universität
wien

MASTERARBEIT

Titel der Masterarbeit

„Architektur zur Gewährleistung der Resilience für Informationssysteme im Katastrophenschutzeinsatz“

verfasst von

Pia Patricia Hoschek, BSc

angestrebter akademischer Grad

Diplom–Ingenieurin (Dipl. Ing.)

Wien, 2015

Studienkennzahl lt. Studienblatt:	A 066 926
Studienrichtung lt. Studienblatt:	Masterstudium Wirtschaftsinformatik
Betreut von:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

universität wien

MASTER THESIS

Title of the Master Thesis

„Architektur zur Gewährleistung der Resilience für Informationssysteme im Katastrophenschutzeinsatz“

submitted by

Pia Patricia Hoschek, BSc

in partial fulfilment of the requirements for the degree of

Diplom–Ingenieurin (Dipl. Ing.)

Vienna, 2015

Degree programme code as it appears on the student record sheet:	A 066 926
Degree programme as it appears on the student record sheet:	Masterstudium Wirtschaftsinformatik
Supervisor:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Ehrenwörtliche Erklärung

Ich erkläre hiermit, dass ich die vorliegende Masterarbeit selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Ich versichere, dass ich diese Masterarbeit bisher weder im Inland noch im Ausland zur Begutachtung in irgendeiner Form als Prüfungsarbeit vorgelegt habe, und dass diese Arbeit mit der vom Begutachter beurteilten Arbeit übereinstimmt.

Wien, Dezember 2015 Unterschrift

„PHANTASIE IST WICHTIGER ALS WISSEN, DENN WISSEN IST BEGRENZT.“

ALBERT EINSTEIN

Danksagung

Dankend hervorgehoben wird Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr für die außergewöhnliche Betreuung während des Entstehungsprozesses dieser Masterarbeit. Seine Ruhe und Gelassenheit sowie das Zuhören und konstruktive Feedback sind Eigenschaften, die bis zum Schluss als großartige Unterstützung gedient haben. Ebenfalls hervorgehoben wird sein Engagement, welches es ermöglicht hat, einen Teil dieser Arbeit im Rahmen eines Forschungsprojekts an der Universität Wien zu schreiben. Ein weiterer Dank wird auch an die Kooperationspartner des Forschungsprojektes, die BMLVS/LVAk Landesverteidigungsakademie Wien, insbesondere an Dipl.-Ing. Christian Meurers und Dipl.-Ing. Johannes Göllner, MSc, der Universität für Bodenkultur Wien, dem BMI, der h2 projekt.beratung KG wie auch der ingentus decision support KG ausgesprochen. Für die kreativen Gespräche und Mittagessen, aber auch den ein oder anderen wissenschaftlichen Input, sind Mag. Martin Latzenhofer und Roland Petschenig, BSc dankend hervorzuheben. Großer Dank wird auch Lisa Hoschek, BA und Paul Hoschek zur mentalen Unterstützung, Dr. med. Patricia Hoschek und Dipl.-Ing. Wolfgang Hoschek für die finanzielle und mentale Unterstützung, Dipl.-Ing. Peter Wintoniak für Diskussionen über generelle Themen der Informationstechnologie und last but not least Markus Sehnal für die Unterstützung, das Verständnis, die Geduld, die Motivation und das Zuhören ausgesprochen.

Abstract

This master thesis focuses on the development of a disaster management architecture, which ensures a resilient information system. Crisis management and emergency management, standards and norms as well as business continuity management and disaster recovery are part of the first theoretical section of this paper. A business continuity and disaster recovery plan for small and medium enterprises is developed and the resilience of information systems and technologies, based on the CMU-CERT Resilience Management Model, is analysed. Based on the literature research a business process model focused on business continuity management is developed and completed with latest information technology infrastructure solutions. The general usability of this business continuity model is verified through a comparison with the service design phase of the IT infrastructure library framework.

Zusammenfassung

Diese Masterarbeit befasst sich mit der Entwicklung einer Architektur zur Gewährleistung der Resilience für Informationssysteme im Katastrophenschutzeinsatz. Der Theorieteil behandelt die Bereiche Krisenmanagement und Notfallmanagement, Normen und Standards wie auch Business Continuity Management und Disaster Recovery. Anschließend wird ein Business Continuity und Disaster Recovery Plan für kleine und mittlere Unternehmen erstellt und die Resilience von Informationssystemen wie auch Technologien, basierend auf dem CMU-CERT Resilience Management Model, analysiert. Aufbauend auf der Literaturrecherche wird im Praxisteil ein Business Continuity Management Modell entwickelt und mit aktuellen IT-Infrastrukturlösungen ergänzt. Abschließend wird das Business Continuity Management Modell mit der Service Design Phase des IT Infrastructure Library Frameworks überprüft.

Keywords: Business Continuity Management, Disaster Recovery, Resilience, Business Process Management, IT Infrastructure Library

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Die Entwicklung der Informationstechnik hat zur Folge, dass die Wirtschaft, Wissenschaft und viele andere Lebensbereiche stetigen Veränderungen ausgesetzt sind. Die effektiv und global wachsenden Kapazitäten Informationen zu übertragen, Informationen zu speichern und Wissen jedem und überall zugänglich zu machen, sind Bereiche, die essentiell für jeden wirtschaftlichen Vorgang, wie auch die Weiterentwicklung der Gesellschaft sind. Eine zentrale Fragestellung ist daher, wie IT-Infrastrukturen bei Eintreten einer Katastrophe aufrechterhalten werden können. Hier setzt diese Arbeit an und beschäftigt sich mit der Entwicklung einer Architektur, die eine erhöhte Widerstandsfähigkeit von Informationssystemen im Katastrophenschutzeinsatz gewährleistet. Um dieses Ziel zu erreichen, wird zu Beginn das Business Continuity Management näher betrachtet und allgemein der Frage nachgegangen, wie widerstandsfähig IT-Infrastrukturen sind. Es wird ein Notfall- und Krisenmanagement aufgebaut, so dass wichtige Geschäftsprozesse in kritischen Situationen nicht oder nur kurz unterbrochen werden und somit die Existenz der Unternehmen gesichert bleibt. Ein weiteres Augenmerk liegt auf der Einleitung von Maßnahmen, welche die Datenwiederherstellung und das Wiederaufsetzen der Infrastruktur, Hardware und der Organisation im Allgemeinen sicherstellen. Aufbauend auf der grundlegenden, ausreichend recherchierten Theorie, wird ein aussagekräftiges Architekturkonzept entwickelt. Dieses Konzept wird in Kooperation mit der BMLVS/LVAk Landesverteidigungsakademie Wien, der Universität für Bodenkultur Wien, dem BMI, der h2 projekt.beratung KG und der ingentus decision support KG innerhalb eines Forschungsprojektes umgesetzt. Der inhaltliche Schwerpunkt liegt auf der Entwicklung einer cloudbasierten simulationsgestützten Entscheidungshilfe zur Erstellung von aktuellen Lagebildern sowie simulierten Szenarien und kurz- bis mittelfristigen Zukunftsanalysen. Insbesondere wird eine prozessorientierte Informationssystemarchitektur konzipiert, welche ein Prozessmodell, die Informationssystemarchitektur sowie die unterstützenden Infrastrukturkomponenten umfassen, und deren Ziel es ist, die Bereitstellung der nötigen Informationen für die Simulation zu ermöglichen. Gegen Ende der Arbeit wird auf eine detaillierte Dokumentation der Vorgehensweise bei der Entwicklung des Lösungsansatzes eingegangen, wie auch anschließend auf eine Darstellung des Modells. Als Unterstützung zur Entwicklung des Modells wird das Geschäftsprozessmanagementtool ADONIS verwendet. Um die Funktionalität des Architekturkonzepts zu gewährleisten,

wird das entwickelte Modell mit der Service Design Phase des ITIL Frameworks verglichen und anschließend kritisch in Form einer Diskussion behandelt.

2 Business Continuity Management

Um den Begriff Business Continuity Management näher definieren zu können, wird zuerst dem Statement von [HeES04] „Crisis management can be considered the roots of BCM,...“ nachgegangen. In [Thie14] wird Krisenmanagement aus der Perspektive des Stakeholders Management betrachtet. In Organisationen sind Krisen von Strategien untrennbar. Als Strategie wird die Festlegung einer Vision zur Erreichung von Zielen verstanden und Krisen explizieren für Organisationen was noch nicht möglich ist. Somit sind Krisen für Organisationen sowohl Ziele als auch eine wichtige Kategorie ihrer Strategien. Während einer Krise übernimmt die strategische und operative Unternehmensführung die Managementfunktionen im Unternehmen, um ein Unternehmen mit eingeschränkten Entscheidungsmöglichkeiten und Entscheidungsoptionen zu steuern und zu führen. Für das Krisenmanagement haben sich stützende Funktionen etabliert, um die Unternehmensführung in Sondersituationen zu ermöglichen. Dazu zählen das Erkennen früher Signale über das Risikomanagement und das Business Continuity Management wie auch die Analyse von Wirkungsbeziehungen. Krisenmanagement kann als Ursprung des Business Continuity Managements betrachtet werden (vergleiche [HeES04]), jedoch kann Business Continuity Management auch als Teil des Krisenmanagements angesehen werden, nämlich zur Unterstützung von Prozessen bei der Bewältigung von Krisen. Das Business Continuity Management ist Teil eines Notfallplans und ermöglicht Unternehmen oder Institutionen nach einer Katastrophe wieder arbeitsfähig zu sein und zu einem normalen Dienstbetrieb zurückzukehren. [Thie14] Weitere Definitionen von Business Continuity Management sind in diversen Standardisierungen zu finden, auf die im nächsten Kapitel noch näher eingegangen wird. Die ersten Schritte der Entwicklung einer Architektur, die als Grundlage für die Erstellung eines Modells dienen, sind die theoretische Aufarbeitung möglicher Zusammenhänge des Notfallmanagements mit dem Business Continuity Management wie auch die Ausarbeitung eines Leitfadens zur Einführung eines Business Continuity Management Plans für kleine und mittlere Unternehmen.

2.1 Standardisierungen

Business Continuity Management ist in verschiedenen Normen sowie nationalen und internationalen Standards zu finden. Als Grundlage des Business Continuity Managements dienen folgende Normen und Standards:

- Die vom British Standards Institute veröffentlichten Richtlinien und Prinzipien:
  - „Business Continuity Management – Part 1: Code Practice“ (BS 25999-1) Standard
  - „Good Practice Guidelines“
  - Public Available Specification 77:2006 „IT Service Continuity Management – Code of Practice“ (PAS 77)
  - „Code of practice for information and communication technology continuity“ (BS 25777)
- „Societal security – Guideline for incident preparedness and operational continuity management“ (ISO/PAS 22399)
- Die internationalen Normen für das Management von Informationssicherheit „Information technology – Security techniques – Information security management systems requirements specification“ (ISO 27001) und „Information technology – Code of practice for information security management“ (ISO 27002)
- Der Standard „Contingency Planning Guide for Information Technology Systems“ (NIST SP 800-34) als Notfallvorsorgeplanung für IT-Systeme
- „Information technology – Security techniques – Guidelines for information and communication technology disaster recovery services“ (ISO/IEC 24762)
- „IT Infrastructure Library“ (ITIL)
- Der Standard ISO/IEC 20000 „IT Service Management“
- ÖNORM A 7799 et cetera

Die Auswahl, wie auch die Umsetzung solcher Standards, stellt oft erhebliche Hürden dar. Einerseits weisen diese Standards eine hohe Komplexität wie auch eine nur für Experten verständliche Darstellung auf. Eine detaillierte Beschreibung dieser und weiterer Standards sind in der Diplomarbeit von Herrn Tinkl [Tink11] nachzulesen. Da viele dieser Standards kostenpflichtig sind, wurde als Grundlage für die weitere Recherche und gegen Ende hin die Entwicklung des Modells der BSI-Standard 100-4 des Bundesamts für Sicherheit in der Informationstechnik [Bund08a] wie auch das österreichische Informationssicherheitshandbuch [Bund13] herangezogen.

2.2 Notfallmanagement

Wesentliche Merkmale des Notfallmanagements sind kritische Geschäftsprozesse aufrecht zu erhalten und Auswirkungen von Schadensereignissen auf Institutionen so gering wie möglich zu halten. Das Notfallmanagement ist ein Prozess, der sowohl die Notfallvorsorge, die Notfallbewältigung wie auch die Notfallnachsorge umfasst. Das Treffen strategischer Entscheidungen, die Etablierung von Organisationsstrukturen und

die Umsetzung von Maßnahmen sind wesentliche Schritte, um die Ziele des Notfallmanagements zu erreichen. Der Notfallmanagementprozess (vergleiche Abbildung 1) besteht aus folgenden Prozessschritten: Das Notfallmanagement wird initiiert, ein Konzept erstellt, das Notfallvorsorgekonzept umgesetzt, der Notfall bewältigt, Tests und Übungen durchgeführt wie auch alle Notfallmanagementprozesse aufrecht erhalten und kontinuierlich verbessert. [Bund08a]

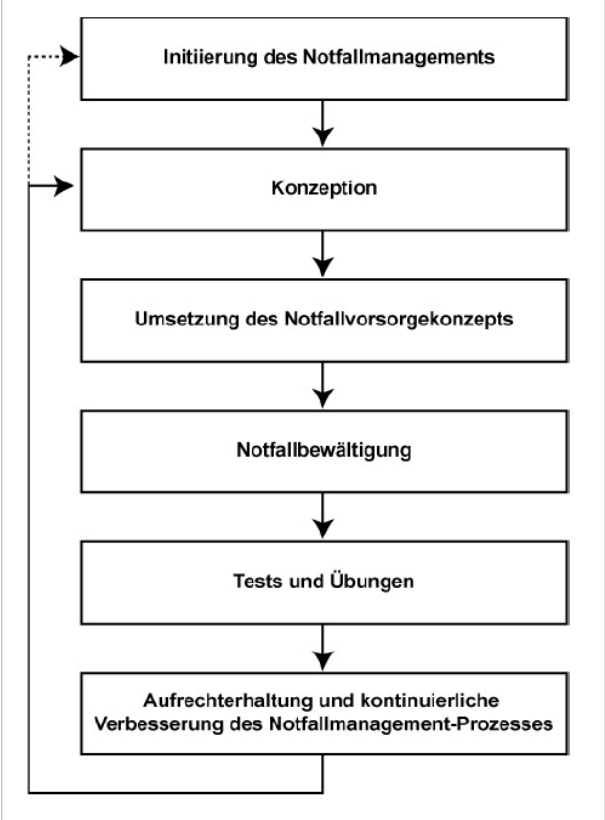

Abbildung 1: Notfallmanagementprozess [Bund08a]

Die Initiierungsphase startet mit der Übernahme der Verantwortung durch die Behörden bzw. die Unternehmensleitung wie auch die Entwicklung von Leitaussagen zum Notfallmanagement. Fortgesetzt wird diese Phase mit der Definierung der Ziele für das Notfallmanagement, die Festlegung der Geltungsbereiche, die Ermittlung der Rahmenbedingungen und die Festlegung der Strategie. Die Festlegung von Rollen für unterschiedliche Verantwortungsbereiche, die Erstellung einer Leitlinie zum Notfallmanagement, die Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen und die Einbindung aller Mitarbeiter in die Unternehmenskultur sind organisatorische Voraussetzungen, welche die erste Phase des Notfallmanagements abschließen. Die Entwicklung eines Notfallkonzepts, bestehend aus dem Notfallvorsorgekonzept und Notfallhandbuch, beinhaltet die Identifizierung der Verfügbarkeitsanforderungen von Geschäftsprozessen, das Erkennen von Schwachstellen und die Etablierung von Gegenmaßnahmen. Diese notwendigen

Informationen werden mit Hilfe einer Business Impact Analyse und einer Risikoanalyse ermittelt und die Geschäftsfortführung wird durch die Erstellung von Kontinuitätsstrategien ermöglicht. Zur Umsetzung des Notfallvorsorgekonzepts zählen eine Kosten- und Aufwandsschätzung, die Festlegung von Aufgaben und Verantwortungen wie auch realisierungsbegleitende Maßnahmen. Die Notfallbewältigung erfolgt durch die Identifikation und Analyse von möglichen Notfall- und Krisensituationen, die Entwicklung von Bewältigungsstrategien, sowie die Einleitung und Verfolgung von Gegenmaßnahmen. Die Kommunikation während und nach einer Krise mit den verschiedenen Interessensgruppen wie auch die Erstellung eines Notfallhandbuchs schließen den Prozess der Notfallbewältigung ab. Die Vorsorgemaßnahmen, die organisatorischen Strukturen und die unterschiedlichen Pläne sind regelmäßig durch Tests und Übungen nachzuprüfen. Zum Schluss muss der Notfallmanagementprozess regelmäßig auf seine Wirksamkeit und Effizienz überprüft werden. [Bund08a]

Der Notfallmanagementprozess ist vom Prozessaufbau ähnlich strukturiert wie der Business Continuity Management Prozess vom Business Continuity Institut (siehe Abbildung 2).

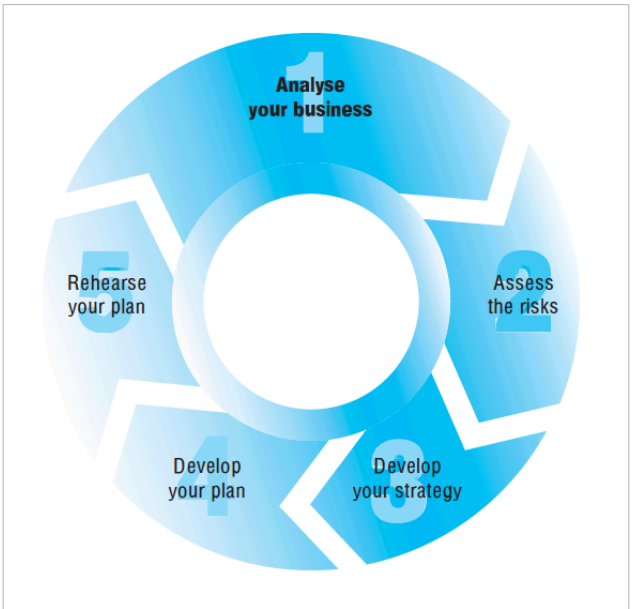

Abbildung 2: Business Continuity Management Schritte [LoNB03]

Der Business Continuity Management Prozess vom Business Continuity Institut startet mit der Analyse des Unternehmens (Ist-Zustand) und endet mit der Feststellung der Risiken, der Entwicklung einer Strategie wie auch der Erstellung und Erprobung eines Plans.

Auf Basis des Notfallmanagementprozesses [Bund08a] und der Business Continuity Management Schritte [LoNB03] in Kombination mit [WhMa14] wird nun im nächsten

Schritt ein Leitfaden zur Umsetzung eines Business Continuity Managements für KMU erstellt.

2.3 Contingency Planning

Die Notfallplanung, oder auch Contingency Planning genannt, bezeichnet das Ermitteln, Reagieren und Wiederherstellen von Ereignissen innerhalb einer Organisation, welche die Informationssicherheitsressourcen gefährden können. Mögliche Ereignisse bzw. Bedrohungen können Naturkatastrophen (Erdbeben, Hochwasser), vom Menschen verursachte Katastrophen (Terroranschläge) oder auch technische Katastrophen (Cyberangriffe) sein. Grundsätzlich sind zwei wesentliche Prozesse zu beachten, nämlich die präventive Entwicklung von Maßnahmen und die Sicherstellung der Fortführung von kritischen Geschäftsoperationen im Fall einer Katastrophe. [Bank03] Das Ziel der Notfallplanung ist die Wiederherstellung der herkömmlichen Operationen mit einem geringen Kostenaufwand und kurzer Unterbrechung der Geschäftsaktivitäten. Die Notfallplanung gliedert sich in vier wesentliche Komponenten (siehe Abbildung 3 und Abbildung 4). Der erste Schritt ist die Business Impact Analyse, welche die notwendigen Informationen über kritischen Geschäftsprozesse und Ressourcen liefert. Weitere Schritte sind das Incident Response Planning, also die Vorgehensweise beim Eintreffen eines Ereignisses, und das Disaster Recovery Planning, wobei hier ein Notfallplan erstellt wird. Schließlich gibt es noch das Business Continuity Planning, das die Entwicklung von Strategien vorsieht, um den Fortbestand von organisationsinternen Prozessen zu gewährleisten. [WhMa14]

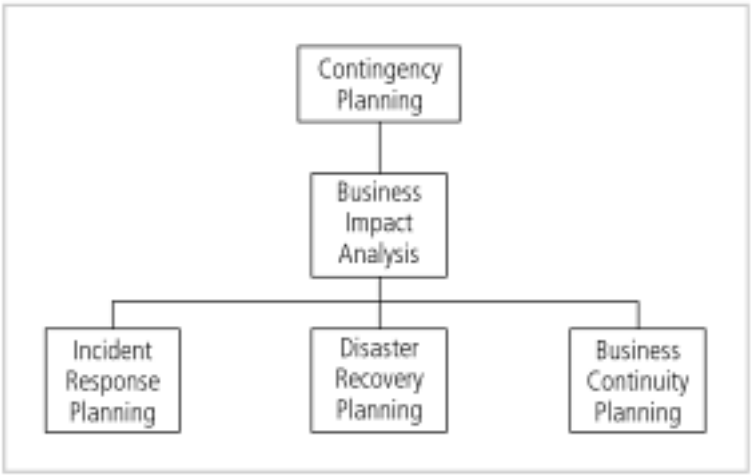

Abbildung 3: Contingency planning Hierarchien [WhMa14]

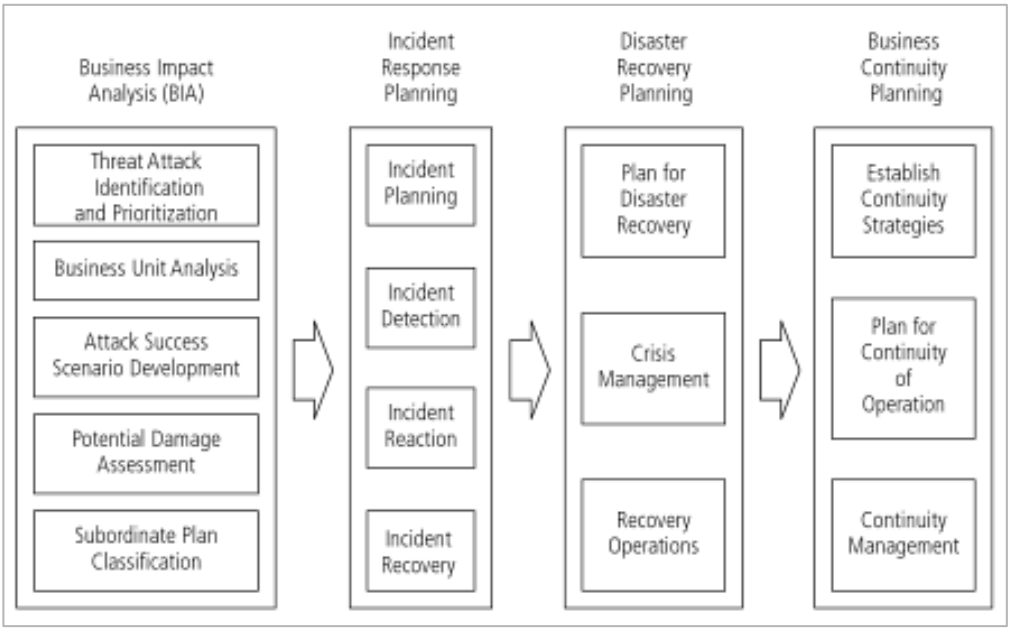

Abbildung 4: Hauptaufgaben des contingency plannings [WhMa14]

