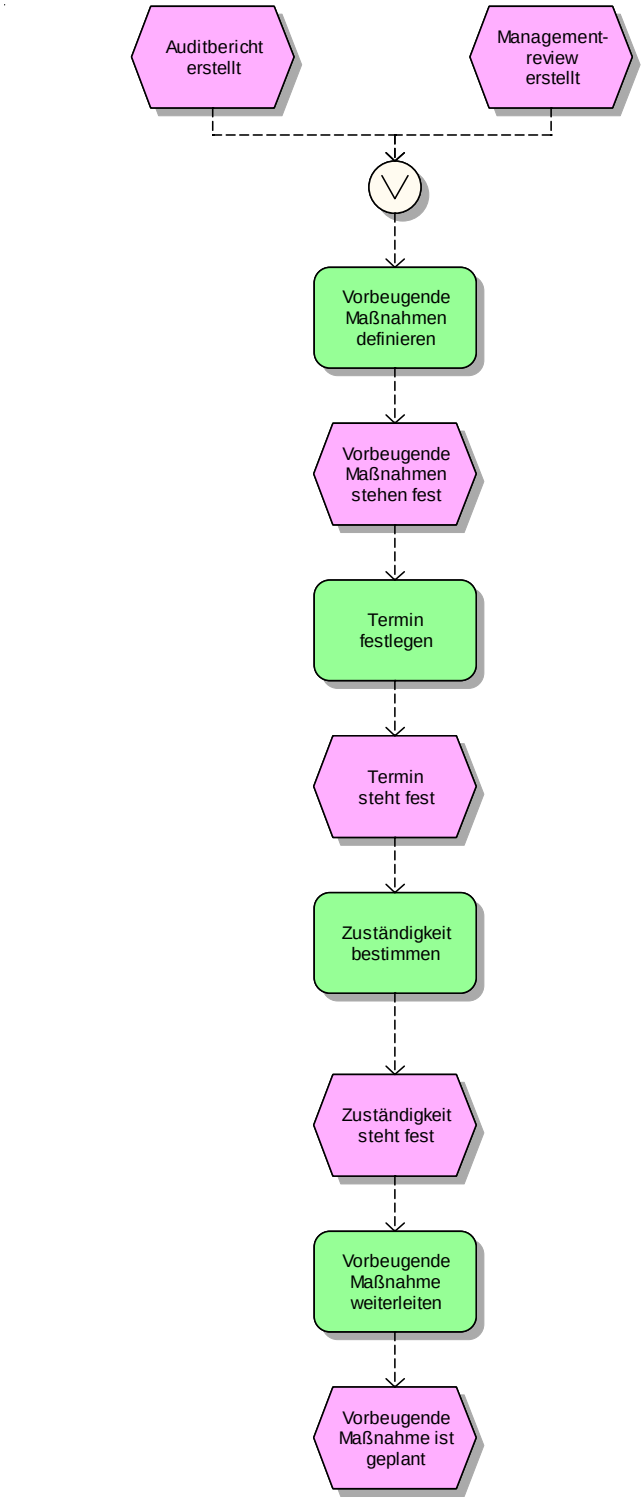
Wertschöpfungskettendiagramm: 7.3.b Ermittlung und Umsetzung erforderlicher Vorbeugungs- maßnahmen