2.3.1 Business Impact Analyse

Unter einer Folgeschädenabschätzung, auch Betriebsunterbrechungsanalyse genannt, werden Geschäftsprozesse verstanden, die für die Aufrechterhaltung des Geschäftsbetriebs und damit für die Institution wichtig sind und beinhaltet die Folgen, die ein Ausfall auslösen kann. Die Business Impact Analyse ist ein Verfahren, um die Wiederanlaufpunkte der Geschäftsprozesse, eine Priorisierung für den Wiederanlauf und damit die Kritikalität der Geschäftsprozesse festzulegen, und die benötigten Ressourcen zu identifizieren. [Bund08a] Die Durchführung einer BIA kann in folgende Teilschritte untergliedert werden:

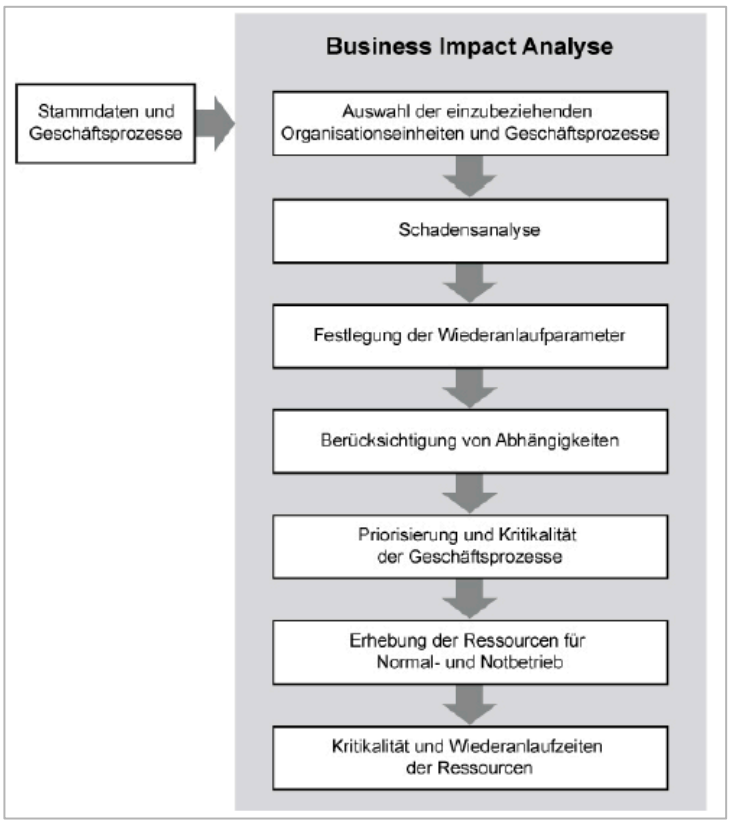

Abbildung 5: Übersicht BIA [Bund08a]

Eine detaillierte Beschreibung der einzelnen Prozesse ist in Kapitel 5.1.2 zu finden.

2.3.1.1 Risikoanalyse

Die Risikoanalyse dient dazu, die Gefährdungen zu identifizieren, die eine Unterbrechung von Geschäftsprozessen verursachen können, und die damit verbundenen Risiken zu bewerten. [Bund08a] In Kapitel 5.1.3 wird näher auf die Durchführung einer Risikoanalyse eingegangen.

2.3.2 Incident Response Planning

Der Incident Response Plan ist eine detaillierte Sammlung von Prozessen und Abläufen, die Auswirkungen von unerwarteten Ereignissen vorhersagt, feststellt und entschärft. Dieser Plan umfasst Maßnahmen, die bei einer Bedrohungen eingesetzt werden können, und besteht aus drei Bereichen:

- Vorgehensweise vor einer Bedrohung/Attacke (Nutzer und Technologie Services)
- Vorgehensweise während einer Bedrohung/Attacke (Nutzer und Technologie Services)
- Vorgehensweise nach einer Bedrohung/Attacke (Nutzer und Technologie Services) [WhMa14]

2.3.3 Disaster Recovery Planning

Nach der Geschäftsauswirkungsanalyse (Business Impact Analyse) und der Risikoanalyse ist es notwendig, eine Wiederherstellungsstrategie zu erstellen. Nachdem die Strategie definiert und die kritischen Geschäftsprozesse identifiziert wurden, ist eine Liste mit technischen und organisatorischen Maßnahmen zu entwerfen. Der Wiederherstellungsplan setzt die Fertigstellung des Katastrophen-/Notfallplans voraus. Der Widerherstellungsplan ist ein technisch orientierter Plan, entworfen für Arbeiter in der Informations- und Kommunikationstechnik, um Geschäftsprozesse wiederherzustellen und um zu normalen Operationen zurückzukehren. Von großer Wichtigkeit ist die Anpassung der Pläne an die Anforderungen der Organisationen, die Kosten, die Festlegung der maximal tolerierten Diskontinuität und die Wiederherstellungszeit. Das Resultat der gewählten Strategie kann unterschiedliche Ausprägungen annehmen: Datensicherungsrichtlinien, Datenreproduktion, aktive und passive Geräte, Festplattenspiegelung des Systems oder auch der Daten, Verwendung von RAID Technologien, Einführung von Fehlerstromschutzschalter, unterbrechungsfreie Stromversorgung, Notstromaggregate, Brandschutz, Server Virtualisierung, Datenbanksicherung und Viren- und Firewall Absicherung. [Pint11]

2.3.3.1 Notfallhandbuch

Alle Maßnahmen, die nach Eintritt eines notfallauslösenden Ereignisses zu ergreifen sind, und alle dazu erforderlichen Informationen sind in einem Notfallhandbuch (Grundlagen [Bund08a] und [Bund13]) zu dokumentieren. Ein Notfallhandbuch besteht aus dem Sofortmaßnahmenplan, einem Krisenstabsleitfaden, einem Krisenkommunikationsplan, einem Geschäftsfortführungsplan und einem Wiederanlaufplan. Eine detaillierte Aufzählung dieses Maßnahmenkatalogs (siehe Tabelle 1) gliedert sich wie folgt.

Tabelle 1: Notfallhandbuch Maßnahmenkatalog [Bund13]

1) Teil A: Sofortmaßnahmen
a) Alarmierung im Notfall i) Alarmierungsplan und Meldewege ii) Notrufnummern b) Handlungsanweisung für spezielle Ereignisse, Treffpunkte i) Ausfall der Datenfernübertragung
2) Teil B: Regelungen für den Notfall (Krisenmanagement)
a) Allgemeine Regelungen i) Rollen, Zuständigkeiten und Kompetenzen b) Krisenstabsraum/Lagezentrum c) Krisenstabsarbeit Lagebeurteilung d) Dokumentation im Krisenstab e) Deeskalation f) Analyse und Bewertung der Notfallbewältigung
3) Teil C: Kommunikation und Öffentlichkeitsarbeit im Krisenfall
4) Teil D: Wiederanlaufpläne für kritische Komponenten (Wiederherstellung)
a) Wiederanlaufplanung i) Wiederanlaufplan für Komponente 1 (1) Wiederbeschaffungsmöglichkeit (2) Interne/Externe Ausweichmöglichkeiten (3) DFÜ Versorgung (4) Eingeschränkter IT-Betrieb (5) Wiederanlaufreihenfolge ii) Wiederanlaufplan für Komponente 2
5) Teil E: Geschäftsfortführung
a) Tabelle der Verfügbarkeitsanforderungen der Organisationseinheit b) Geschäftsfortführungspläne (Szenarien) i) Organisationseinheiten Kritikalität A ii) Organisationseinheiten Kritikalität B
6) Teil F: Dokumentation
a) Beschreibung der IT-Systeme i) Beschreibung des IT-Systems A (1) Beschreibung der Hardware-Komponenten (2) Beschreibung der Software-Komponenten (a) Bestandsverzeichnis der Systemsoftware

(b) Bestandsverzeichnis der zu dem IT-System gehörenden Systemdaten
(3) Beschreibung der Netzanbindung des IT-Systems
(4) Beschreibung der IT-Anwendungen
(a) Bestandsverzeichnis der zu einer IT-Anwendung gehörenden Daten
(b) Kapazitätsanforderungen einzelner IT-Anwendungen im Normalfall
(c) Minimale Kapazitätsanforderungen der IT-Anwendungen für den Normalfall
(d) Wiederanlaufverfahren der IT-Anwendungen
(5) Datensicherungsplan
(6) Beschreibung der Notwendigen Infrastruktureinrichtungen
(7) Sonstige Unterlagen (Handbücher etc.)
ii) Beschreibung des IT-Systems B

2.3.4 Business Continuity Planning

Laut [Pint11] und [SnRi14] ist das Business Continuity Planning eine Methode, einen Plan zu erstellen und zu validieren, der vor, während und nach einer Katastrophe die Aufrechterhaltung der Geschäftstätigkeiten sicherstellt. Das betriebliche Kontinuitätsmanagement ist ein Planungsprozess, wobei auch potentielle Auswirkungen von internen und externen Gefahren, und die dadurch entstehenden Verluste, identifiziert werden. Unfälle, Attacken oder Katastrophen können zu einem Verlust von Geschäftsprozessen führen. Die häufigsten gemeldeten Notfälle werden als „Kurzfristige Störungen“ und „Mittel bis schwerwiegende Vorfällen“ klassifiziert. Zu den kurzfristigen Störungen zählen Stromausfälle oder geringe Störungen des Netzwerkes. Zu den mittel bis schwerwiegenden Vorfällen zählen Feuer, Hochwasser, Hackangriffe, Diebstahl oder Verlust sensibler Daten. Das Ziel ist einen Plan und eine Umgebung zu entwickeln, welche den Fortbestand und die Wiederherstellung von kritischen Prozessen von einem festgelegten minimalen Level zu einem bestenfalls originalen Zustand zu garantieren. [Pint11]

BCM basiert auf der technischen Katastrophenwiederherstellung in Organisationen. Mögliche Maßnahmen zur Wiederherstellung von Geschäftsprozessen sind die Verwendung von Cloud Computing Servicemodellen wie SaaS (Software as a Service), PaaS (Platform as a Service) oder IaaS (Infrastructure as a Service) und lagern IT Services aus (Outsourcing). Um Business Continuity Management Maßnahmen zu verbessern und Feedback zu erhalten, werden Prüfverfahren durchgeführt. Dabei werden Standards (Information Security Management) und Governance Frameworks (COBIT, ITIL) verwendet und mit Kontrollen und Trainings kombiniert. [Järv12]

2.3.4.1 Leitfaden

Bei kleinen und mittelständischen Unternehmen besteht erheblicher Nachholbedarf beim Business Continuity Management. Die existierenden Standards und Prüfvorschriften werden häufig als zu komplex und ihre Umsetzung als zu aufwendig und teuer empfunden.

Im Folgenden wird ein Leitfaden (Kombination aus [Pint11], [ThTh10] und [Lond03]) zur Implementierung eines unternehmensspezifischen BCM vorgestellt, der eine Lösung für IT-Laien und kleine und mittlere Organisationen darstellt.

1) **Einleitung und Definition**

   Dieser Leitfaden kann kein individuelles Konzept ersetzen. Voraussetzungen müssen ausreichend personelle und zeitliche Ressourcen sowie ein angemessenes Budget sein.

2) **Vorgehensweise zur Umsetzung eines BCM Konzepts**

   Dieses Kapitel orientiert sich am Management-Zyklus für BCM, umfasst den Abschnitt der empfohlenen Grundsätze sowie die unterschiedlichen Phasen des Managementzyklus, nämlich die Vorbereitung, die Maßnahmenplanung für Prävention bzw. Bewältigung, den Eintritt eines Ereignisses und Nachbearbeitung. Die zentralen Punkte Dokumentation/Einführung, Test/Schulung und Verbesserung/Aktualisierung sind in allen vier Phasen gleichermaßen anzuwenden.

   a) Vorbereitung und Analyse

   Der erste Schritt beinhaltet die Analyse der aktuellen Situation und besteht aus folgenden Stufen: die Bereitschaft des Managements zur Durchführung des Projekts, die Identifikation von Kernprozessen (Ressourcen und kritische Aktivitäten) [Pint11] und die SWOT-Analyse (Bestandsaufnahme). Die daraus resultierenden Krisenherde werden klassifiziert und priorisiert (High-Risk-Szenario) sowie anschließend eine anzuwendende Strategie für jedes Szenario bestimmt. Die Bestimmung der Strategie führt zur Ausarbeitung von Maßnahmenkatalogen von Krisenplänen, um die Ausfallrisiken zu reduzieren. Ein Krisenstab ist für die Ausarbeitung verantwortlich und alle Tätigkeiten inklusive Ereignisse müssen Teil eines Krisenhandbuchs sein.

   b) Feststellen der Gefahrenquelle

   Zu dieser Phase zählen die Risikoanalyse (identifizieren kritischer Geschäftsprozesse) sowie die Business Impact Analyse (Untersuchung der identifizierten Risiken auf ihre Auswirkungen hinsichtlich der kritischen Geschäftsprozesse).

   c) Maßnahmenplanung für die Prävention bzw. Bewältigung

Dieser Plan unterscheidet zwischen proaktiven (Prävention von Unterbrechungen organisatorischer Abläufe) und reaktiven (Behebung von kritischen Unterbrechungen) Maßnahmen. Für jedes priorisierte Szenario können eigene Maßnahmenkataloge bzw. Krisenpläne erstellt werden, die Teil eines unternehmerischen Krisenhandbuchs sind.

d) Entwicklung einer Strategie und Eintritt eines Ereignisses

Diese Phase beschreibt den Strategieentwurf zur Identifikation möglicher Ereignisse und deren Rückmeldungen und den sinnvollen im Vorfeld geplanten Umgang mit existenzbedrohenden Schadensereignissen. Für die Bewältigung der identifizierten Ausfallszenarien helfen die praktischen Handlungsanweisungen, die im Notfallplan bzw. Krisenplan festgehalten sind.

e) Entwicklung eines Plans

Festlegung von Berechtigungen und Verantwortlichkeiten der Beteiligten in Form eines Notfallmanagements und Funktionsbereichen. Es wird unterschieden zwischen einem Krisenteam, einem Koordinationsteam und einem operativen Team.

f) Nachbearbeitung und Erprobung des Plans

Die Nachbearbeitung befasst sich mit den Erkenntnissen und Erfahrungen aus überstandenen Krisen zur Verbesserung des Krisenplans.

3) Quickcheck

Tabelle 2: Quickcheck [ThTh10]

Schritte	Details
1. Krisenstab definieren	Krisenorganisation mit klarer Zuständigkeits-/Verantwortungszuweisungen Krisensprecher bestimmen Kontaktinformationen bzw. Kontaktliste
2. Kritische Bestandsaufnahme des Unternehmens mit SWOT-Analyse	
3. Risikoanalyse zur Identifizierung von Krisenherden	
4. BIA zur Bestimmung der Auswirkungen hinsichtlich der kritischen Geschäftsprozesse	
5. Identifikation der Überlebensdauer	

eines Unternehmens im Falle eines Ausfalles	
6. Risiken klassifizieren	
7. Bestimmung der Strategie nach Geschäftsbereichen	Risiken akzeptieren (keine Veränderungen vornehmen) Risiken möglichst reduzieren und Vorkehrung zur Hilfeleistung nach einem Vorfall treffen Risiko vermeiden Risiko auslagern (Risiko transferieren)
8. Präventionsmaßnahmen festlegen	Infrastruktur/Logistik (z.B. Brandschutz) Personal (z.B. 4-Augen-Prinzip) Externe Dienstleister (Zweitlieferanten) Technik (Datensicherung, Datenspiegelung)
9. Bewältigungsmaßnahmen für High-Risk-Szenarien festlegen	Evakuierungspläne Zweitstandortpläne Zweitlieferantenpläne IT-Disaster-Recovery Pläne
10. Richtlinien und Checklisten aufgrund erstellter Krisenpläne	
11. Maßnahmen schulen	
12. Pläne testen	
13. Pläne verbessern	
14. Pläne regelmäßig aktualisieren (empfohlen 1 Mal jährlich)	

2.4 Zertifizierungen/Lehrgänge/Ausbildungen

Zertifizierungen, Lehrgänge und Ausbildungen für BCM-Interessenten werden von zwei österreichischen Unternehmen angeboten. Die Quality Austria – Trainings, Zertifizierungs und Begutachtungs GmbH bietet eine kostenpflichtige Business Continuity Management Lehrgangsreihe an mit entsprechenden Berufsbildern wie BCM-Beauftragter oder BC-Manager. [Qual15] Die staatlich ausgezeichnete TÜV Austria Akademie GmbH bietet fachspezifische kostenpflichtige Seminare an zum Thema Business Continuity Management, wobei die Teilnehmer einer Teilnahmebestätigung als Kursabschluss erhalten. [Tüva15]

3 Resilience von Informationssystemen

Resilience, wörtlich übersetzt Belastbarkeit [Deut03] oder auch Widerstandsfähigkeit, bezeichnet die Fähigkeit von Organisationen wie auch Informationssystemen, Unterbrechungen zu vermeiden, zu überleben und Prozesse wiederherzustellen. [Jack10] Die Publikation [BhDB11] zeigt eine sehr gute literarische Aufbereitung des Ist-Zustandes des Forschungsgebiets Resilience für KMU. Der Begriff Resilience ist in den Bereichen der physischen Systemen, in Ökosystemen, in Sozialökosystemen, in der Psychologie, im Disaster Management, im Individuum, im Organisationsbereich und der Technik zu finden. Grundlegend definiert sich Resilience durch vier wichtige Merkmale, nämlich der Flexibilität, der Motivation, der Ausdauer und des Optimismus. [Fiks03] definiert Resilience als das Wiederherstellen von Störungen sowie das Gründen neuer Systemgleichgewichte und stabiler Domänen, um Systemen das schnellere Anpassen auf neue Umgebungen zu ermöglichen. Resilience kann somit als Kernaussage der Nachhaltigkeit von Informationssystemen gesehen werden. Wie in Abbildung 6 zu sehen ist, hat jedes System einen stabilen Zustand.

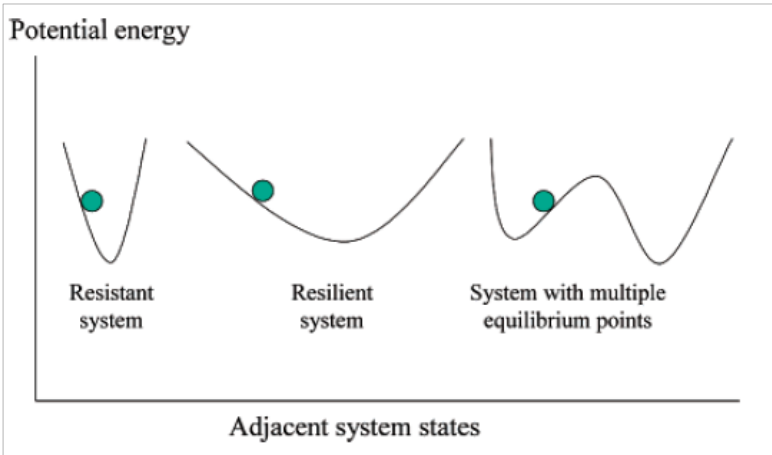

Abbildung 6: Systemzustände [Fiks03]

Ein resistentes, kontrolliertes System kann sich nach einer kleinen Störung schnell wiederherstellen, jedoch keine große Störung überstehen. Ein resilientes System übersteht große Störungen, und Systeme mit mehreren ausgeglichenen Zuständen tolerieren sogar sehr große Störungen. Resiliente Systeme zeichnen sich durch vier Charakteristiken der nachhaltigen Systementwicklung aus:

- **Vielfalt** Existenz von mehreren Systemformen und Verhalten
- **Effizienz** Leistung mit schlichtem Ressourcenverbrauch
- **Anpassungsfähigkeit** Flexibilität zur Veränderung
- **Zusammenhalt** Bestehen von Verbindungen [Fiks03]

Die Resilience wird unter anderem auch als eine Kombination aus Fehlertoleranz, im Sinne der funktionalen Sicherheit, und Zuverlässigkeit, im Sinne der Informationssicherheit, verstanden. [BeFD10] Unterbrechung, Vermeidung, Überleben und Wiederherstellung sind zusammenfassend Schlagwörter für Resilience. [PfLe12] Der Harvard Business Review Artikel bringt es jedoch auf den Punkt: „Any company that can make sense of its environment, generate strategic options, and realign its resources faster than its rivals will enjoy a decisive advantage. This is the essence of resilience.“ [HaVä03]

3.1 Resilience Management Systeme

Resilience ist eine Kombination aus technischen Design Eigenschaften wie der Fehlertoleranz und Zuverlässigkeit und organisatorischen Eigenschaften wie der Aufmerksamkeit, dem Training und der dezentralisierte Entscheidungsfindung. [MüKA13] Aus organisatorischer Sicht wurde Resilience von [HoOr97] definiert als eine „... fundamental quality of individuals, groups, organizations, and systems as a whole to respond productively to significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behaviour.”. Individuen, Gruppen und Organisationen wie auch Systeme wurden von [MüKA13] durch den Managementsystemprozess Operational Resilience (siehe Abbildung 7) näher definiert. Dieser wird von einer Organisation entworfen, entwickelt, implementiert und verwaltet. Darüber hinaus verbessert er Schutzstrategien und verbindet Menschen, Informationen, Technologien und Dienstleistungen miteinander. In diesem Prozess werden technische und organisatorische Ansichten, IS Sicherheit, Business Continuity und IT Operationen integriert und mit betrieblichen Informationssystemen kombiniert. [MüKA13]

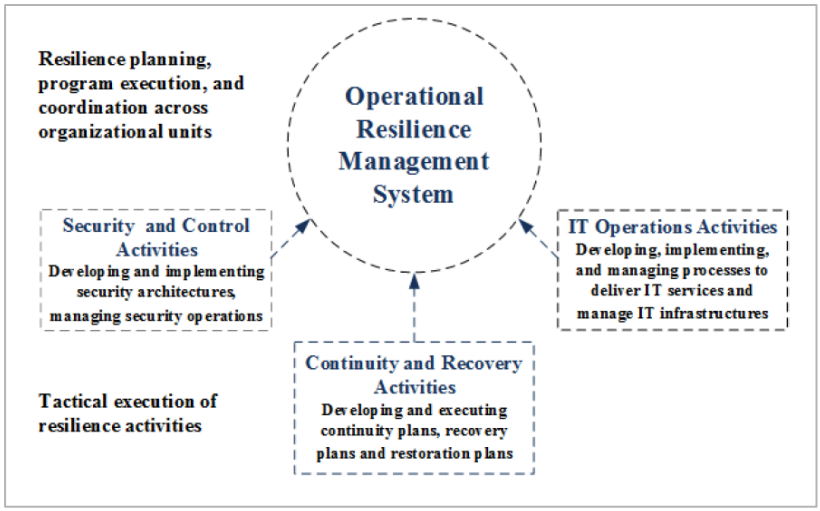

Abbildung 7: Operational Resilience Management System [MüKA13]

Basierend auf dem Operational Resilience Management System hat [MüKA13] einen Resilience Management Cycle (siehe Abbildung 8) entwickelt, der als Unterstützung zur Umsetzung des Prozesses eines widerstandsfähigen Business Process Managements, dient.

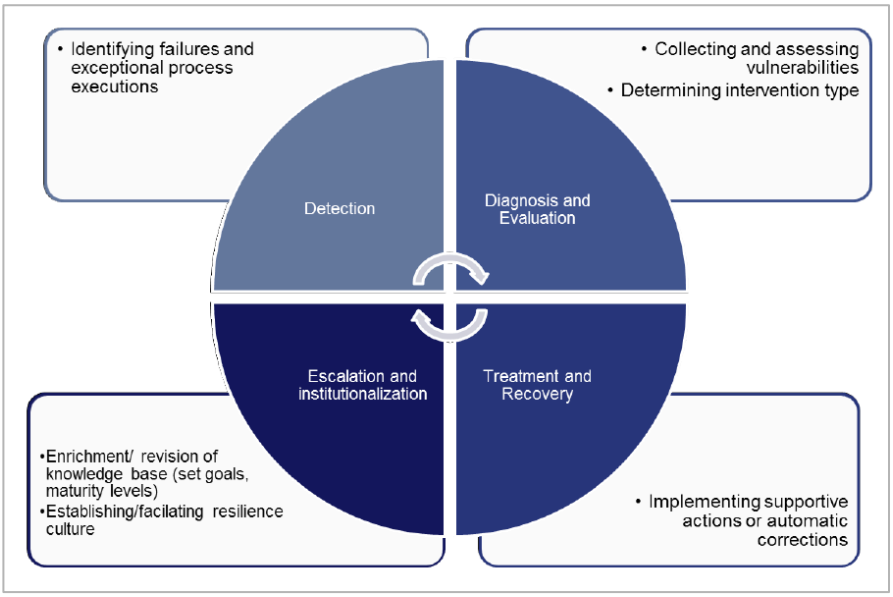

Abbildung 8: Resilience Management Cycle [MüKA13]

Dieser Resilience Management Cycle besteht aus 4 Phasen:

- **Erkennung** Identifikation von Ausfällen, potentiellen Schwächen und ungewöhnlichen Prozessabläufen
- **Diagnose und Evaluation** Sammeln und Bewerten von Schwachstellen, infolgedessen Festlegung von Interventionen
- **Bearbeitung und Wiederherstellung** Auswahl und Durchführung von unterstützenden Aktionen und automatischen Verbesserungen
- **Eskalation und Institutionalisierung** Sicherstellung der Bereicherung oder Überarbeitung der aktuellen Wissensbasis

3.1.1 CMU-CERT Resilience Management Model

Das CERT Resilience Management Model (CERT-RMM) definiert Prozesse des Umgangs mit betrieblicher Resilience in komplexen und risikoreichen Umgebungen und umfasst sowohl die Bereiche Sicherheit und Business Continuity, wie in Abbildung 9 zu sehen ist, als auch IT Operation Management. Operational Resilience definiert die Prozesse Entwurf, Entwicklung, Ausführung und Kontrolle von Strategien einer Organisation zum Schutz von hochwertigen Services und Geschäftsprozessen. [CACW10a]

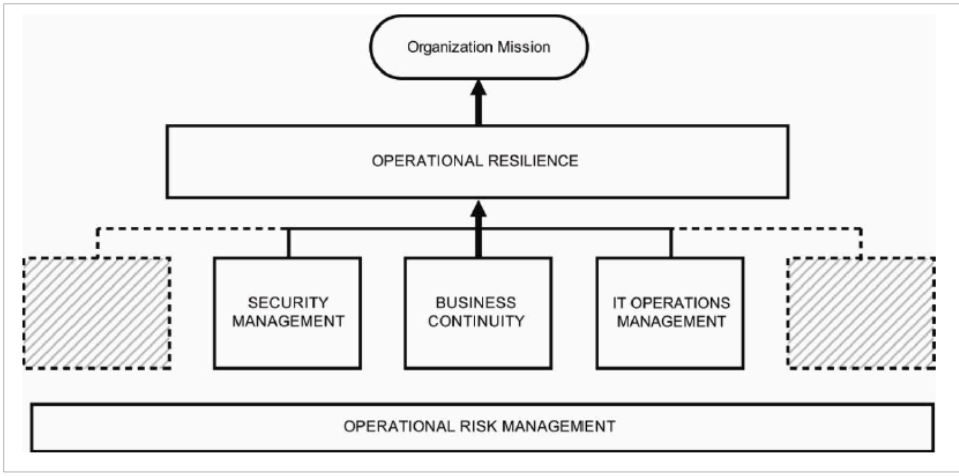

Abbildung 9: Operational Resilience [CACW10b]

Das CERT-RMM besteht aus 26 Prozess-Bereichen und diese sind in vier Kategorien unterteilt: Engineering, Enterprise Management, Operations und Process Management (siehe Tabelle 3).

Tabelle 3: CERT-RMM Process areas [CACW10a]

Engineering		**Operations**	
ADM	Asset Definition and Management	AM	Access Management
CTRL	Controls Management	EC	Environmental Control
RRD	Resilience Requirements Development	EXD	External Dependencies Management
RRM	Resilience Requirements Management	ID	Identity Management
RTSE	Resilient Technical Solution Engineering	IMC	Incident Management and Control
SC	Service Continuity	KIM	Knowldge and Information Management
Enterprise Management		PM	People Management
COMM	Communications	TM	Technology Management
COMP	Compliance	VAR	Vulnerability Analysis and Resolution
EF	Enterprise Focus	**Process Management**	
FRM	Financial Resource Management	MA	Measurement and Analysis
HRM	Human Resource Management	MON	Monitoring
OTA	Organizational Training and Awareness	OPD	Organizational Process Definition
RISK	Risk Management	OPF	Organizational Process Focus

Das CERT-RMM stellt verschiedene Modellsichten (Engineering, Operations, Enterprise Management und Process Management) wie auch Objektsichten (Personen, Informationen, Technologien und Ausstattungen) mit unterschiedlichen Perspektiven dar. Für die Resilience von Informationssystemen ist, wie in Abbildung 10 zu sehen ist, die Objektsicht Technologie relevant, welche die Komplexität der Software- und Systemresilience wie auch die Architekturresilience thematisiert.

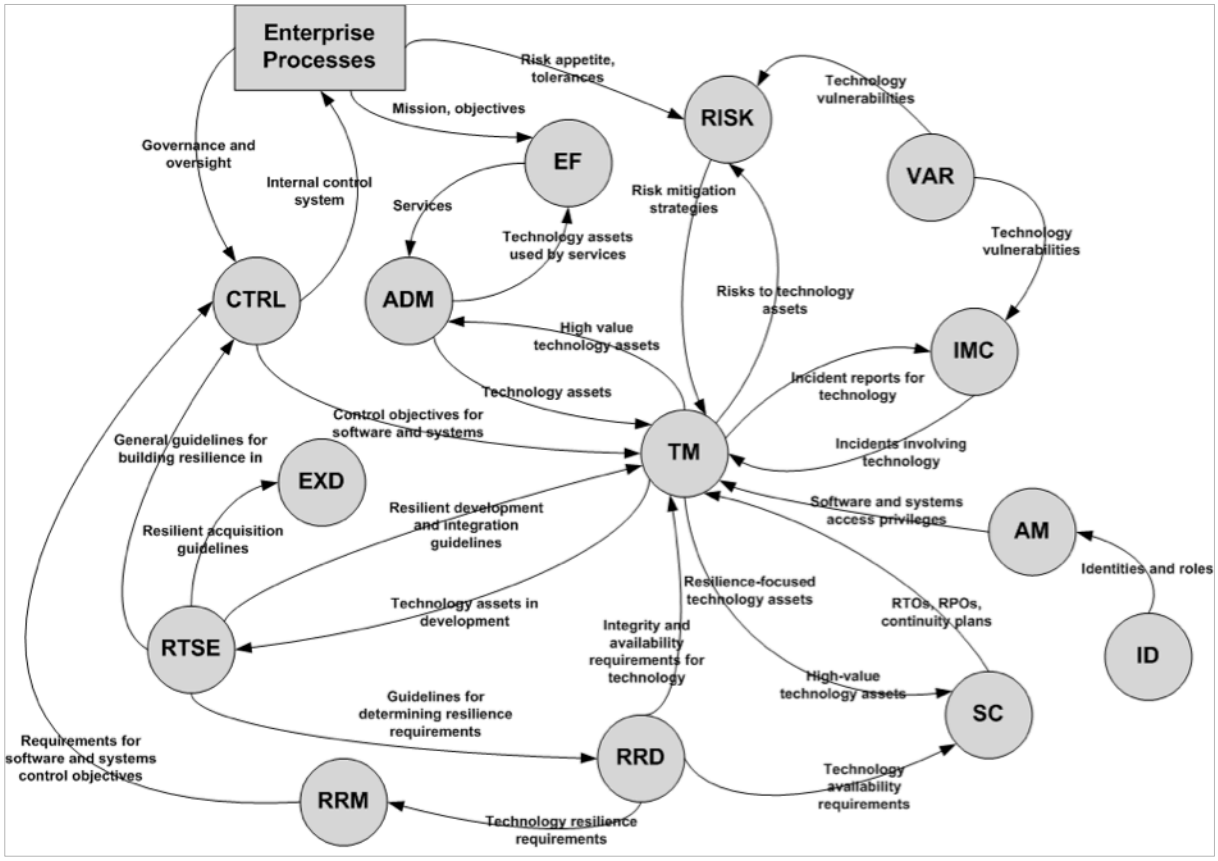

Abbildung 10: CERT-RMM Technology Resilience [CACW10b]

Die Aufgabe des Technologiemanagements ist es, eine Kontrollebene für die Integrität und Verfügbarkeit der Technologie (Software, Hardware, Firmware, Netzwerkverbindungen) zu schaffen, mit dem Ziel, widerstandsfähige Operationen zu unterstützen, aufzubauen und zu managen. Die unterstützenden Prozesse des Technologiemanagements sind:

- Festlegung der Resilience Anforderungen (RRD, RRM, RTSE)
- Identifikation, Definition und Management der Technologien (ADM, ID, IMC)
- Risikomanagement (RISK, VAR)
- Unternehmenssteuerung (CTRL)
- Zugriffskontrolle (AM)
- Entwicklung von Service Continuity Plänen (SC)
- Festlegung der Beziehungen mit externen Instanzen (EXD) [CACW10b]

Um das CERT-RMM mit dem Fokus auf die Technologie-Resilience anzuwenden, sind nun folgende Schritte durchzuführen:

- **Feststellung und Priorisierung der Technologien** Welche Technologie kann zur Unterstützung widerstandsfähiger Systeme eingesetzt werden?
- **Technologie-Schutz** Administrative, technische und physische Kontrollen werden identifiziert und eingeführt.
- **Technologiemanagement** Technologierisiken werden identifiziert und bewältigt.
- **Integrität der Technologien** Die Integrität, Konfiguration und Veränderungen der widerstandsfähigen Technologien werden verwaltet.
- **Verfügbarkeit der Technologien** Die Verfügbarkeit, Funktionalität, Aufrechterhaltung, Belastbarkeit und Interoperabilität der Technologien werden verwaltet. [CACW10b]

3.2 Technologie-Resilience

Da nun ein Leitfaden für die Umsetzung eines Prozessmanagements für die Einführung widerstandsfähiger Technologien in kleinen und mittleren Unternehmen vorgestellt wurde, wird folgend eine Analyse der bestehenden und zukünftigen Technologien erarbeitet. Computernetzwerke und insbesondere das Internet sind fest in der Gesellschaft verankert, um permanenten Zugriff auf Informationen und Services zu ermöglichen, Finanzgeschäfte abzuwickeln, und online zu kommunizieren. Das Internet wird als Routine für Geschäftsprozesse und die weltweite Wirtschaft wie auch die globale Gesellschaft angesehen. Ein Zusammenbruch des globalen Netzwerks hätte große Auswirkungen auf Einzelpersonen, Institutionen und die wirtschaftliche Stabilität und Sicherheit. [StHu15] Die Resilience von Netzwerkinfrastrukturen wird somit als notwendig eingestuft und folglich sind die erwartenden Anforderungen an das „Future Internet“ unter anderem Zuverlässigkeit, Fehlertoleranz, Sicherheit, Mobilität, Anpassungsfähigkeit, Widerstandsfähigkeit und Energieeffizienz. [BeFD10] Diese Anforderungen können in zwei Disziplinen, nämlich der Toleranz und der Zuverlässigkeit, klassifiziert werden, und als Überbegriff Sicherheit zusammengefasst werden. Sie können auch durch Maßnahmen erweitert werden und über die Robustheit verbunden sein (vergleiche Abbildung 11). Fehlertoleranz, Überlebensfähigkeit, Störungstoleranz (Herausforderungen entstehend durch Umwelt und Netzwerkarten) und Datenverkehrtoleranz (DDoS Angriffe) sind Teil der Anforderungen im Sinne der Toleranzherausforderungen. Die allgemeinen Schutzziele der Informationssicherheit wie Vertraulichkeit (confidentiality), Integrität (integrity), Verfügbarkeit (availability), Zuverlässigkeit (reliability), Authentizität (authenticy), Instandhaltbarkeit (maintainability),

Verbindlichkeit (non repudiation), Nachvollziehbarkeit (auditability), und Autorisierung (authorisability) wie auch die Quality of services (QoS) sind Teil der Resilience Anforderungen zum Schutz von Informationen und Daten. [StHu15]

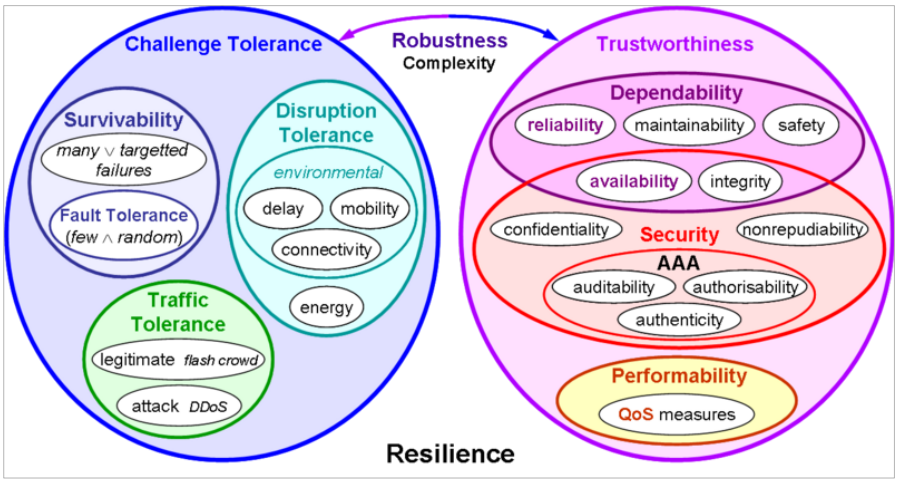

Abbildung 11: Resilience Anforderungen [StHu15]

3.2.1 IT-Infrastruktur Resilience Techniken

Mit IT Outsourcing-Aktivitäten wird heute immer mehr der Begriff Cloud-Computing in Verbindung gebracht. Für kleine und mittlere Unternehmen kann Outsourcing eine Optimierung und Standardisierung von IT-Prozessen sowie die Nutzung neuester Technologien ermöglichen und dadurch die Flexibilität steigern. Herausforderungen der Informationstechnologie sind die Senkung der IT-Kosten, die Verbesserung der IT-Sicherheit und die Virtualisierung von IT-Infrastrukturen. [ThZa13]

3.2.1.1 Cloud Computing

Das National Institute of Standards and Technology definiert Cloud Computing wie folgt: „Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.“ [MeGr11]

Cloud Computing Modelle zeichnen sich durch Flexibilität, Kostenreduzierung und Innovation aus. Es werden drei Einsatzmodelle unterschieden, nämlich private Clouds, unternehmensinterne Server mit internen Zugriffen, öffentliche Clouds, diverse Anbieter mit globalem Zugriff, sowie hybride Clouds, eine Verbindung beider Umsetzungsformen. Weiters wird Cloud-Computing durch drei Cloud-Service Modelle definiert:

- **Infrastructure as a Service** (IaaS), die Bereitstellung von IT-Infrastrukturen,

- **Platform as a Servcie** (PaaS), die Bereitstellung von Programmier-, Entwicklungs- und Laufzeitumgebungen, und
- **Software as a Service** (SaaS), die Bereitstellung von Anwendungsprogrammen und Betriebssystemen. [LeGi03]

Diese klassischen Services können noch durch Storage as a Service und Disaster Recovery as a Service (DRaaS) bzw. Recovery as a Service (RaaS) erweitert werden. [SnRi14]

3.2.1.1.1 Disaster Recovery as a Service (DRaaS)

Cloudbasiertes Disaster Recovery in Form von Disaster Recovery as a Service (DRaaS) oder auch Recovery as a Service (RaaS) befindet sich noch im Entwicklungsprozess. Es werden drei mögliche Architekturmodelle unterschieden:

- **To-Cloud** Die ursprünglichen Daten werden auf einem privaten Server bzw. Rechenzentrum gespeichert und die Cloud wird nur als Back-up und zur Widerherstellung der Daten verwendet.
- **In-Cloud** Alle Daten inklusive dem Backup und der Widerherstellung befinden sich in der Cloud.
- **From-Cloud** Alle Daten befinden sich in der Cloud, jedoch das Backup und die Wiederherstellung erfolgt über ein privates Rechenzentrum. [Mars13] [SnRi14]

3.2.1.1.2 Virtualisierung

Die Widerstandsfähigkeit des heutigen Internets gegen äußere Einflüsse (zum Beispiel Katastrophen) beschränkt sich auf die Netzwerkschicht. Durch die Virtualisierung wird die Widerstandsfähigkeit von Diensten in der Anwendungsschicht zusätzlich unterstützt und die Komplexität der zu verwaltenden Ressourcen (physikalisch wie auch virtuell) erhöht. Durch die rechtzeitige Verlagerung virtueller Ressourcen kann dem Ausfall kritischer Hardware entgegengewirkt werden und die Partitionierung physikalischer Ressourcen ermöglicht es den Nutzern die Hardware für mehrere Aufgaben gleichzeitig zu nutzen. Dadurch können mehrere virtualisierte Dienste auf einer einzelnen Hardwareinstanz zusammengeführt werden. Somit stellt die Virtualisierung homogene, flexible und dynamisch rekonfigurierbare Ressourcen zur Verfügung. Es gibt zwei Arten der Virtualisierung: die Aggregation von Ressourcen, die Abbildung virtueller Umgebungen auf mehrere Geräte und das Aufsplitten von Ressourcen, das Aufteilen eines Gerätes in mehrere virtuelle Umgebungen. Bei der Systemvirtualisierung werden Ressourcen gesplittet und es wird eine virtuelle Maschine (VM), bestehend aus einer virtuellen Hardware, erzeugt. Die Abstraktion erlaubt, Dienste im Netzwerk von einer Hardwarekomponente auf eine andere zu migrieren und somit auf den Ausfall von

Hardwarekomponenten zu reagieren. Die Erzeugung virtueller Maschinen und die Zuteilung von Ressourcen erfolgt durch einen VM-Monitor, der mehrere virtuelle Maschinen gleichzeitig und unabhängig voneinander bereitstellen kann. [BeFD10]
Links und Router werden miteinander kombiniert und erzeugen zusammen virtuelle Netzwerke, die sogenannte Netzwerkvirtualisierung. Reduktion des Verwaltungsaufwandes, dynamische Rekonfigurierbarkeit und die Unterstützung unterschiedlicher Netzwerkarchitekturen zählen zu den Vorteilen der Netzwerkvirtualisierung. Bei der Linkvirtualisierung werden zwei Formen unterschieden, das Virtual Local Area Network (VLAN) und das Virtual Private Network (VPN). VLAN ermöglicht eine logische Segmentierung lokaler Netzwerke auf der Verbindungsschicht und VPN erstellt verschlüsselte Tunnel und verbindet damit entweder einzelne Rechner untereinander, einzelne Rechner mit einem Netzwerk oder mehrere Netzwerke untereinander über das öffentliche Internet. [BeFD10] Cisco [Cisc08] beschreibt zwei Konzepte der Routervirtualisierung, nämlich den Software-Isolated Virtual Router (SVR) und den Hardware-Isolated Virtual Router (HVR). Bei beiden Konzepten werden Ressourcen per Software oder Hardware voneinander isoliert.
Ein weiterer Ansatz zur Virtualisierung sind Peer-to-Peer (P2P) Netzwerke, die Erzeugung logischer Links auf der Applikationsebene. Es werden zwischen reinen P2P-Overlays, alle Peers haben die gleichen Aufgaben und hybriden P2P-Overlays, unterschiedliche Peers haben unterschiedliche Aufgaben, unterschieden. Wenn die Erzeugung des Overlays einem bestimmten Muster (zum Bespiel einem Ring) folgt, wird von einem strukturierten P2P-Overlay gesprochen, wenn dies nicht der Fall ist, von einem unstrukturierten P2P-Overlay. [BeFD10]

3.2.2 Internet Resilience Techniken

Das heutige Internet funktioniert erstaunlich gut, es kann jedoch nicht als widerstandsfähig bzw. „resilient“ bezeichnet werden. Im Laufe der Jahre haben sich jedoch die Anforderungen an das Internet weiterentwickelt. Beeinträchtigungen wie der Ausfall eines Routers oder ein Denial-of-Service Angriff können Funktionen eines Systems einschränken. Zur Abwehr von Beeinträchtigungen werden einerseits proaktive Mechanismen, wie der Einsatz von redundanten Servern und Verschlüsselungen, andererseits reaktive Mechanismen wie der Einsatz von Firewalls, eingesetzt. Eine Übersicht verschiedener Resilience Techniken ist in Tabelle 4 nachzulesen und wird in den nächsten Unterkapiteln noch näher beschrieben. [KaFC10]

Tabelle 4: Übersicht verschiedener Resilience Techniken (ISO/OSI Referenzmodell) [KaFC10]