Gruppenpfad:\\Referenzmodell\7. ISMS-Verbesserung\Managementsicht



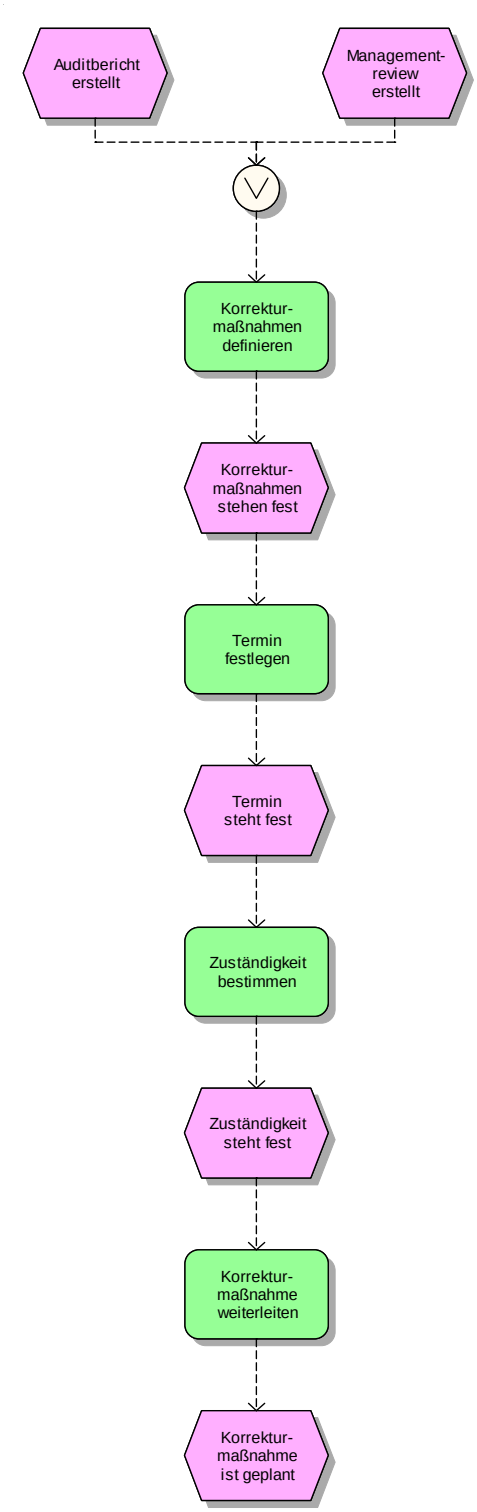
EPK: Ermittlung und Umsetzung planen

Gruppenpfad:\\Referenzmodell\7. ISMS-Verbesserung\Arbeitssicht



EPK: Korrekturmaßnahmen planen

Gruppenpfad:\\Referenzmodell\7. ISMS-Verbesserung\Arbeitssicht



Quellenverzeichnis

Ahrens, Volker: Allgemeine und ethische Grundlagen von Managementsystemen, in: Ahrens, Volker; Hofmann-Kamensky, Matthias: Integration von Managementsystemen, Ansätze für die Praxis, München 2001, S. 3 – 17

Becker, Jörg; Vossen, Gottfried: Geschäftsprozessmodellierung und Workflow-Management, Eine Einführung, in: Vossen, Gottfried; Becker, Jörg: Geschäftsprozeß-modellierung und Workflow-Management, Modelle, Methoden, Werkzeuge, Bonn u.a. 1996, S. 17 – 26

Bishop, Matt: Computer Security: Art and Science, 4. Auflage, Boston 2003

Böhm, Rolf; Wegner, Sven: Methoden und Techniken der System-Entwicklung, 2.Auflage, Zürich 1996

British Standards Institution BSI (Hrsg.): BS 7799-2:2002 Informationssicherheits-Managementsysteme - Spezifikation mit Anleitung zur Anwendung, London 2002

Brosius, Gerhard: Access 2000 professionell - Datenbank-Management mit Office 2000, München 1999

Bruhn, Manfred: Qualitätsmanagement für Dienstleistungen, Grundlagen, Konzepte, Methoden, 5.Auflage, Heidelberg u. a. 2004

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch, Berlin 2004, http://www.bsi.de/gshb/deutsch/index.htm (2006-02-12)

Bundesamt für Sicherheit in der Informationstechnik: ITSEC, Berlin 1998
http://www.bsi.de/zertifiz/itkrit/itsec-dt.pdf (2006-02-12)

Callio Technologies (Hrsg): o. V., http://www.callio.com/bs7799/id,361 (2006-02-12)

Deutsches Institut für Normung DIN (Hrsg.): DIN EN ISO 9000:2000 Qualitätsmanagementsysteme, Grundlagen und Begriffe, Berlin 2000

Deutsches Institut für Normung DIN (Hrsg.): DIN EN ISO 9001:2000 Qualitätsmanagementsysteme, Anforderungen, Berlin 2000

Görtz, Horst; Stolp, Jutta: Informationssicherheit in Unternehmen - Sicherheitskonzepte und -lösungen in der Praxis, Bonn u. a. 1999

Grief, Jürgen: ARIS in IT-Projekten – Zielgerichtet zum Projekterfolg, durch fundiertes ARIS-Wissen, jede Menge Praxiserfahrung, erprobte Lösungen, Wiesbaden 2005

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

Hornberger, Werner; Schneider, Jürgen: Sicherheit und Datenschutz mit SAP-Systemen – Maßnahmen für die betriebliche Praxis, Bonn 2000

Hunter, John M.D.: An Information Security Handbook, 2. Auflage, London 2002

International Organisation for Standardization ISO (Hrsg.): ISO/IEC 13335-1:2004 Information technology – Management of information and communications technology security, Geneva 2004