OSI-Schicht	Technik	Verbreitung
7 Anwendungsschicht	Peer-to-Peer-Netze, DHTs	Zunehmend verbreitet
7 Anwendungsschicht	Server-Virtualisierung, Cloud Computing	Zunehmend verbreitet, Umzug in anderes Subnetz zur Zeit noch schwierig
7 Anwendungsschicht	DNSSEC	Mittelfristige Einführung
7 Anwendungsschicht	DNS-Balancing	Weit verbreitet
5 Sitzungsschicht	RSerPool	Bald verfügbar
4 Transportschicht	SCTP	Verfügbar, derzeit kaum verwendet
4 Transportschicht	TCP	Extrem weit verbreitet
4 Transportschicht	HIP, LISP, Mobile IPv6	Zum Teil verfügbar, kaum eingesetzt
3 Vermittlungsschicht	HIP, LISP, Mobile IPv6	Zum Teil verfügbar, kaum eingesetzt
3 Vermittlungsschicht	DNSSEC	Mittelfristige Einführung
3 Vermittlungsschicht	Netzwerk-Staukontrolle	In Entwicklung
3 Vermittlungsschicht	IPv6	Noch gering, nimmt aber zu
3 Vermittlungsschicht	IP-FRR	Bald verfügbar
3 Vermittlungsschicht	Routing-Optimierung	Wird benutzt
3 Vermittlungsschicht	Netzwerkvirtualisierung	Link-Virtualisierung existiert; Router- und Netz-Virtualisierung in Entwicklung
3 Vermittlungsschicht	MPLS-FRR	Weit verbreitet, ausgereift
2 Sicherungsschicht	MPLS-FRR	Weit verbreitet, ausgereift
2 Sicherungsschicht	Netzwerkvirtualisierung	Link-Virtualisierung existiert; Router- und Netz-Virtualisierung in Entwicklung
2 Sicherungsschicht	Protection Switching	Weit verbreitet, ausgereift
1 Bitübertragungsschicht	Protection Switching	Weit verbreitet, ausgereift
-	Clean-Slate-Ansätze	In Entwicklung

Die Funktionsfähigkeit des Internets ist durch das Routing bekannt und unterscheidet sich durch das Intradomain-Routing (Weiterleitung der Pakete innerhalb eines einzelnen Systems) und dem Interdomain-Routing (Datenverkehr über Providergrenzen hinweg zu

einem anderen autonomen System). Intradomain-Routingprotokolle und das Border Gateway Protocol (Interdomain-Routing) können auf Änderungen der Netzwerktopologie reagieren, jedoch erfolgt die Reaktion auf einen Ausfall nicht schnell genug. Dadurch kann das Routing zwischen zwei oder mehreren autonomen Systemen über einen längeren Zeitraum gestört sein und betroffene Netze können während dieser Zeit nicht über das Internet kommunizieren. Bei überlasteten Leitungen können zwar Traffic Engineering Techniken eingesetzt werden, jedoch können diese nur in längeren Zeitintervallen angewandt werden und eine schnelle Reaktion verhindern. Fehlende Sicherheitskonzepte und die geringe Verbreitung von kryptografischen Signaturen sind Probleme, die vermieden werden können. [KaFC10]

3.2.2.1 Heute verwendete Resilience Techniken

Einzelne Teile des Netzwerks sind resilienter als andere und unterscheiden sich durch die verschiedenen Schichten der Netzwerkprotokolle. Die heute verwendeten Resilience Techniken sind:

- **Netzwerktopologien**
- **Protection Switching** Prophylaktische Backup-Pfade werden eingerichtet und reserviert und Ausfälle einzelner Links und Knoten werden durch den Einsatz von Ringtopologie minimiert.
- **Multiprotocol Label Switching** Das MPLS bildet eine Zwischenschicht zwischen der Sicherungsschicht und der Vermittlungsschicht. IP-Pakete werden beim Eintritt in ein MPLS-Netzwerk in MPLS-Pakete eingekapselt. Diese Pakete werden entlang vorkonfigurierter MPLS-Pfade zu ihrem Ziel geleitet und dem normalen IP-Routingprozess übergeben. MPLS ermöglicht Fast ReRouting, wo im Falle eines Hardwareausfalls der Datenverkehr auf Back-up Pfaden umgeleitet wird.
- **Routing** Das Routing wird so optimiert, dass auch bei einem Ausfall keine Überlastungssituation eintritt.
- **Transmission Control Protocol** Das TCP erkennt den Verlust einzelner Pakete und behebt diesen durch den automatischen Neuversand von Paketen. Weiters werden Netzüberlastungen erkannt und die Senderate reduziert.
- **DNS und Content Distribution Networks** DNS ermöglicht dass Servernamen auf mehrere, dynamisch wechselnde IP-Adressen aufgelöst werden und erlaubt dadurch den Einsatz vieler gleichartiger und datenreplizierbarer Server.
- **Virtualisierung, Serverreplikation** Hauptspeicher eines (virtuellen) Betriebssystems können im laufenden Betrieb über das Netzwerk übertragen

werden und das System kann auf einer anderen Hardware wiederhergestellt werden. [KaFC10]

3.2.2.2 Zukünftige Resilience Techniken

Etliche weitere Resilience Technik Verfahren sind im Entstehen oder kurz vor einer breiteren Anwendung.

- **IP Fast ReRoute und andere IP-Routing-Ansätze** Auf jedem Router werden Back-up-Pfade direkt auf IP-Ebene geschaltet, um im Fehlerfall das schnelle Umschalten auf alternative Datenpfade zu ermöglichen.
- **Staukontrolle im Internet** Durch dynamische Routingprotokolle und dynamische Traffic Engineering Protokolle werden kurzfristige Linküberlastungen verhindert.
- **Internet Protokoll, Version 6** Die enorme Vergrößerung des Adressraums behindert Wurmausbreitungen und verhindert das „Stehlen“ von IP-Adressen durch den Einsatz von kryptografischen Signaturen (Secure Neighbor Discovery).
- **Mobile IP, HIP, LISP** Diese Standards erlauben den Wechsel der IP-Adresse während einer Verbindung, zum Beispiel bei einem Umzug des Servers auf eine andere Maschine oder in ein anderes Netz.
- **Stream Control Transmission Protocol** Das SCTP, Nachfolger des TCP, ermöglicht Multithoming, die gleichzeitige Nutzung mehrerer IP-Verbindungspfade.
- **Reliable Server Pooling** Die SCTP-basierte Protokollsuite erlaubt die Verwaltung eines Serverpools und die zuverlässige Verbindung mit solch einem Pool zum schnellen Umschalten zwischen redundanten Servern.
- **DNS Security Extensions** Die DNS Security Extensions sichern DNS-Antworten mit kryptografischen Signaturen gegen Verfälschungen ab.
- **Overlay-Netze** Techniken wie Peer-to-Peer Netze oder virtuelle LAN’s bauen virtuelle Verbindungen oberhalb der existierenden Topologie auf.
- **Netzwerkvirtualisierung** Die Virtualisierung von Netzwerkkomponenten (Links, Router/Switches) erlaubt eine striktere Netztrennung sowie einfachere Netzwartung, Netzerweiterung und Migration virtueller Netzkomponenten.
- **Peer to Peer Netze** Durch ihren inhärenten dezentralen Aufbau liegen Daten und Services im P2P-Netze auf vielen Knoten zugleich und Ausfälle werden systematisch berücksichtigt.
- **Cross Layer Informationsaustausch** Der Cross Layer Ansatz weicht das traditionelle Kommunikationsverbot auf welches besagt, dass die Kommunikation

nur zwischen unmittelbar benachbarter Schichten stattfinden darf, und verbessert somit den Informationsfluss zwischen den verschiedenen Schichten.

- **Clean State Ansätze** Bei aktuellen Forschungsansätzen wird zwischen dem evolutionären Ansatz, also der Verbesserung des Internets durch die Einführung neuer Protokolle, sowie dem revolutionären Ansatz, dem Clean State Ansatz, unterschieden. Dieser Ansatz schlägt vor, die Netzarchitektur vollständig zu überarbeiten, um ein grundlegend neues Internet zu schaffen. Ein neues Konzept könnte es erlauben, Resilience Techniken nicht optional sondern fest in der Architektur des zukünftigen Netzes zu verankern. [KaFC10]

3.3 Energieeffizienz und unabhängige Energieversorgung

Die ansteigenden Energiekosten, der steigende Stromverbrauch von IT- und Kommunikationsinfrastrukturen und die weltweit beabsichtigte Reduktion der CO2-Emissionen sind heute treibende Kräfte für die Entwicklung zukünftiger Technologien. Beim sogenannten Clock Gating wird die CPU-Frequenz durch Techniken wie SpeedStep, PowerNow, Cool'n'Quiet oder Demand Based Switching vermindert, um dadurch die Stromaufnahmen und die Hitzeentwicklung zu verringern. Beim Power Gating können einzelne Bestandteile von Prozessoren deaktiviert werden. Im zukünftigen Internet muss jedoch ein Paradigmenwechsel erfolgen. Im ökonomischen Ressourcenmanagement wird zwischen zwei Prinzipien [BeFD10] unterschieden:

- **Ökonomisches Maximumprinzip (vorgegebener Input, maximaler Output)** Die vorgegebenen Ressourcen werden so genutzt, dass das Ergebnis maximiert wird.
- **Komplementäres Minimumprinzip (vorgegebener Output, minimaler Input)** Um einen energieeffizienten Betrieb der verfügbaren Hardware zu erreichen, wird im Voraus ein Ergebnis definiert und durch den Einsatz einer minimalen Menge von Ressourcen erbracht.

3.4 Aktuelle Forschungsgebiete

Wissenschaftler erkunden Möglichkeiten und Techniken für die schnellere Systemwiderherstellung nach Ausfällen, dem sogenannten Recovery Oriented Computing. [CBFP04] Dabei geht es um den Entwurf von Systemen die sehr schnell wiederhergestellt werden können, sowie um Werkzeuge, die Fehlerursachen in einem aus vielen Komponenten bestehenden System erkennen und die Probleme schnell beheben. Wenn Unternehmen die Ressourcen oder die Erfahrungen fehlen, um eine eigene hoch verfügbare Computerumgebung bereitzustellen, können sie einzelne

Sicherheitsfunktionen an sogenannte Management Security Service Provider (MSSP) auslagern, eine Art Serviceprovider für Sicherheitsmanagement. MSSPs überwachen die Netzwerk- und Rechneraktivität (Monitoring) und testen die Systeme hinsichtlich Anfälligkeiten. Sie können auch selbst Angriffe durchführen (Penetrationstest), um die Sicherheit der Systeme zu kontrollieren. [LaLS10]

4 Vorgehensweise bei der Entwicklung des Lösungsansatzes

Aufbauend auf der literarischen Aufarbeitung der Themengebiete Business Continuity und Resilience von Informationssystemen ist der nächste Schritt die Entwicklung eines Lösungsansatzes, also die Erstellung eines Geschäftsprozessmodells.

4.1 Strategiefindung

Zur Unterstützung der Strategiefindung wurde der Business Process Management Ansatz von [JKSK00] verwendet und dient als Grundlage für die weitere Konzipierung (siehe Abbildung 12). Die Produkte, Geschäftsprozesse und Organisationen stehen untereinander in einer wechselseitigen Beziehung und sind mit der Informationstechnologie eng verbunden.

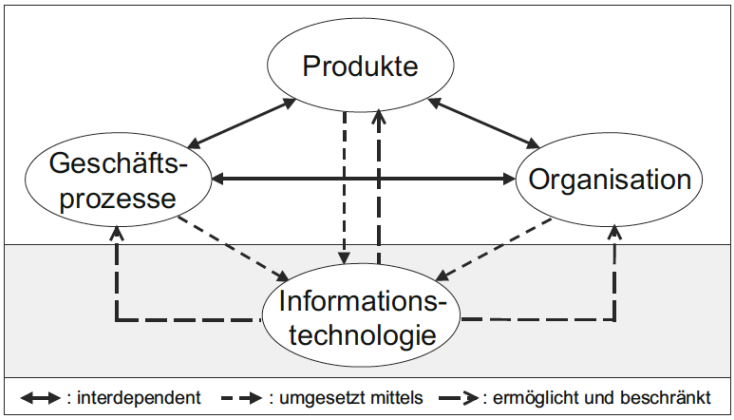

Abbildung 12: Business Process Management Ansatz [JKSK00]

Dieser Business Process Management Ansatz zeigt, dass sowohl die Geschäftsprozesse des Business Continuity Managements modelliert werden, als auch die dazugehörenden Produkte, die Organisation und insbesondere die Informationstechnologie modelliert werden.

4.1.1 Balanced Scorecard

Die Balanced Scorecard (siehe Abbildung 13) als Strategie-Formulierungssystem dient als Unterstützung bei der Strategiefindung. Das Kundensegment sind kleine und mittlere Unternehmen. Lösungen sollten möglichst kostengünstig umzusetzen sein, Veränderungen leicht adaptiert, werden und möglichst alle notwendigen Geschäftsprozesse abgebildet werden. Die Ergänzung der Balanced Scorecard durch die Eigenschaften wie Szenarien- und Unternehmensunabhängigkeit, die Einsatzgebiete im

Wirtschafts- und IT-Sektor (Vorbeugung von Katastrophen) wie auch der Fokus auf Business Continuity Management, Disaster Recovery und Resilience von IT-Systemen runden die Strategie ab.

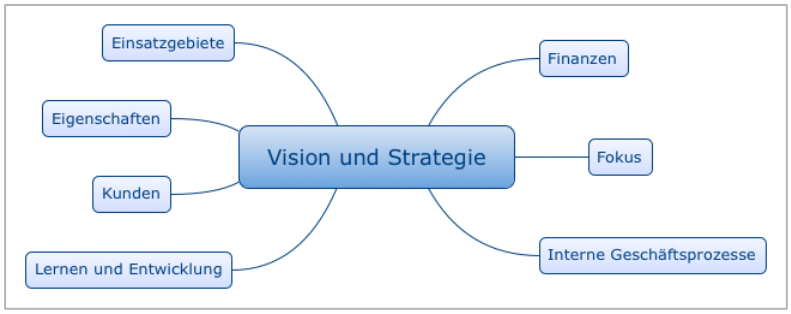

Abbildung 13: Perspektiven der Balanced Scorecard [KaNo96]

4.2 Architekturkonzept

Zur Entwicklung einer Informationssystemarchitektur wurde als Grundlage die Vorlage für die Informationssystemrealisierung von [HaNe09] verwendet, zu sehen in Abbildung 14. Diese IS-Architektur beschreibt Prozesse, Organisation, Funktionen, Daten und Kommunikationsbeziehungen eines Informationssystems.

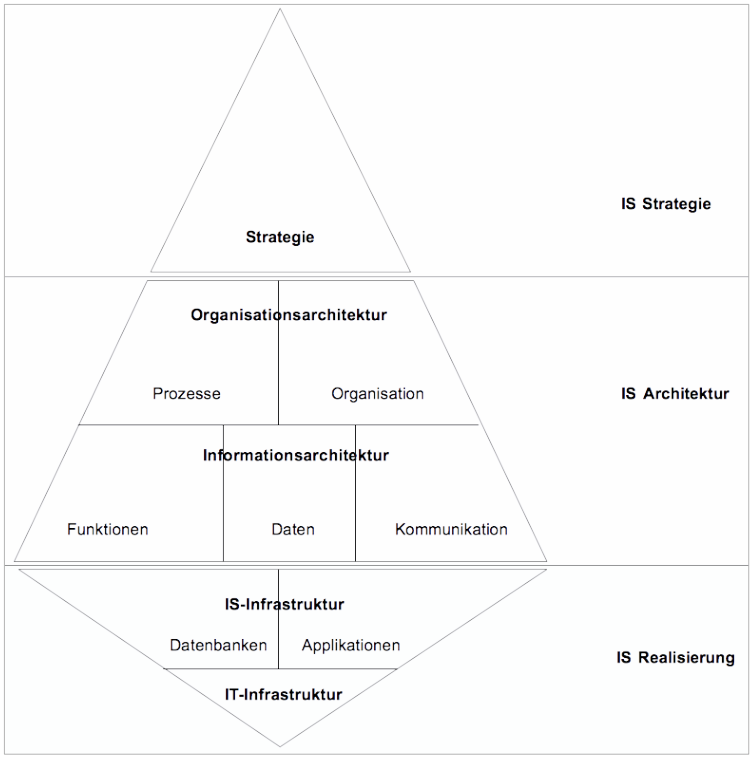

Abbildung 14: IS Architekturplanung [HaNe09]

Bei der Erstellung der IS-Architektur wurden die grundlegenden Aspekte Vollständigkeit, horizontale Integrität, Verständlichkeit und Flexibilität berücksichtigt. [HaNe09] Zusätzlich wurde die Architektur des Boeing Information Service (vergleiche Abbildung 15) [McSp02] herangezogen und mit der IS Architekturplanung kombiniert.

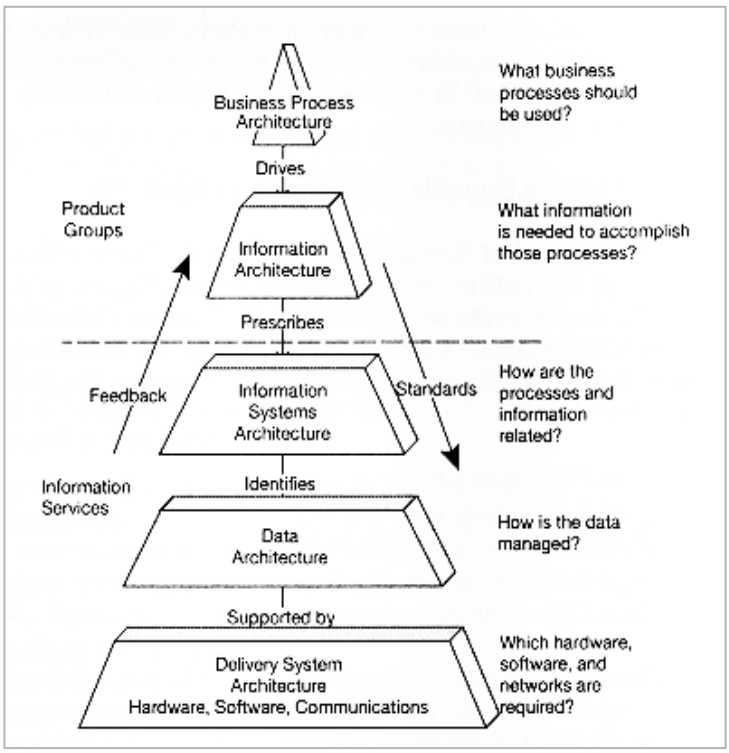

Abbildung 15: The Boeing Information Services [McSp02]

Um nun das komplette Architekturkonzept darzustellen wurde noch der PDCA-Cycle [Baye13] berücksichtigt und, wie in Abbildung 16 zu sehen ist, an das Business Continuity Management [Pint11] angepasst.

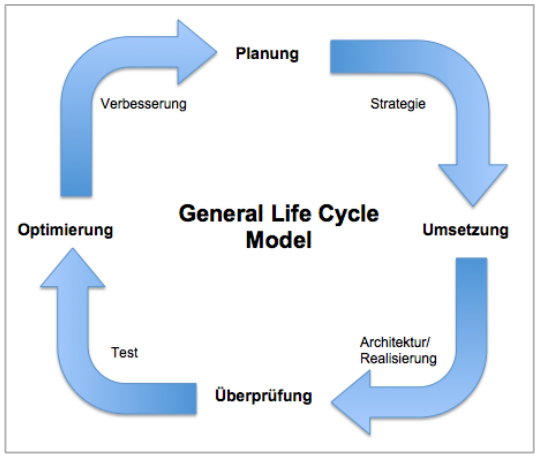

Abbildung 16: General Life Cycle Model [Baye13] [Pint11]

Die Kombination aus der IS-Architekturplanung, dem Boeing Information Service und dem PDCA-Cycle haben, wie in Abbildung 17 zu sehen ist, eine mögliche Architektur für die Umsetzung eines Business Continuity Managements ergeben. Die Planung befasst sich mit der Strategiefindung, die Umsetzung mit der Architektur und der Realisierung, die Überprüfung mit der Verwendung von Tests und die Optimierung mit der Fehlerbehebung.

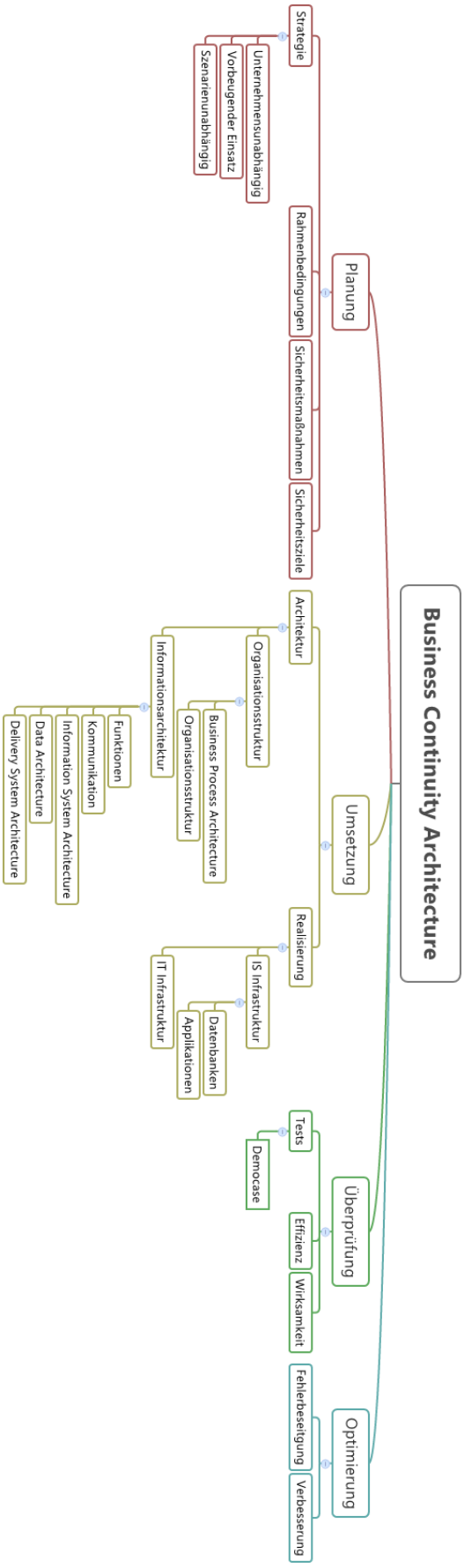

Abbildung 17: Business Continuity Architecture

4.2.1 Zachman Framework

Der letzte Schritt der Entwicklung des Architekturkonzepts ist die Verwendung des domänen- und technologieneutralen Zachman Framework. Dieses Framework dient zur Beschreibung organisationsweiter IT-Architekturen und besteht aus sechs allgemeinen Architektur-Sichten und sechs zu den Architektur-Sichten orthogonal liegenden Sichtenaspekten. Das Grundprinzip des Zachman-Frameworks ist es, dass Systeme komplett modelliert werden können, indem die Antworten auf die Fragen Warum?, Wer?, Was?, Wie?, Wo?, Wann? Beschrieben, und verschiedene Sichten wie die Kontextsicht, die Geschäftssicht, die Systemsicht, die Technologiesicht, die Integrationssicht und die Laufzeitsicht berücksichtigt werden. [VACI09]

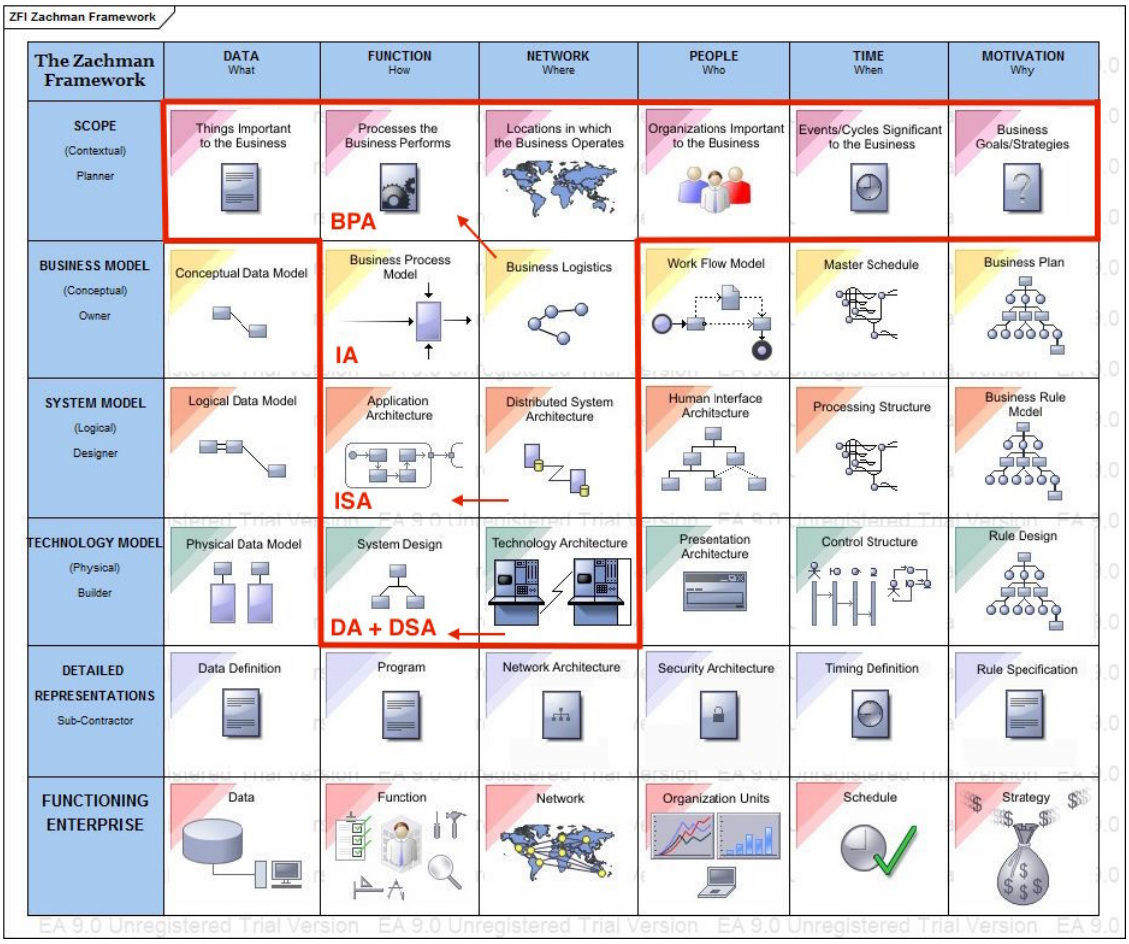

Abbildung 18: Zachman Framework [Ugav07]

Die für die Modellierung der Business Continuity Prozesse relevanten Sichten, kombiniert mit dem Boeing Information Service [McSp02], sind in Abbildung 18 markiert. Die komplette Rolle der Planung (Business Process Architecture), das Unternehmensmodell (Information Architecture), das Systemmodell (Information System Architecture) und das Technologiemodell (Data Architecture und Delivery System Architecture) werden nun im nächsten Kapitel modelliert und getestet.

5 Modellentwicklung

Mithilfe des Architekturkonzepts wird nun ein Framework modelliert, welches in kleinen und mittleren Unternehmen zur Unterstützung bei der Einführung eines Business Continuity Managements eingesetzt werden kann. Als Grundlage für die Modellierung dieses Frameworks diente [SnRi14] und [Bund08a] wie auch die Projektmanagement Austria Baseline [Proj08]. Zur Modellierung der Prozesse wurde das Geschäftsprozessmanagement Tool ADONIS:Community Edition [Boci00] verwendet.

5.1 Projektstrukturplan

Der Projektstrukturplan, ein Orientierungsraster, dient als Übersicht aller Prozesse und besteht aus vier Phasen:

- Projektdefinition
- Projektparameter (Anwendungsbereich, Qualität)
- Projektanforderungen
- Work Breakdown Struktur (Beschreibung aller Arbeitsschritte)
    - Project Definition/Initiation
    - Business Impact Analysis
    - Risikoanalyse
    - Schadensminderungsstrategieentwicklung
    - Business Continuity und Disaster Recovery Plan Entwicklung
    - Training, Testen, Prüfen
    - Aufrechterhaltung des BC/DR Plans [SnRi14]

Der Projektstrukturplan, hier Business Continuity Management genannt (vergleiche Abbildung 19), beginnt mit der organisatorischen Unterstützung, der Projektvorbereitung. Weitere Schiritte sind die Business Impact Analyse, die Risikoanalyse, die Entwicklung der Schadensminimierungsstrategie, die Entwicklung des Business Contiunity und Disaster Recovery Plans, das Training, Testen und die Auditierung sowie die Gewährleistung des Fortbestands des Business Continuity und Disaster Recovery Plans.

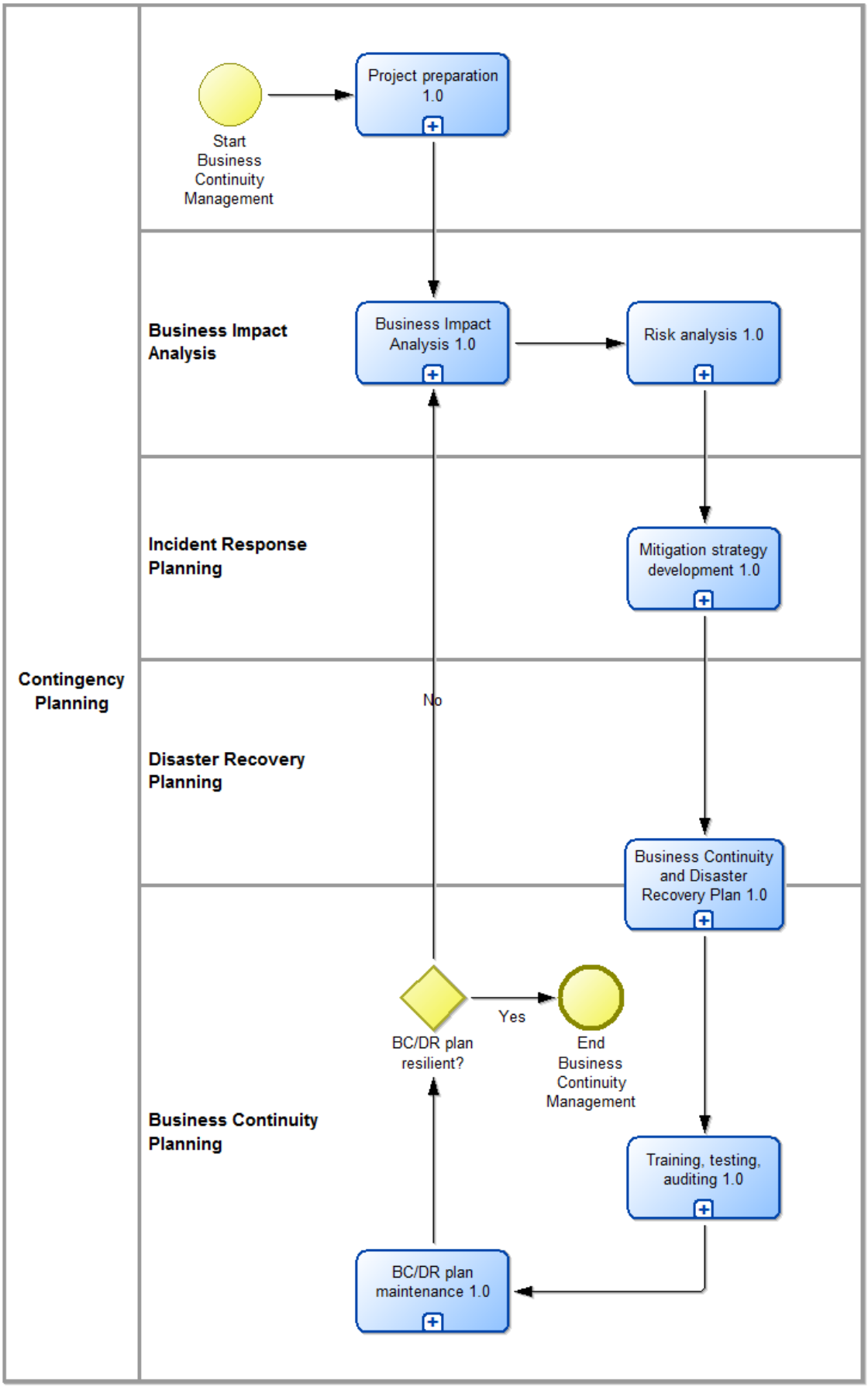

Abbildung 19: Business Continuity Management

5.1.1 Projektvorbereitung

Die wesentlichen Schritte eines Projekts, zu sehen in Abbildung 20, sind die Definition des Projekts, die Auswahl eines Projektteams, die Projektorganisation, die Planung des Projekts, die Projektdurchführung, die Projektverfolgung und der Projektabschluss. [Proj08]

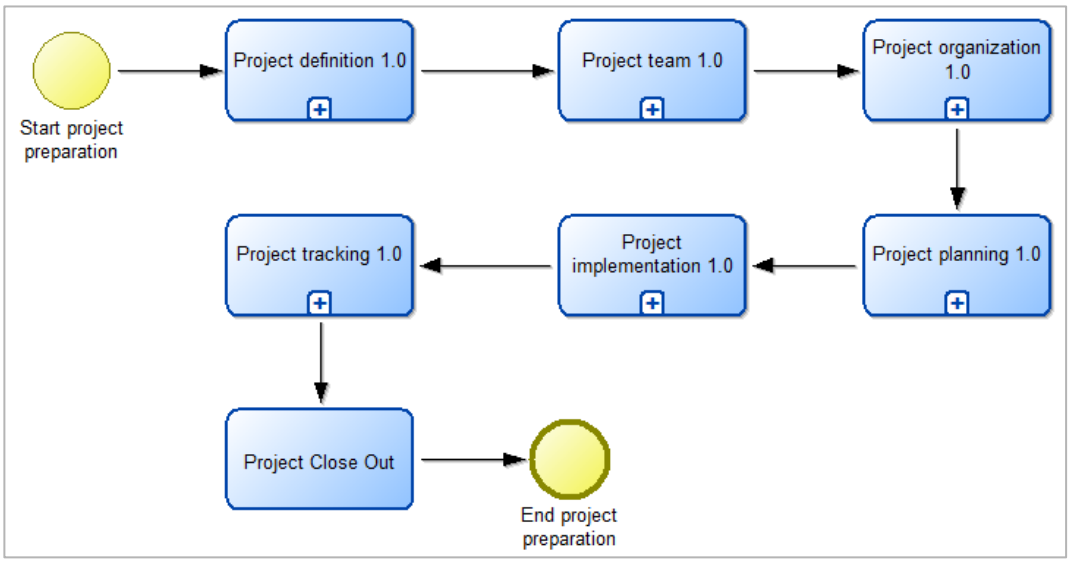

Abbildung 20: Projektvorbereitung

5.1.1.1 Projektdefinition

Die erste Phase der Projektvorbereitung ist die Projektdefinition (siehe Abbildung 21). Der erste Schritt ist die Kontaktaufnahme mit der zuständigen Person zur Projektvergabe, dem sogenannten Projektsponsor. Dieses Gespräch beinhaltet die Übereinstimmung der Erwartungen wie auch die Rahmenbedingungen des Projekts. Die Feststellung der Probleme wie auch des Auftrags und die Entwicklung potentieller Lösungen sind die letzten Schritte des Prozesses zur Festlegung der Erwartungen. Sobald die Erwartungen abgeklärt und vom Projektsponsor genehmigt sind, startet das Projekt mit der Erstellung einer Liste notwendiger Anforderungen und Beschränkungen sowie möglicher Erfolgskriterien. Sollten die Erwartungen falsch definiert sein, werden diese noch einmal neu erarbeitet. Nach der Auswahl des optimalen Lösungskonzepts wird ein Projektvorschlag erstellt und eingereicht. [SnRi14]

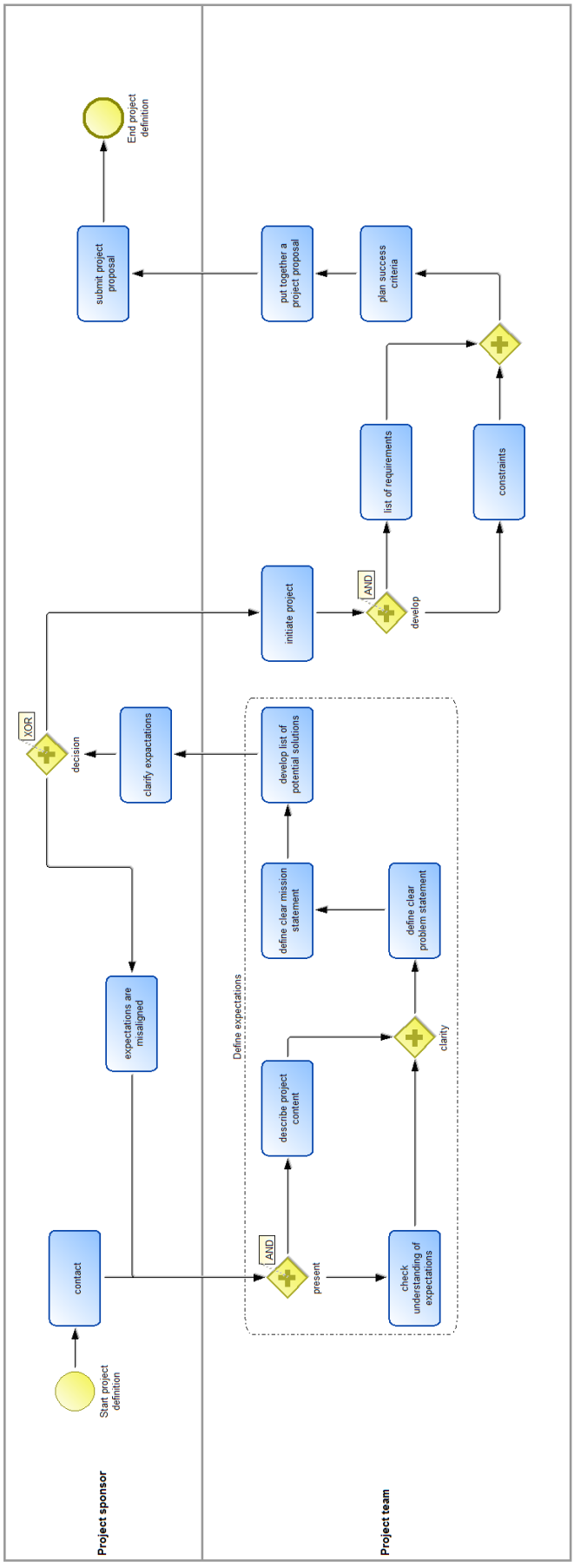

Abbildung 21: Projektdefinition

5.1.1.2 Projektteam

Der nächste Schritt der Projektvorbereitung ist, wie in Abbildung 22 dargestellt, die Bildung eines Projektteams. Experten aus unterschiedlichen Abteilungen werden zur Bildung eines Projektteams herangezogen. Der erste zu rekrutierende Bereich ist die Unternehmensorganisation, als Überblick zur Personalaufstellung. Dies ist hilfreich für die Identifikation der geographischen Lage wie auch die Funktionsdiagnostik des Unternehmens. Technische Spezialisten, insbesondere aus der IT Abteilung, aber auch Spezialisten im Bereich der Funktionalität der Gebäudeeinrichtungen sollten ebenfalls Teil des Projektteams sein. Verantwortliche im Bereich Versorgung und Beschaffung sowie Personen für interne und externe politische Aspekte werden ebenfalls als Experten benötigt und ausgewählt. [SnRi14]

5.1.1.3 Projektorganisation

Der Prozess der Projektorganisation (siehe Abbildung 23), als Hilfestellung zur Durchführung von Projekten, startet mit der Identifikation richtiger Projektsponsoren. Die Entwicklung von Projektzielsetzungen erfolgt in den Bereichen der Erstellung eines Business Continuity Plans, ein Plan zum Fortbestand der Operationen, ein Disaster Recovery Plan, ein Crisis Communication Plan, ein Cyber Incident Response Plan wie auch ein Occupant Emergency Plan. Die Projektbeteiligten des Business Continuity und Disaster Recovery Plans sind die Regierung, Ordnungsbehörden, der Finanzmarkt, private wie auch staatliche Aktionäre, Arbeitnehmer, Verkäufer, Zulieferer und Unternehmer. Weitere Interessensvertreter sind Führungskräfte in den Bereichen Facility Management, Human Resource, Supply Chain Management, Operations Management, Marketing/Sales/PR Management, Financial/Legal Management und IT-Management. Auf Interessen und Anliegen der Projektbeteiligten wird eingegangen und diese werden kategorisiert. Der nächste Schritt ist die Bestimmung von technischen und funktionellen Projektanforderungen wie die E-Commerce Funktionalität, der E-Commerce Kundenservice, das Customer Order Fulfillment und die Bezahlung der Mitarbeiter. Weiters sind die Projektparameter Anwendungsbereich, Budget, Zeitplan und Qualität zu definieren. Als Unterstützung des Projekts ist eine Projektinfrastruktur notwendig. Die Verwendung von Ressourcen und Tools wie Computer, Software Applikationen, Testlabore und Kommunikationsgeräte sind essentiell. Teambesprechungen, Berichterstattung, Eskalation, Qualitätskontrolle, Änderungsmanagement und Projektfortschritt sind Projektprozesse, welche als Unterstützung für einen reibungslosen Verlauf des Projekts benötigt werden. Die Erstellung eines Kommunikationsplans erleichtert die abteilungsübergreifende Kommunikation. [SnRi14]