International Organisation for Standardization ISO (Hrsg.): ISO/IEC 15408-1:2005 Security techniques - Evaluation criteria for IT security, Geneva 2005

International Organisation for Standardization ISO (Hrsg.): ISO/IEC 15408-2:2005 Security techniques - Evaluation criteria for IT security, Geneva 2005

International Organisation for Standardization ISO (Hrsg.): ISO/IEC 15408-3:2005 Security techniques - Evaluation criteria for IT security, Geneva 2005

International Organisation for Standardization ISO (Hrsg.): ISO/IEC 17799:2000 Information technology – Code of practise for information security management, Geneva 2000

Kaminske, Gerd F.; Brauer, Jörg-Peter: Qualitätsmanagement von A bis Z, 4. Auflage, München u. a. 2003

Mertens, Peter: Integrierte Informationsverarbeitung 1, 14. Auflage, Lengerich 2004

Michael, H.; Morawietz, P.: Qualitätsmanagement nach EN 2900001-4 (DIN EN ISO 9001-4), in Hansen, Wolfgang; Jansen, Herbert H.; Kaminske, Gerd. F.: Qualitätsmanagement im Unternehmen, Grundlagen, Methoden und Werkzeuge, Praxisbeispiele, Heidelberg, 1995

MPS consult Unternehmensberatung GmbH (Hrsg.): o. V.,
http://secuquest.com/secuquest/content.asp?ssid=131 (2006-02-12)

Müller, Klaus-Rainer: IT-Sicherheit mit System - Strategie - Vorgehensmodell - Prozessorientierung - Systempyramide, Wiesbaden 2003

Northwest Controlling Corporation Ltd. (Hrsg.): o. V., http://noweco.com/riskrege.htm (2006-02-12)

Olev (Hrsg.): Burkhardt Krems
http://www.olev.de/l.htm (2006-02-12)

Parson, Talcott: The Social System, With a New Preface by Bryan S. Turner, Abingdon 2001, S. 3 - 24

Reiter, Christian: Toolbasierte Referenzmodellierung - State-of-the-Art und Entwicklungstrends, in: Schütte, Reinhard (Hrsg.): Referenzmodellierung - State-of-the-Art und Entwicklungsperspektiven, Heidelberg 1999, S. 45 - 64

Rosemann, Michael: Komplexitätsmanagement in Prozeßmodellen – Methodenspezifische Gestaltungsempfehlungen für die Informationsmodellierung, Wiesbaden 1996

Rosemann, Michael; Schütte, Reinhard: Multiperspektivische Referenzmodellierung, in: Schütte, Reinhard (Hrsg.): Referenzmodellierung – State-of-the-Art und Entwicklungsperspektiven, Heidelberg 1999, S. 23 - 44

Scheer, August-Willhelm: ARIS - Vom Geschäftsprozess zum Anwendungssystem; 4. Auflage, Berlin u.a. 2002

Scheer, August-Willhelm: ARIS - Business Process Modeling; 2. Auflage, Berlin u.a. 1999

Scheer, August-Wilhelm; Jost, Wolfram: Geschäftsprozessmodellierung innerhalb einer Unternehmensarchitektur, in: Vossen, Gottfried; Becker, Jörg: Geschäftsprozeßmodellierung und Workflow-Management, Modelle, Methoden, Werkzeuge, Bonn u. a. 1996, S. 27 - 45

Scheer, August-Willhelm: Wirtschaftsinformatik: Referenzmodelle für industrielle Geschäftsprozesse, 2. Auflage, Berlin u. a. 1998

Scheer, August-Willhelm; Jost Wolfram: ARIS in der Praxis - Gestaltung, Implementierung und Optimierung von Geschäftsprozessen, Berlin u. a. 2002

Schreier, Ulf: Datenbeschreibungssprachen in: Mertens, Peter (Hrsg.): Lexikon der Wirtschaftsinformatik, 2.Auflage, Berlin u. a. 1990

Seidlmeier, Heinrich: Process Modeling with ARIS - A Practical Introduction, Wiesbaden 2004

Staehle, Wolfgang H. (Hrsg.): Management, Eine verhaltenswissenschaftliche Perspektive, München 1991

Symantec (Hrsg.): o. V.,
http://enterprisesecurity.symantec.de/products/products.cfm?productid=111
(2006-02-12)

Abschließende Erklärung

Ich versichere hiermit, dass ich die vorliegende Diplomarbeit selbständig, ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Magdeburg, den 23. Februar 2006