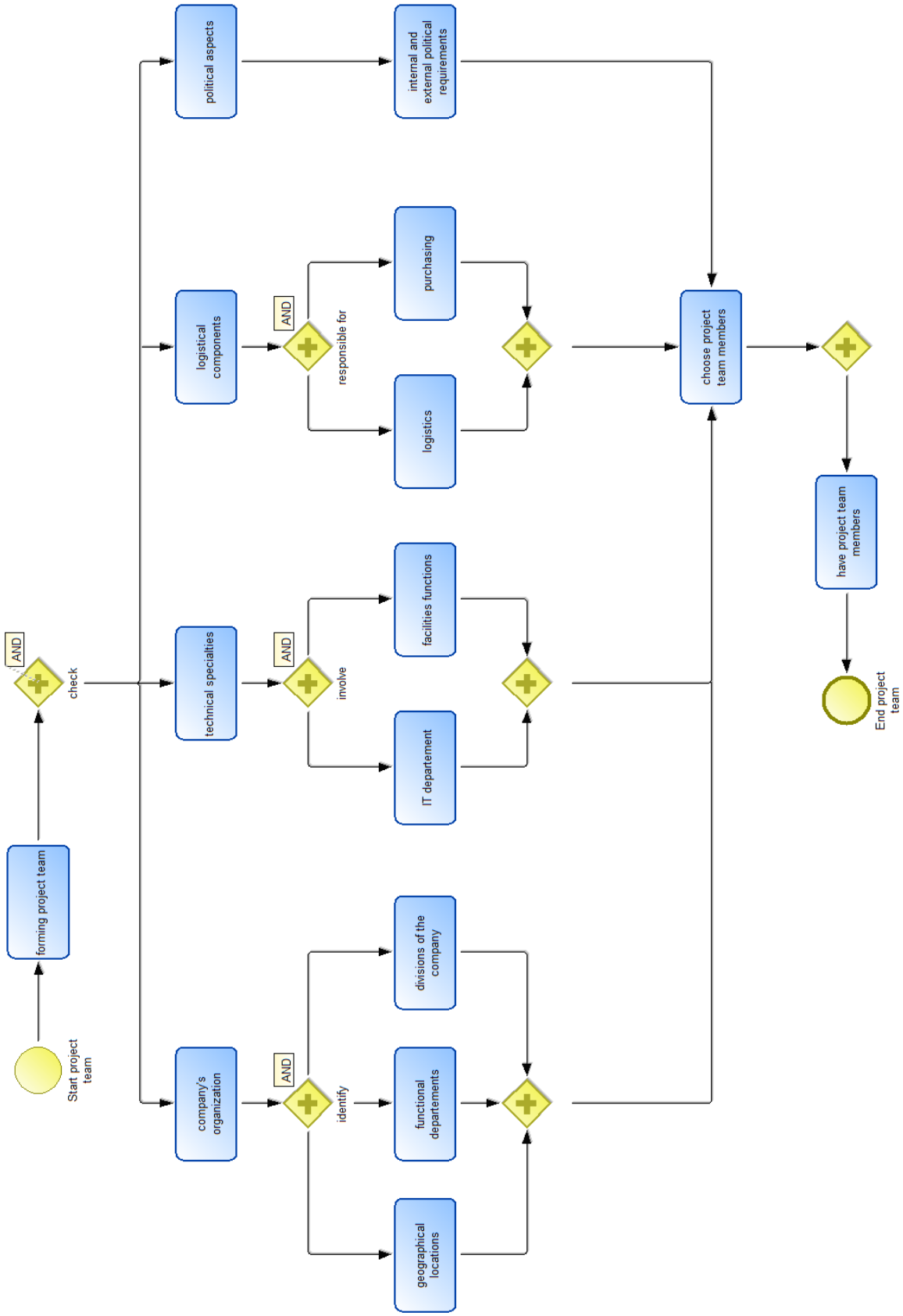

Abbildung 22: Projektteam

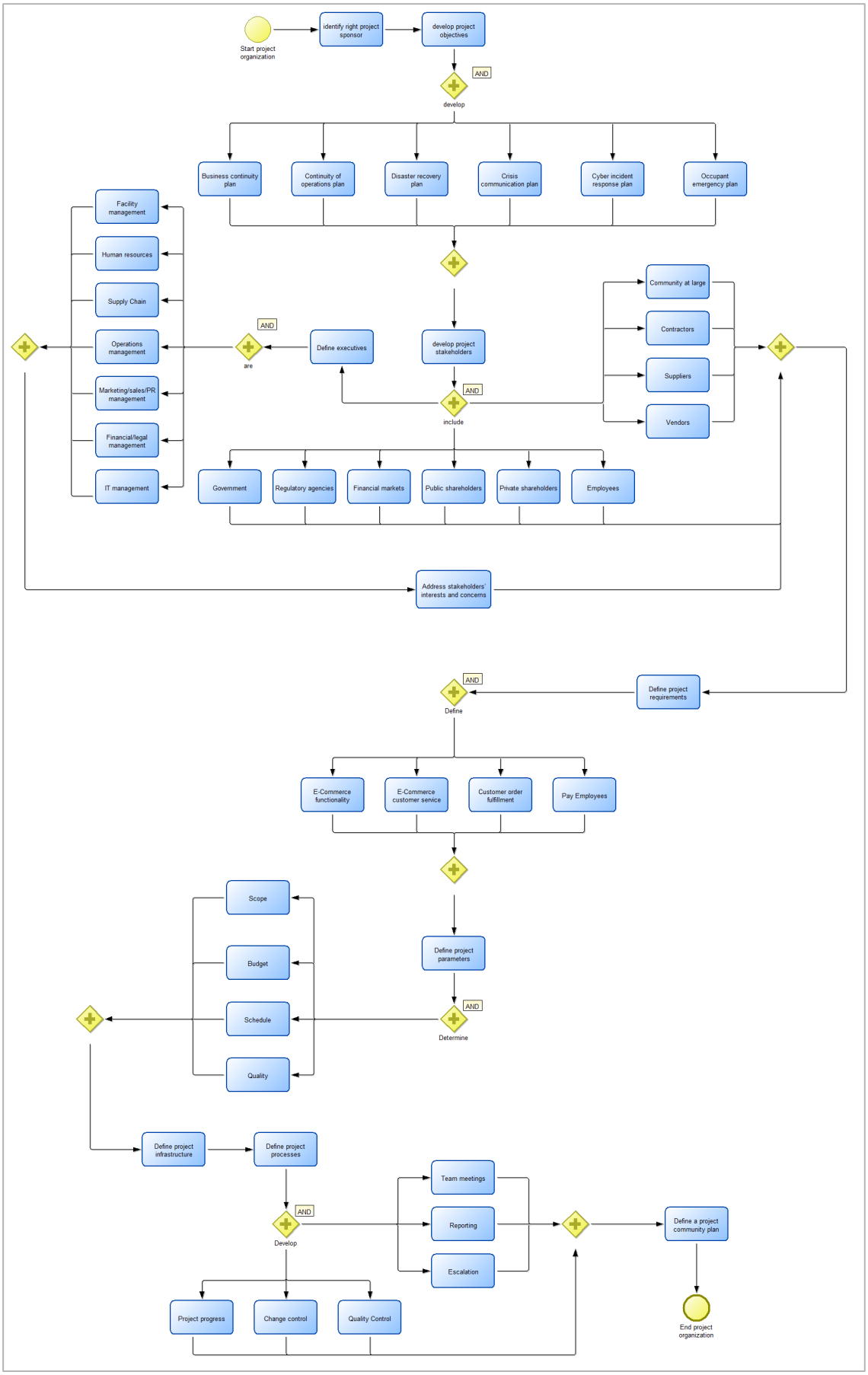

Abbildung 23: Projektorganisation

5.1.1.4 Projektplanung

In der Projektplanungsphase (vergleiche Abbildung 24) liegt der Fokus auf der Entwicklung eines Projektstrukturplans und der Definition des Anwendungsbereichs. [SnRi14]

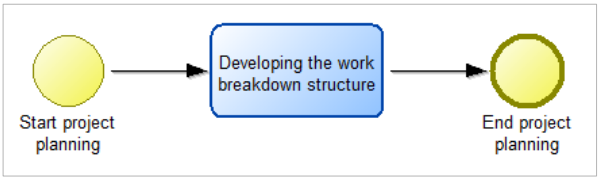

Abbildung 24: Projektplanung

5.1.1.5 Projektrealisierung

Um das Projekt zu realisieren (vergleiche Abbildung 25) sind die Verwaltung des Projektfortschritts wie auch das Bewältigen von Veränderungen von großer Bedeutung. [SnRi14]

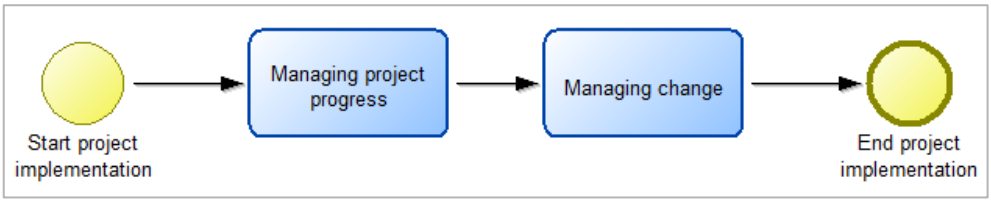

Abbildung 25: Projektrealisierung

5.1.1.6 Projektverfolgung

Mehrere Meilensteine (siehe Abbildung 26) für jede Phase des Projekts sind zu entwerfen, um den Ist-Zustand mit dem Soll-Zustand zu vergleichen. Nach der Projektverfolgung wird das Projekt abgeschlossen. [SnRi14]

Abbildung 26: Projektverfolgung

5.1.2 Business Impact Analyse

Die zentrale Aufgabe einer Business Impact Analyse ist es herauszufinden, welche Geschäftsprozesse für die Aufrechterhaltung des Geschäftsbetriebs und der Institution relevant sind aber auch welche Folgen ein Ausfall haben könnte. Die Business Impact Analyse kann als ein Verfahren definiert werden, im Zuge dessen die Wiederanlaufpunkte der Geschäftsprozesse, eine Priorisierung für den Wiederanlauf und damit die Kritikalität der Geschäftsprozesse festgelegt und die benötigten Ressourcen

identifiziert werden. [Bund08a] Abbildung 27 zeigt die Durchführung einer Business Impact Analyse und ihre Teilschritte. Die Business Impact Analyse startet mit der Erfassung der Stammdaten und Geschäftsprozess und wird fortgesetzt mit der Auswahl relevanter Geschäftsprozesse und Organisationseinheiten, einer Schadensanalyse, der Festlegung von Wiederanlaufparameter, der Berücksichtigung von Abhängigkeiten, der Priorisierung der Geschäftsprozesse anhand ihrer Kritikalität, der Erhebung von Ressourcen für den Normal- und Notbetrieb sowie der Bestimmung der Kritikalität und Wiederanlaufzeiten für Ressourcen.

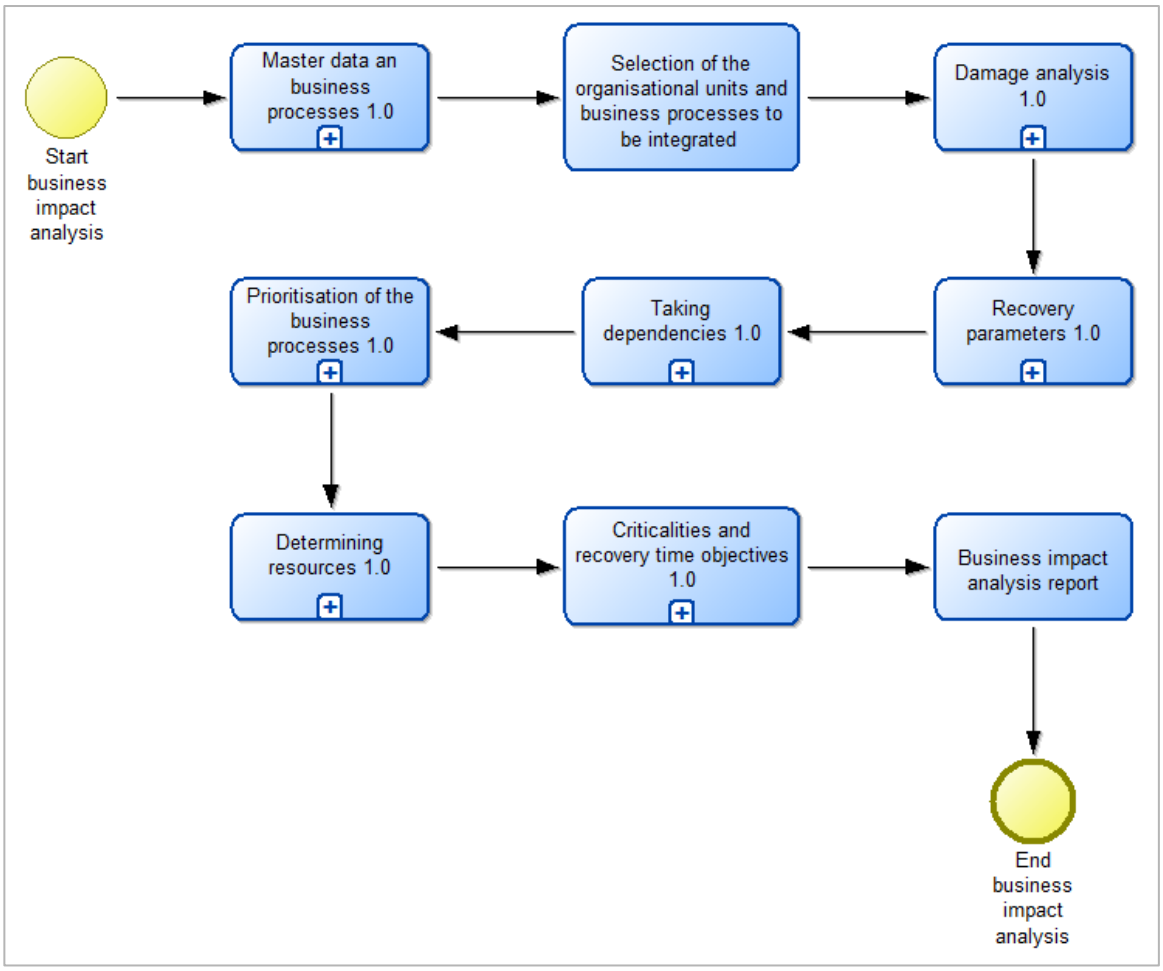

Abbildung 27: Business Impact Analyse

5.1.2.1 Stammdaten und Geschäftsprozesse

Eine Voraussetzung für die Durchführung einer Business Impact Analyse ist die Kenntnis über das Geschäftsmodell, die Aufgaben der Institution und deren Aufbau. Wie in Abbildung 28 zu sehen ist, sollte das Wissen über die Geschäftsprozesse wie auch die Stammdaten der Institutionen vorhanden sein. Im Rahmen der Notfallvorsorge wird eine Geschäftsprozesserhebung durchgeführt wie auch die Abhängigkeiten zwischen den einzelnen Geschäftsprozessen in Form einer Prozesslandkarte (siehe Abbildung 29) aufgezeigt. [Baye13] Zu den Stammdaten zählen Informationen über die Standorte und

die Lieferanten, die Rechtsform, die Branche und über die organisatorische Struktur. Organisationseinheiten und Geschäftsprozesse werden nach ihrer Kritikalität ausgewählt und einbezogen, gegebenfalls auch ausgespart. [Bund08a]

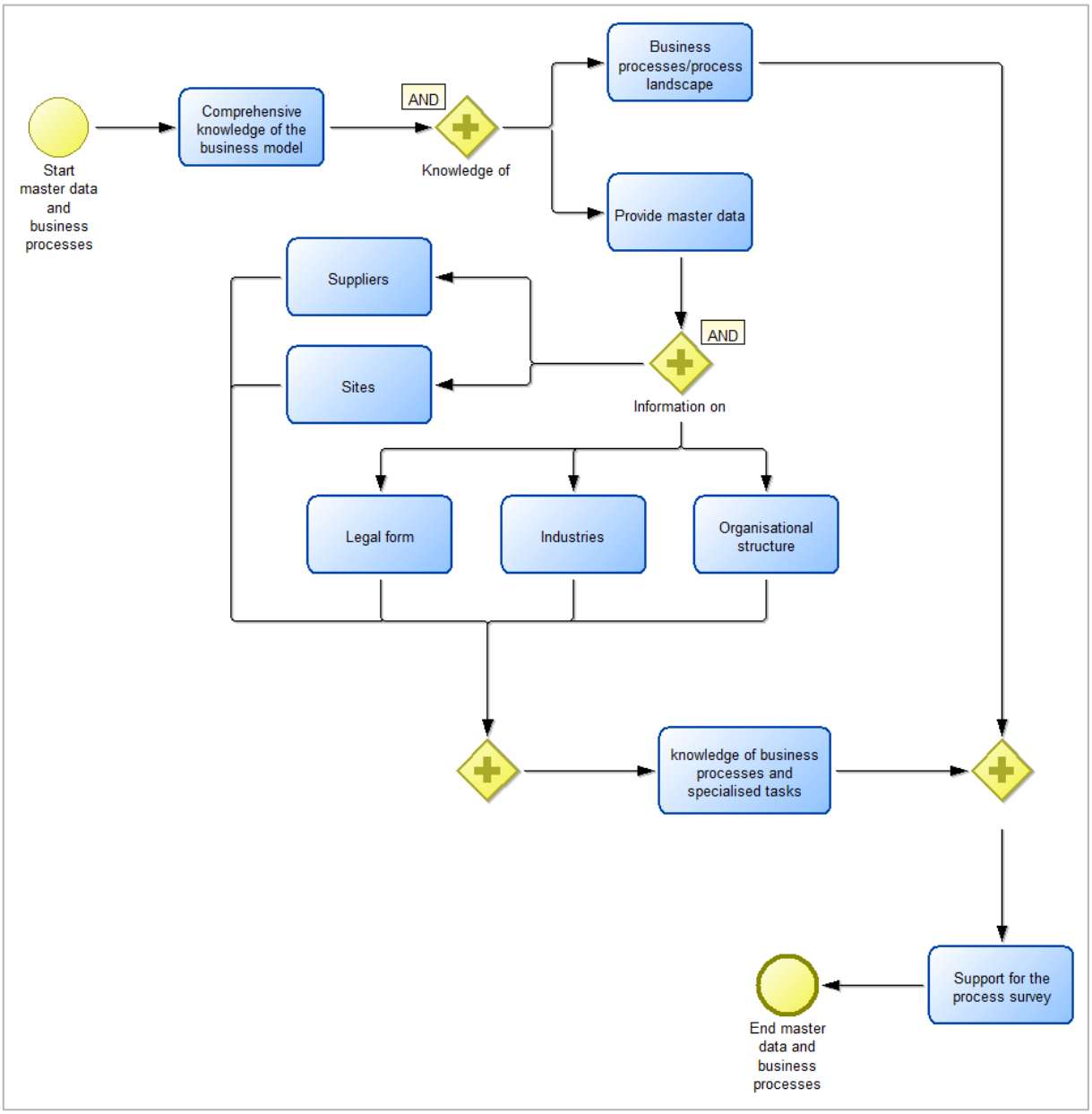

Abbildung 28: Stammdaten und Geschäftsprozesse

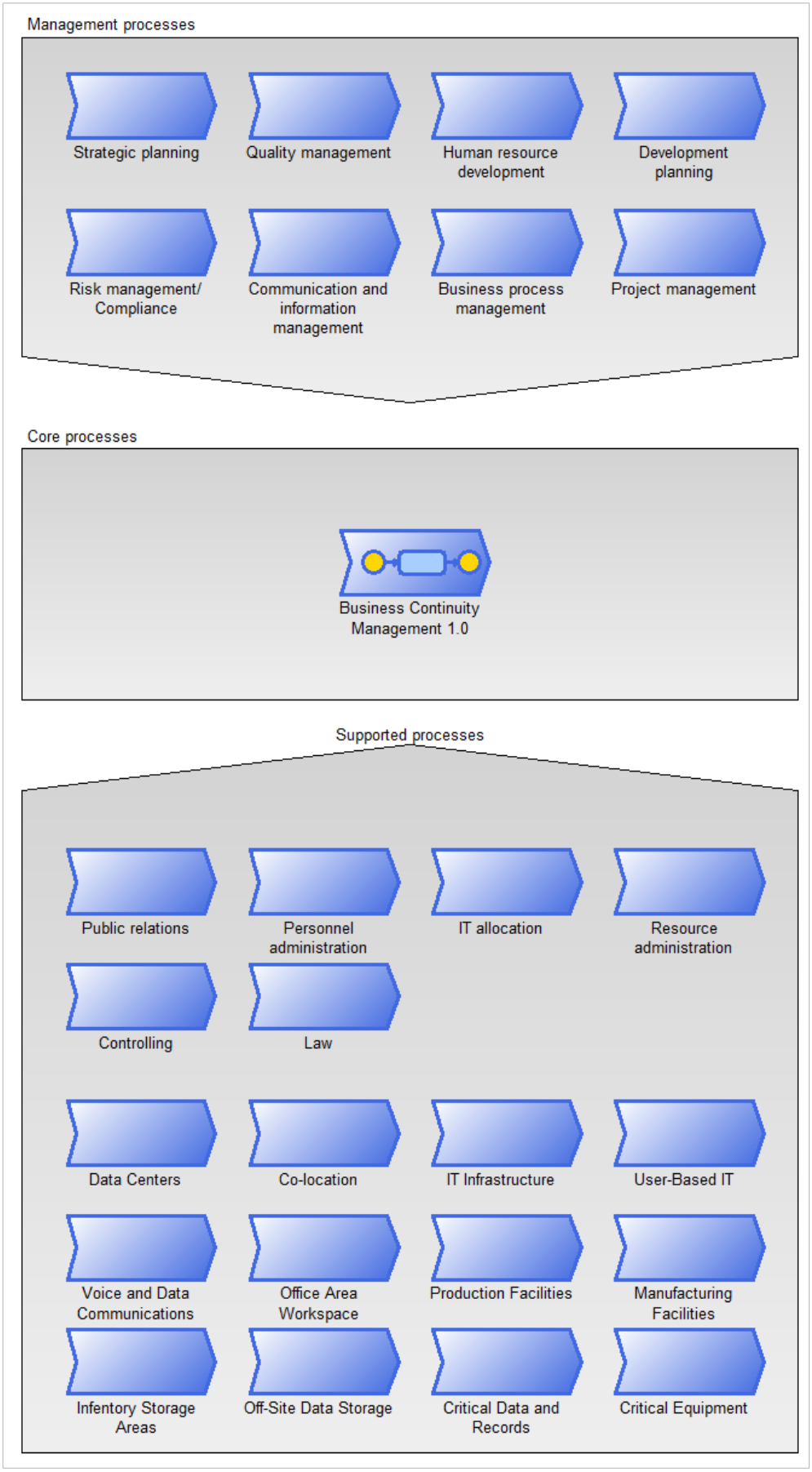

Abbildung 29: Prozesslandkarte

5.1.2.2 Schadensanalyse

Die Schadensanalyse, zu sehen in Abbildung 30, startet mit der Untersuchung von Schäden für die Institutionen, welche durch Ausfälle einzelner Geschäftsprozesse verursacht werden können.

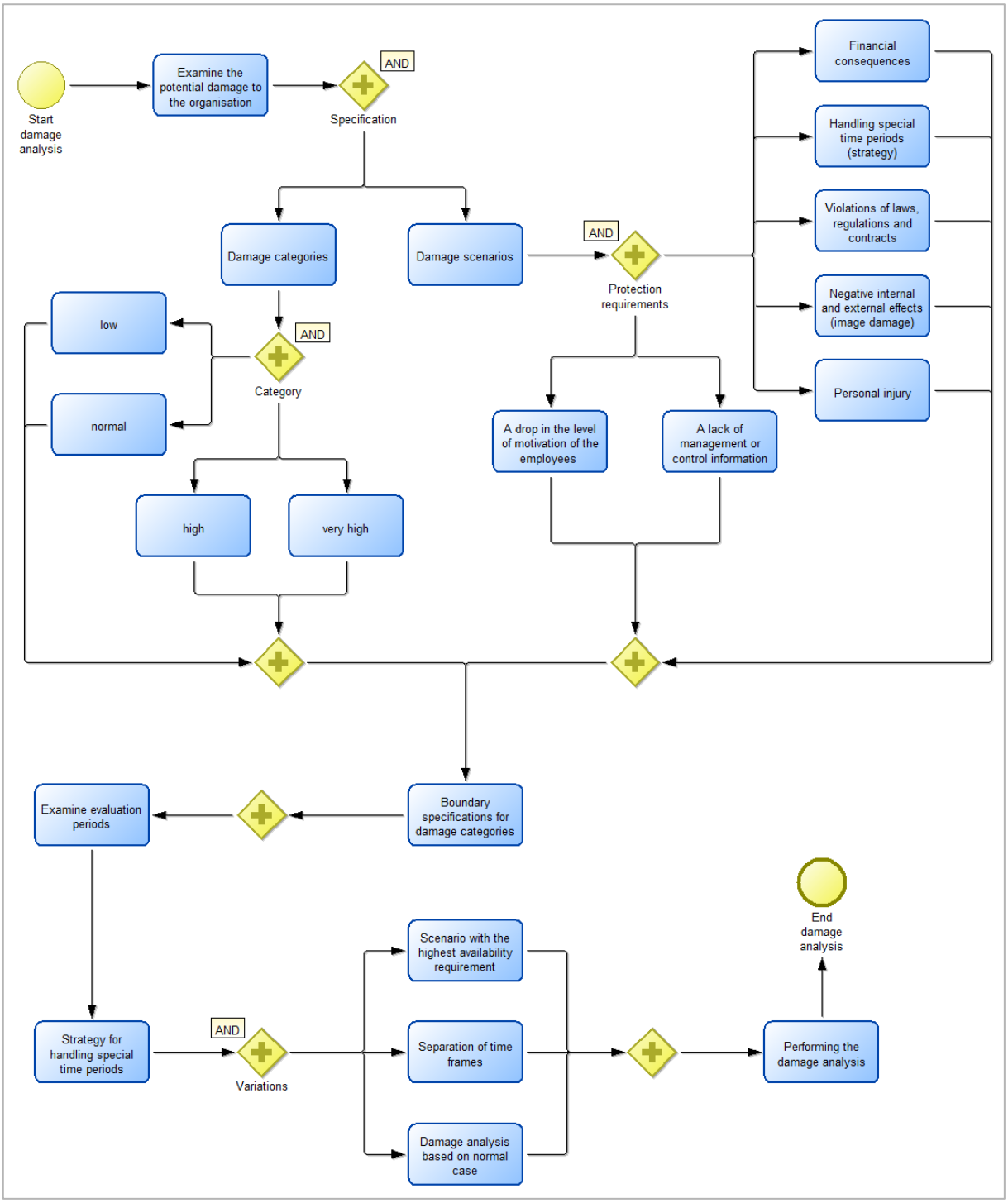

Abbildung 30: Schadensanalyse

Eine qualitative Einstufung in vier Schadenskategorien (niedrig, normal, hoch, sehr hoch) wie auch die Festlegung von Schadensszenarien muss vorgenommen und festgelegt

werden. Diese Schadenskategorien und Schadensszenarien können, wie in Tabelle 5 als Beispiel dargestellt, wie folgt ermittelt werden.

Tabelle 5: Beispiel Ermittlung Schadenskategorien und Schadensszenarien

Schadenskategorie „...“	
Finanzielle Auswirkungen	Beschreibung
Beeinträchtigung der Aufgabenerfüllung	Beschreibung
Verstoß gegen Gesetze, etc.	Beschreibung
Negative Innen- und Außenwirkung	Beschreibung

Schadensszenarien sind unter anderem finanzielle Auswirkungen, Beeinträchtigung der Aufgabenerfüllung, Gesetzesverstöße, Vorschriften und Verträge, negative Innen- und Außenwirkung (Imageschaden) und Beeinträchtigung der persönlichen Unversehrtheit, fehlende Management- oder Steuerungsinformationen oder Rückgang der Mitarbeitermotivation. Bewertungsperioden werden festgelegt, um die Auswirkungen eines Ausfalls eines Prozesses für die Institution zu bewerten und die zeitliche Entwicklung des Schadens aufzuzeigen. Termine und mögliche Ereignisse werden mit deren Eintrittswahrscheinlichkeit erhoben und eine Grobeinschätzung der Schwankungen in den Verfügbarkeitsanforderungen der entsprechenden Prozesse getroffen. Der Schadensanalyse wird die höchste Verfügbarkeit des jeweiligen Geschäftsprozess aus Terminen und Ereignissen für den ganzen Zeitraum, die benötigten Informationen für jede Zeitspanne und der Normalfall zugrunde gelegt. Zuletzt sind für die einzelnen Geschäftsprozesse die Auswirkungen eines Ausfalls für die Institution in den einzelnen Bewertungsperioden anhand der Schadensszenarien abzuschätzen und der Schadensverlauf zu ermitteln. [Bund08a]

5.1.2.3 Festlegung der Wiederanlaufparameter

Im Anschluss an die Schadensanalyse sind Wiederanlaufparameter, die maximal tolerierbare Ausfallzeit (MTPD), die Wiederanlaufzeit (RTO) und das Wiederanlauf-Niveau für die einzelnen Geschäftsprozesse festzulegen (vergleiche Abbildung 31). Der BSI-Standard [Bund08a] definiert die maximal tolerierbare Ausfallzeit eines Prozesses als den „... Zeitrahmen, in der der Wiederanlauf spätestens erfolgen muss, damit die Institution nicht in eine Phase gerät, in der kurz- oder langfristig ihre Überlebensfähigkeit gefährdet ist.“ und die Wiederanlaufzeit ist die „... angestrebte Zeit, in der der Wiederanlauf des Prozesses erfolgen soll. Die Zeit für den Wiederanlauf muss kleiner als die maximal tolerierbare Ausfallzeit sein.“ Der Ablauf des zeitlichen Notfallprozesses ist noch einmal bildlich für ein besseres Verständnis in Abbildung 32 zu sehen.

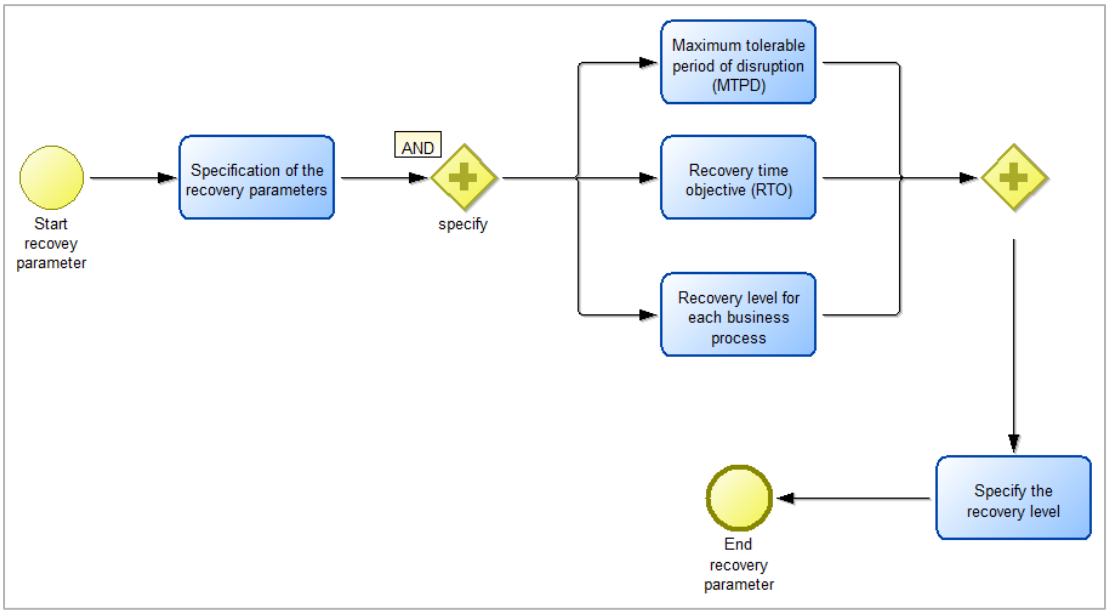

Abbildung 31: Festlegung der Wiederanlaufparameter

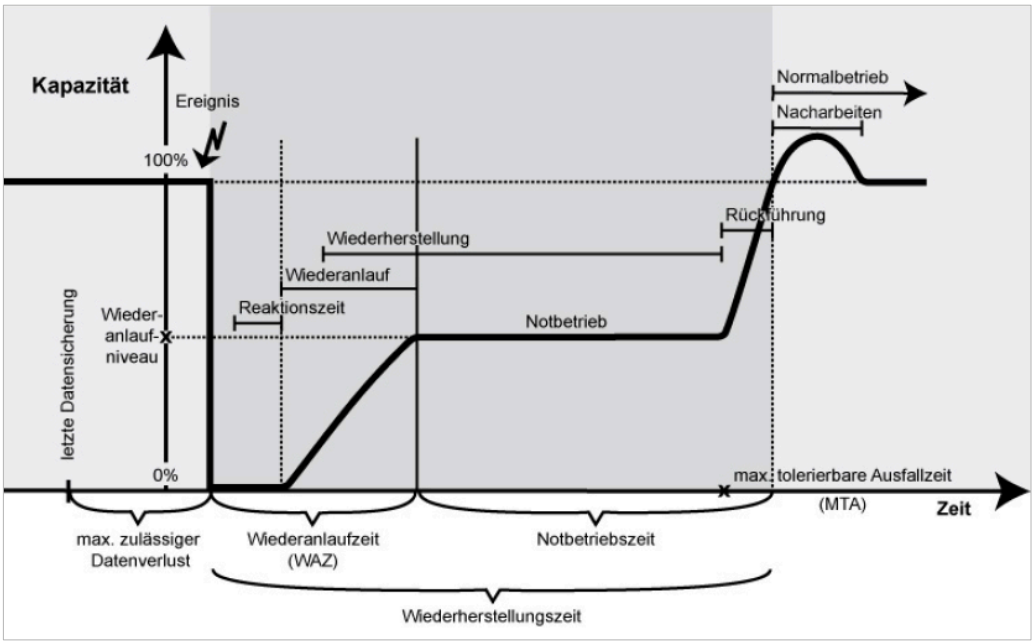

Abbildung 32: Wiederanlaufparameter [Bund08a]

5.1.2.4 Berücksichtigung von Abhängigkeiten

In der nächsten Phase (siehe Abbildung 33) werden die Abhängigkeiten zwischen den Geschäftsprozessen einbezogen und die Verfügbarkeitsanforderungen gegebenenfalls nachkorrigiert. Die Abhängigkeiten zwischen einzelnen Prozessketten werden definiert, die Geschäftsziele werden näher betrachtet sowie Ressourcenabhängigkeiten und die Beachtung besonderer Termine und Ereignisse werden berücksichtigt. [Bund08a]

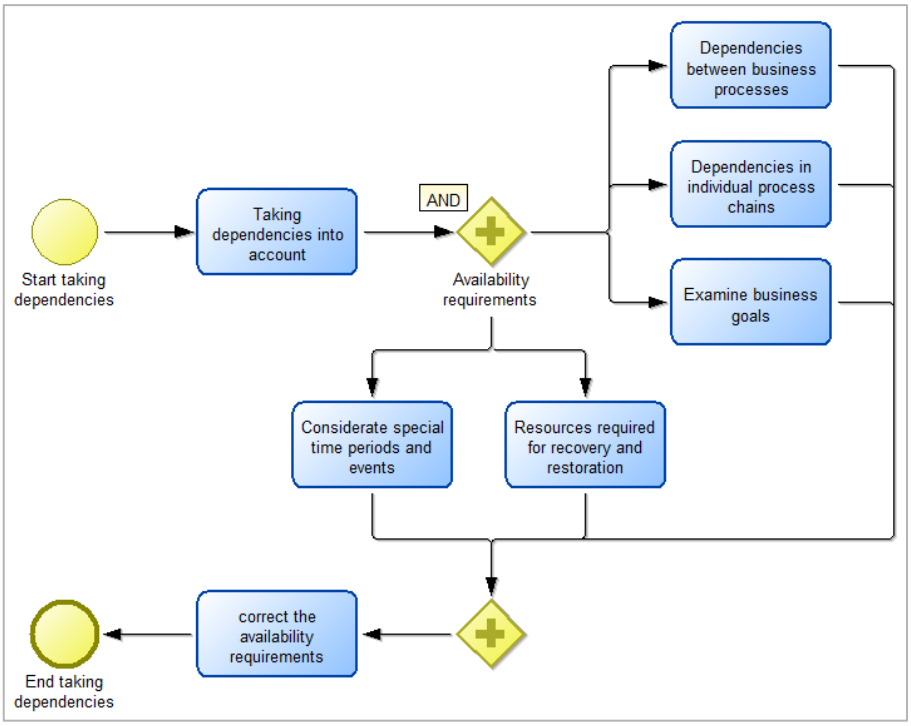

Abbildung 33: Abhängigkeiten

5.1.2.5 Priorisierung und Kritikalität der Geschäftsprozesse

Für die Festlegung der Kritikalität können neben dem Wiederanlauf, der maximal tolerierbaren Ausfallzeit und dem Gesamtschaden Kategorien verwendet werden (siehe Abbildung 34). Die Kritikalitätskategorien könnten unkritisch, wenig kritisch, kritisch und hochkritisch sein. [Bund08a]

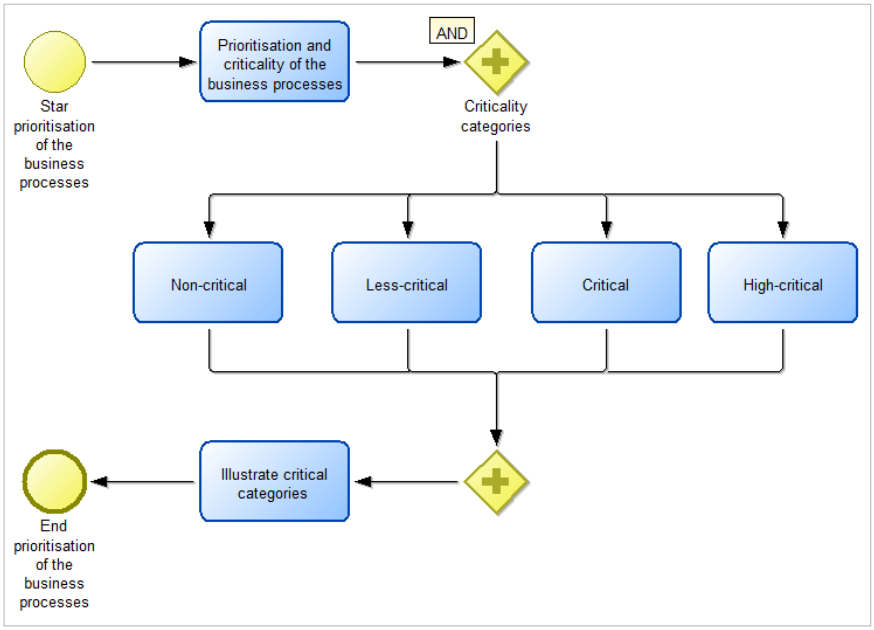

Abbildung 34: Priorisierung und Kritikalität

Tabelle 6 zeigt ein Beispiel einer möglichen Einteilung und Festlegung der Kritikalitätskategorien.

Tabelle 6: Kritikalitätskategorien [Bund08a]

Kritikalitäts-kategorie	Wiederanlauf	Maximale tolerierbare Ausfallzeit	Gesamtschaden nach x Stunden	Allgemein
„unkritisch“	> 720 Stunden	> 504 Stunden	„niedrig	Beschreibung
„wenig kritisch“	≤ 720 Stunden	≤ 504 Stunden	„normal“	Beschreibung
„kritisch“	≤ 168 Stunden	≤ 240 Stunden	„hoch“	Beschreibung
„hoch kritisch“	≤ 4 Stunden	≤ 6 Stunden	„sehr hoch“	Beschreibung

5.1.2.6 Erhebung der Ressourcen für Normal- und Notbetrieb

Welche Ressourcen im Normalbetrieb benötigt werden und welche von mehreren Prozessen genutzt werden, wird nun für kritische Geschäftsprozesse erhoben (siehe Abbildung 35). Zu den Ressourcen für den Normal- und Notbetrieb zählen Personal, Informationen, Informationstechnologie, Dienstleistungen, Infrastruktur und Betriebsmittel. [Bund08a]

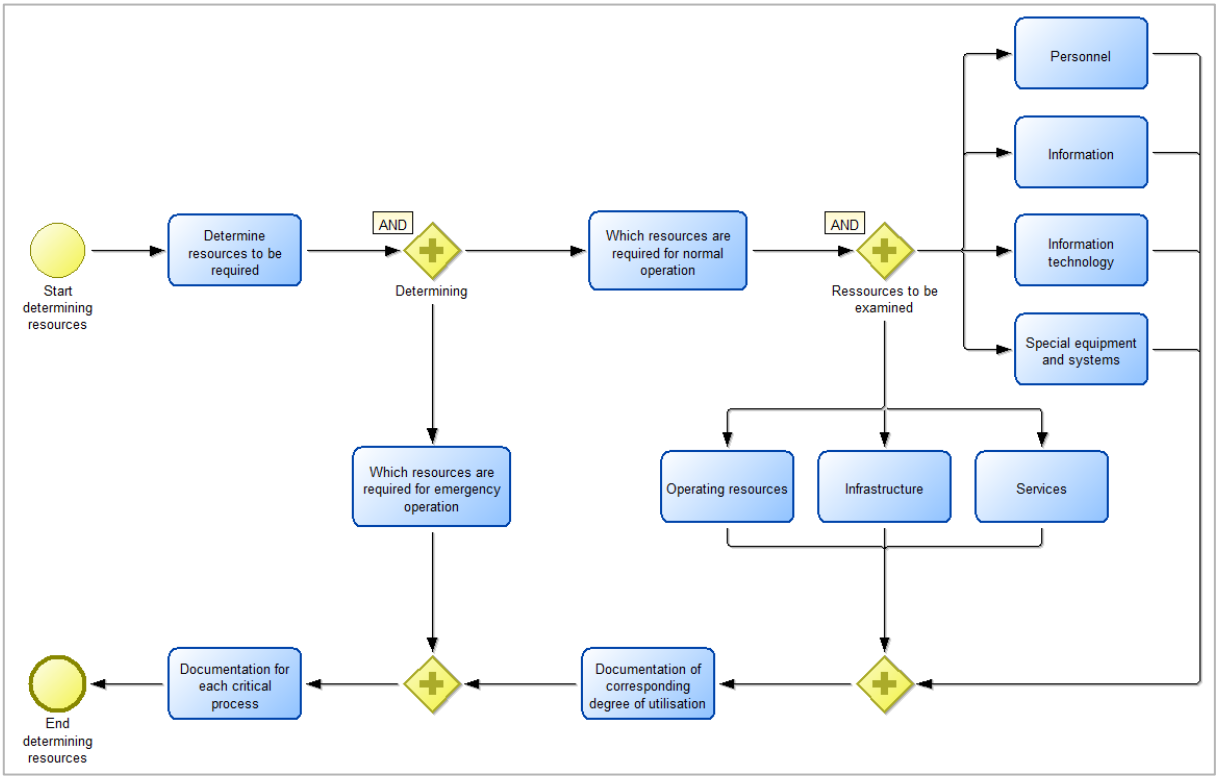

Abbildung 35: Erhebung von Ressourcen

Die Erhebung der benötigten Ressourcen für kritische Prozesse kann das folgenden Schemas (siehe Tabelle 7) zur Unterstützung verwendet werden. Die möglichen Nutzungsgrade werden mit 1 für „sehr hoch“ (unentbehrlich für den Prozess), 2 für „hoch“ (wesentlich für den Prozess), 3 für „mittel“ (wird benötigt) und 4 für „gering“ definiert.

Tabelle 7: Ressourcenerfassung [Bund08a]

Ressourcen			Geschäfts-prozess		Prozess GP1	Prozess GP4	Prozess GP5
			WAZ	kWAZ	92	168	24
			WAZ	kWAZ	72	48	24
Anwendungen		E-Mail	4	4	1	3	-
		Datenbankserver	92	18	1	-	1
		Office Anwendungen	24	24	4	1	1
		SAP	...	...	1	-	-
		EDI	...	...	3	-	-
		Auto CAD	...	...	-	-	1
		Kalender	...	...	4	3	-
		...	...	...	...	...	...
Hardware		Internet Anbindung	48	48	3	-	-
		LAN	...	...	1	1	1
		File Server 1	...	...	1	-	1
		Fileserver 2	...	...	-	1	-
		...	...	...	...	...	...
Infrastruktur		Arbeitsplatz	...	...	1	-	-
		Hochlager	...	...	-	1	-
		Telefonanschluss	...	...	1	-	-
		Fax	...	...	-	2	-
		...	...	...	...	...	...
...		...	...	...	...	...	...

5.1.2.7 Kritikalität und Wiederanlaufzeiten der Ressourcen

Die Kritikalität und die Anforderung an den Wiederanlauf von Ressourcen (siehe Abbildung 36) und die Schutzbedarfsfeststellung von IT-Systemen können mit folgenden Prinzipien ermittelt werden. [Bund08a]

- **Maximumprinzip** Der Schutzbedarf eines IT-Systems wird durch den Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen bestimmt.
- **Kumulationseffekt** Werden mehrere Anwendungen bzw. Informationen auf einem System verarbeitet, dann erhöht sich der Schutzbedarf des IT-Systems und ein hoher Gesamtschaden durch Kumulation mehrerer Schäden auf einem IT-System entsteht.
- **Verteilungseffekt** Eine Anwendung hat einen hohen Schutzbedarf, überträgt ihn aber nicht auf ein betrachtetes IT-System, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen. [Bund08b]

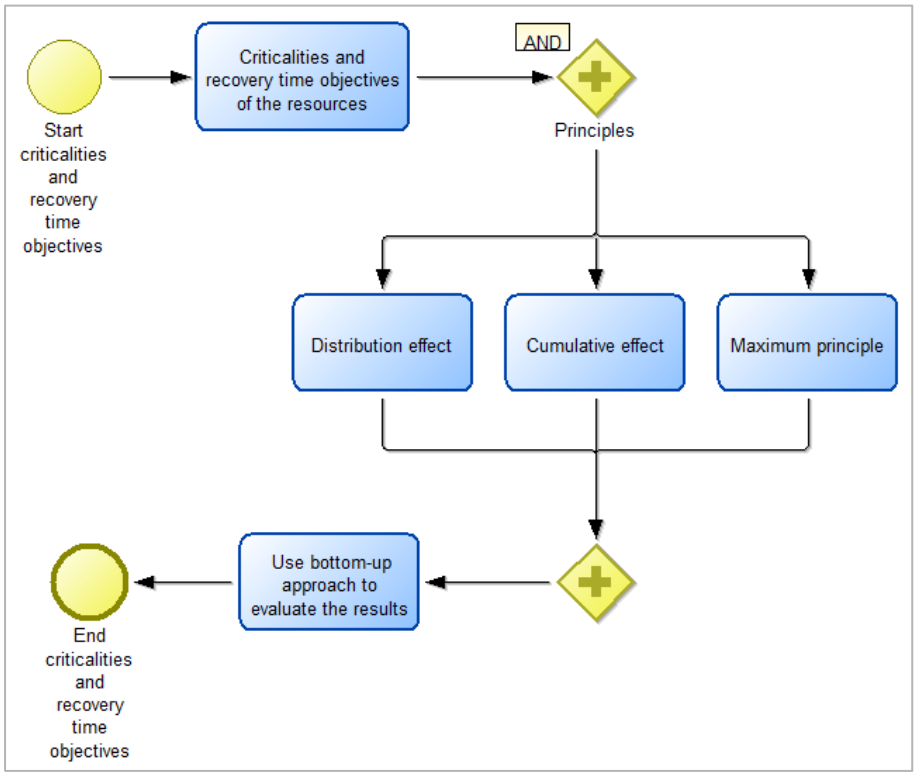

Abbildung 36: Kritikalität und Wiederanlaufzeiten

5.1.3 Risikoanalyse

Die Risikoanalyse (siehe Abbildung 37) dient dazu, die Gefährdungen zu identifizieren, die eine Unterbrechung von Geschäftsprozessen verursachen können und die damit verbundenen Risiken zu bewerten. Die Identifikation der Gefährdung, die für die Institution, den Prozess oder die Ressource relevant sind wie auch eine Risikobewertung

sind durchzuführen. Die Risiken werden durch die Auswirkungen eines Schadens und der Eintrittswahrscheinlichkeit charakterisiert. [Bund08a]

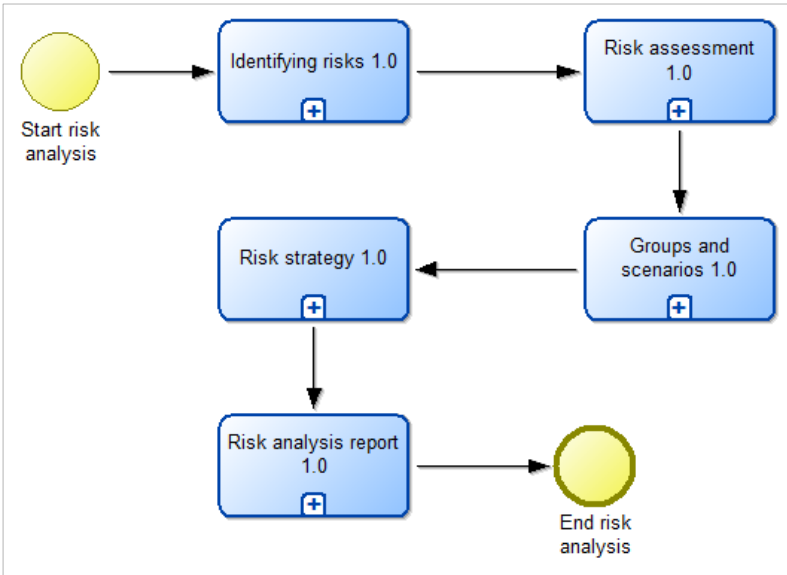

Abbildung 37: Risikoanalyse

5.1.3.1 Risikoidentifizierung

Die Risikoidentifizierung (siehe Abbildung 38) beschäftigt sich mit der Identifizierung möglicher Gefährdungen bzw. Risiken für die kritischen Geschäftsprozesse und es wird die Frage nach den möglichen Ursachen für den Ausfall gestellt. Risiken werden wie folgt kategorisiert:

- Interne und externe Risiken
- Direkt wirkende und indirekt wirkende Risiken
- Durch die Institution beeinflussbare und nicht beeinflussbare Risiken

Zur Identifizierung von offensichtlichen Risiken wird die Kollektionsmethode, beispielsweise Checklisten, SWOT-Analysen oder Interviews, eingesetzt. Zur Identifizierung von weniger offensichtlichen Risiken wird die Suchmethode, beispielsweise FMEA, HAZOP, Fehlerbaumanalyse, morphologische und statistische Verfahren, Brainstorming, Brainwriting, oder die Delphi Methode eingesetzt.

Der nächste Schritt der Risikoidentifizierung ist die Auswahl von Gefährdungen. Dazu zählen höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen wie auch vorsätzliche Handlungen. [Bund08a]

5.1.3.2 Risikobewertung

In dieser Phase, zu sehen in Abbildung 39, sind die identifizierten Risiken auf ihre Relevanz zu bewerten. Dazu werden einerseits die Eintrittswahrscheinlichkeiten, unter Verwendung eines qualitativen Ansatzes, geschätzt und durch Wahrscheinlichkeitsstufen

(unwahrscheinlich, möglich, wahrscheinlich und sehr wahrscheinlich) kategorisiert. Andererseits wird der zu erwartende Schaden geschätzt, die Risiken kategorisiert (niedrig, mittel, hoch und sehr hoch) wie auch eine Risikomatrix zur Übersichtsdarstellung verwendet. [Bund08a]

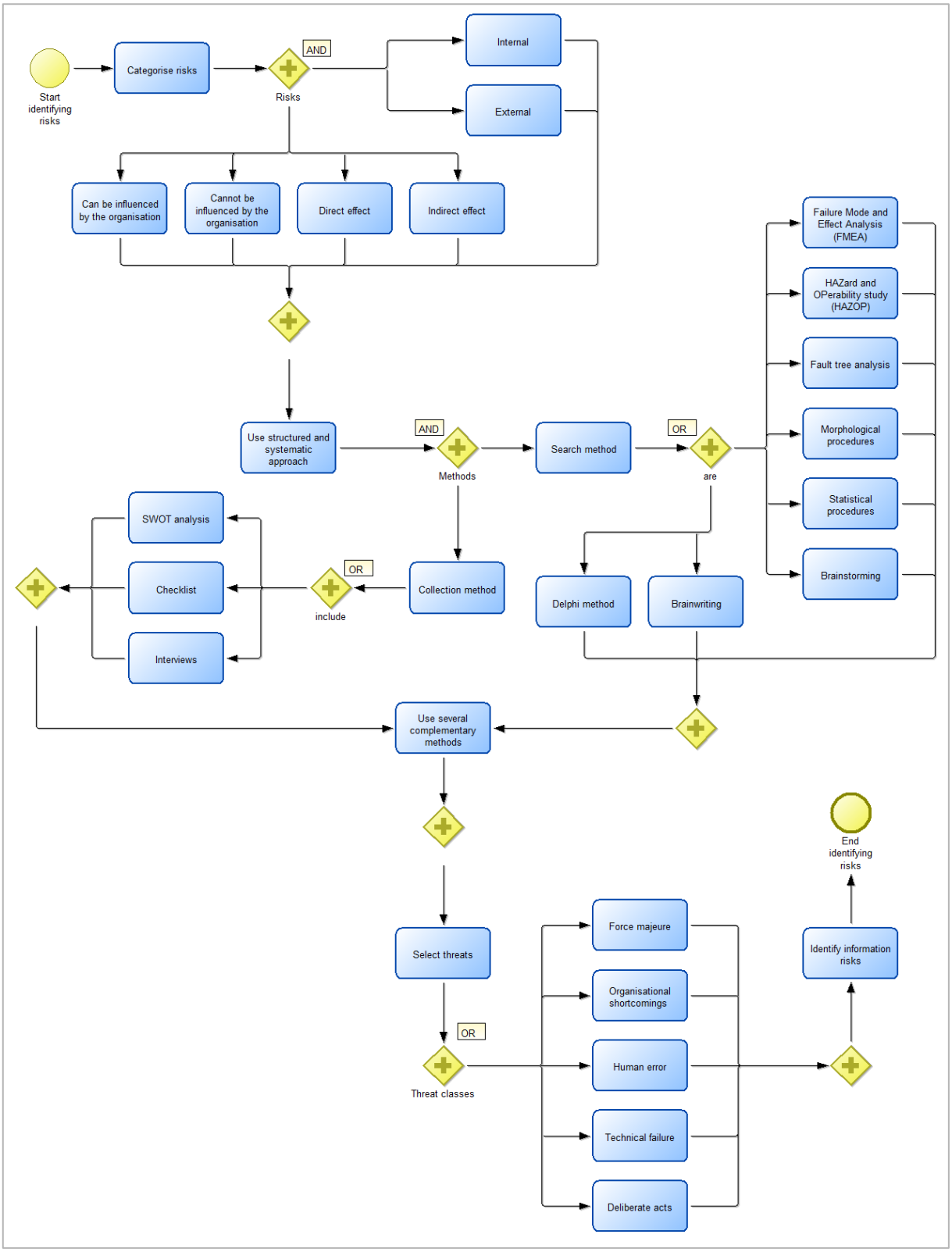

Abbildung 38: Risikoidentifizierung

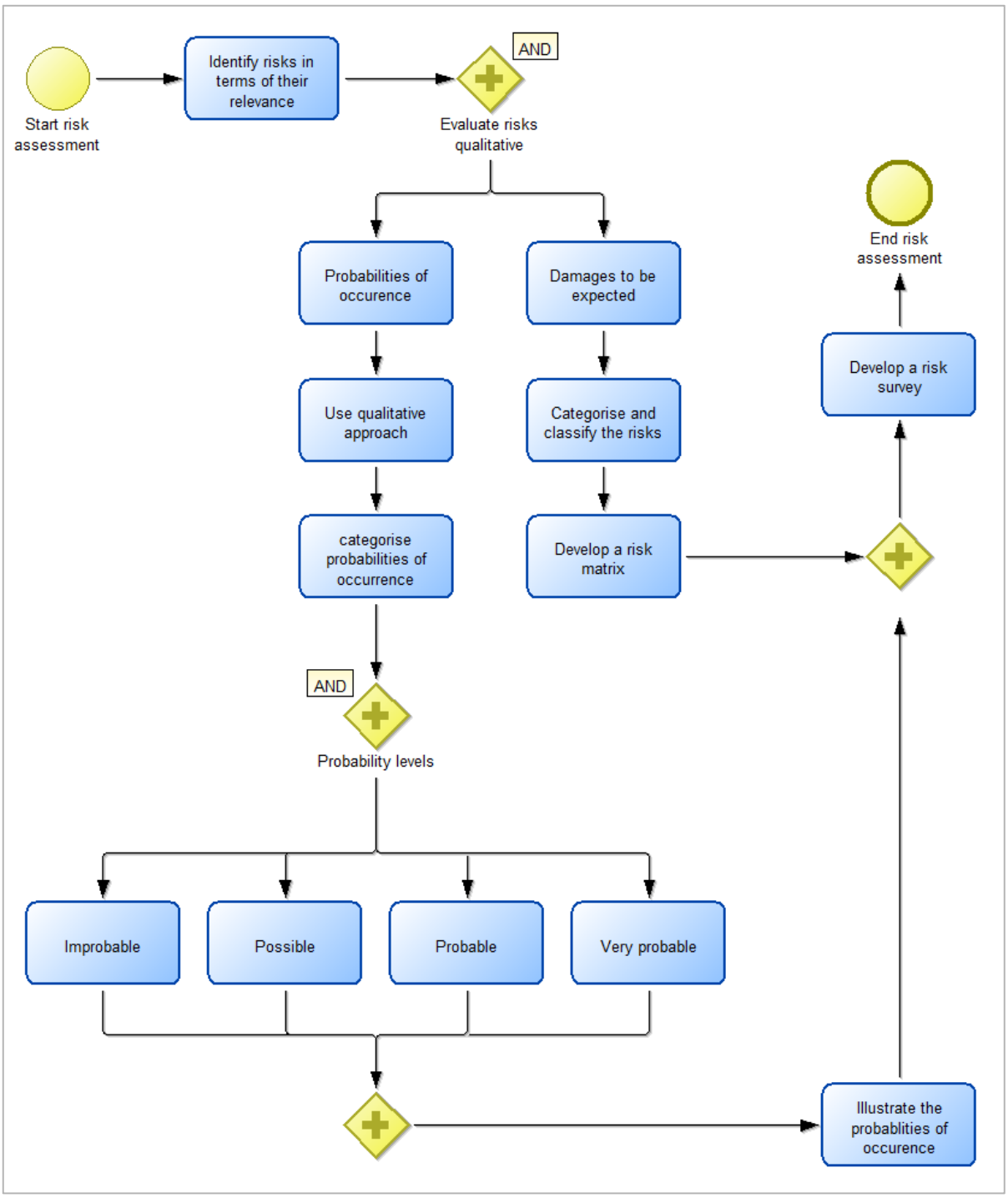

Abbildung 39: Risikobewertung

Die Risiken können in unterschiedlichen Formen erfasst. Eine mögliche tabellarische Erfassung der Risiken ist in Tabelle 8 zu sehen.

Tabelle 8: Beispiel Risikoerfassung [Bund08a]

Ursache	Risiko	Szenario	Auswirkung	Wahrscheinlichkeit	Risikobewertung	Schwach-stellen	Strategie	Maßnahmen	Verantwortliche
Kabelbrand Kurzschluss Erwärmung ...	Brand	Ausfall Rechen-zentrum	Sehr hoch	Möglich	Mittel	Raum-aufteilung	...	...	...
Ausfall externer Stromzufuhr ...	Strom-ausfall	Ausfall Rechen-zentrum	Hoch	Möglich	Mittel	Nur 50% der Server an Notstrom-versorgung		Zusätzliche Strom-generatoren	

5.1.3.3 Gruppierung und Szenarienbildung

Um Vorsorgemaßnahmen zu identifizieren, werden Risiken auf der Prozessebene untersucht sowie allgemeine und praxisnahe Notfallszenarien erarbeitet und entwickelt, denen die Risiken zugeordnet werden können (siehe Abbildung 40).

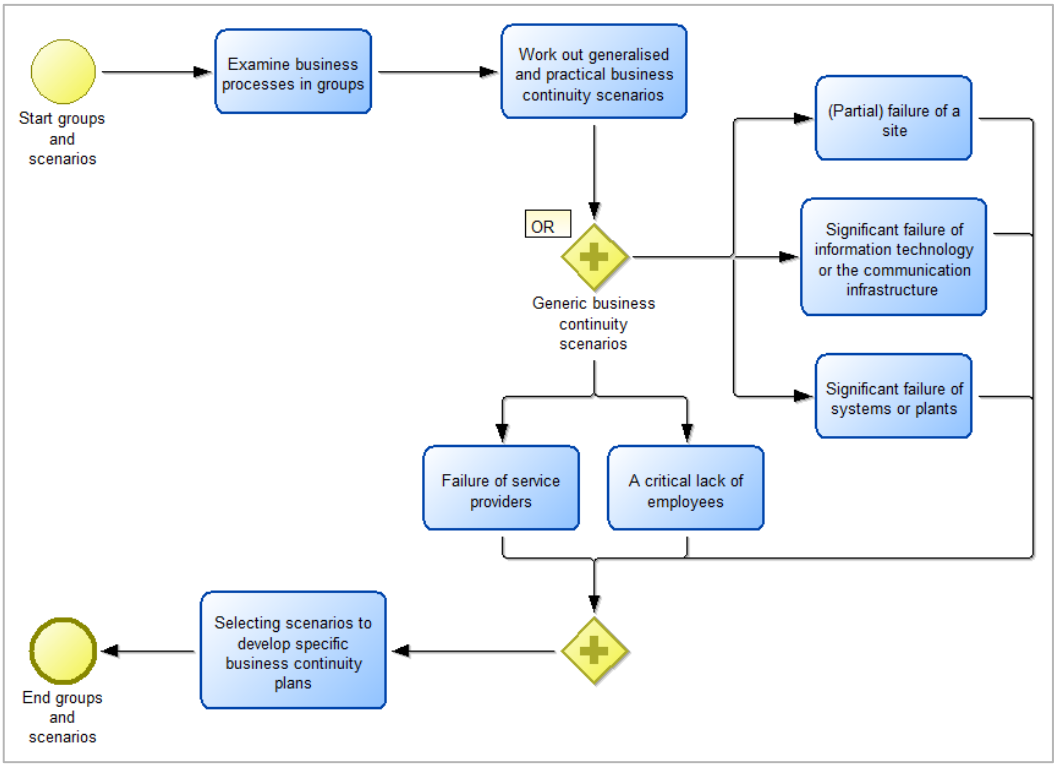

Abbildung 40: Gruppierung und Szenarienbildung

Generische Notfallszenarien können sein:

- (Teil-)Ausfall eines Standortes (z. B. durch Hochwasser, Großbrand, Gebietssperrung, Ausfall der Zutrittskontrolle)
- Erheblicher Ausfall von Informationstechnik oder der Kommunikationsinfrastruktur
- Erheblicher Ausfall von Systemen oder Anlagen (z. B. in der Produktion)
- Ausfall einer kritischen Anzahl von Mitarbeitern (z. B. bei Pandemie, Lebensmittelvergiftung, Streik) sowie
- Ausfall von Dienstleistern (z.B. Zulieferer, Stromversorger). [Bund08a]

5.1.3.4 Risikostrategieoptionen identifizieren

Diese Phase, zu sehen in Abbildung 41, befasst sich mit der Bestimmung und Dokumentation der geeigneten Risikostrategieoptionen für jeden kritischen Geschäftsprozess und jedes Risiko. Zu den möglichen Risikostrategien zählen die Risikoübernahme, der Risikotransfer, die Risikovermeidung und die Risikoreduktion. Bei der Risikoübernahme wird das identifizierte Risiko akzeptiert, bei dem Risikotransfer wird das Risiko auf eine andere Institution übertragen, bei der Risikovermeidung werden Prozessabläufe oder Umgebungsbedingungen so verändert, dass die entsprechende Gefährdung nicht mehr relevant ist und die am häufigsten gewählte Strategieoption ist die Risikoreduktion, bei der die Eintrittswahrscheinlichkeit oder die Schadenshöhe vermindert wird. [Bund08a]

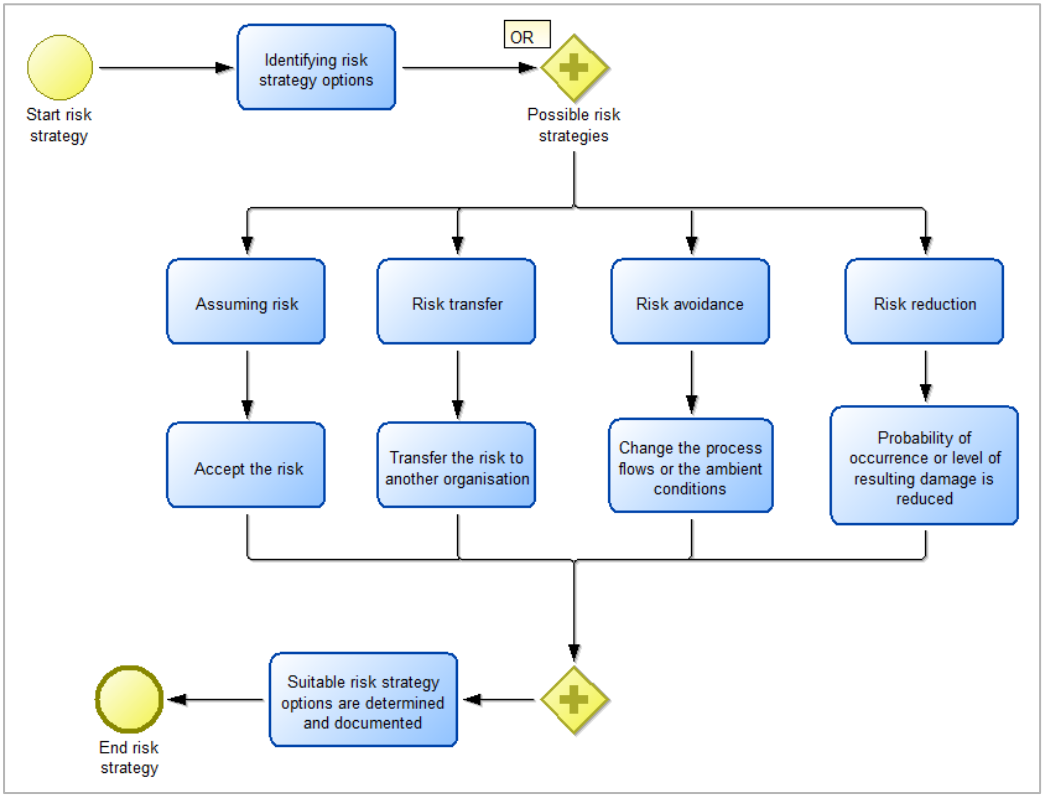

Abbildung 41: Risikostrategie

5.1.3.5 Risikoanalysebericht

Der Risikoanalysebericht (siehe Abbildung 42) dokumentiert die Ergebnisse und beinhaltet eine Management-Übersicht, die verwendeten Methoden der Risikoanalyse, eine Liste der Risiken mit eventuell vorgenommenen Gruppierungen, die Ergebnisse der Risikobewertung, die Risikostrategieoptionen für kritische Prozesse und die Auswahl der Risikostrategien. [Bund08a]

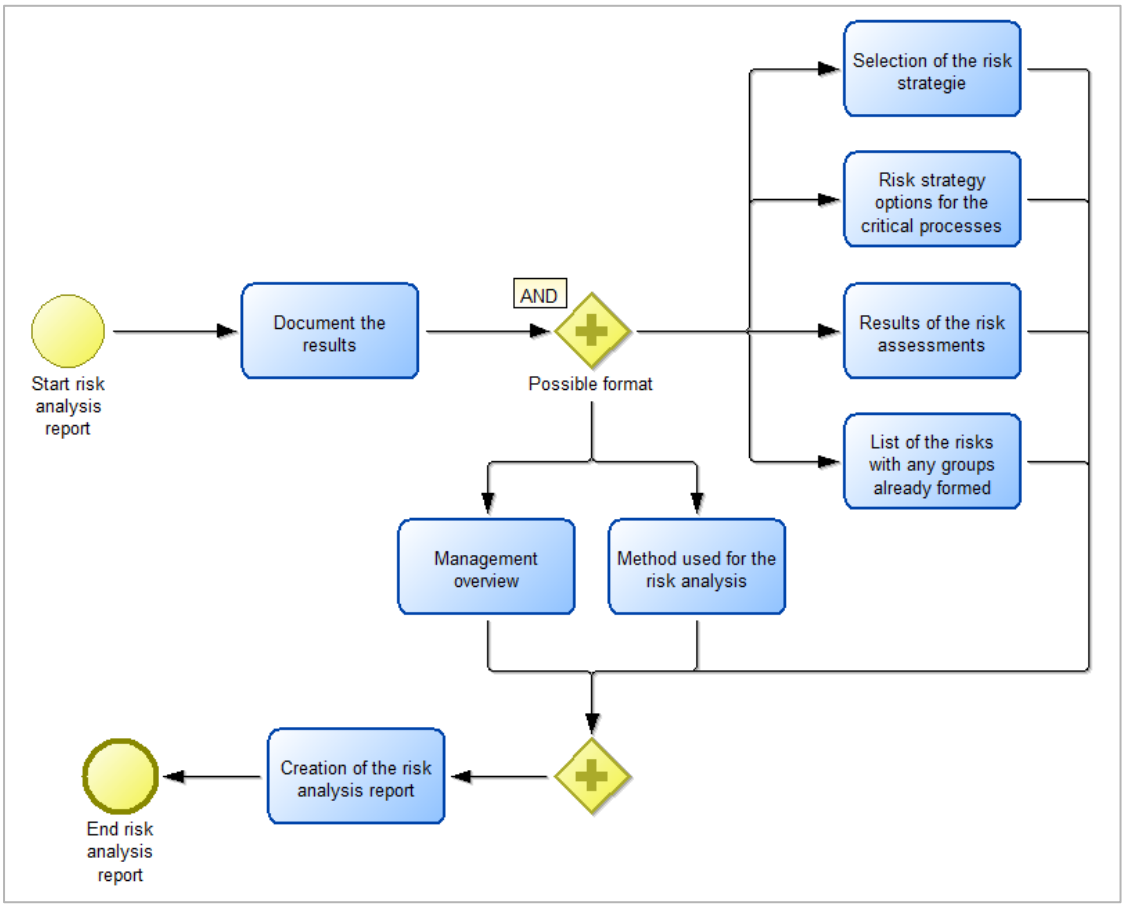

Abbildung 42: Risikoanalysebericht

5.1.4 Schadensminderungsstrategieentwicklung

Um die Risikominderungsstrategien aufzuarbeiten werden zunächst Sicherungs- und Wiederherstellungsmöglichkeiten (siehe Abbildung 43) behandelt. Diese dienen als Grundlage für die Entwicklung von Maßnahmen zur Krisenvermeidung und beinhalten den Prozess der Einführung eines Wiederanlaufplans. Die Verfügbarkeitsanforderungen der einzelnen IT-Anwendungen, die Wiederbeschaffungsmöglichkeiten, die internen und externen Ausweichmöglichkeiten für IT-Anwendungen, die Datenfernübertragung für den Notbetrieb, die im eingeschränkten IT-Betrieb laufenden IT-Anwendungen wie auch der Systemstart der IT-Komponenten und die Einbindung in das IT-System sind wesentliche

Punkte die im Wiederanlaufplan berücksichtigt werden müssen. Ein möglicher Wiederanlaufprozess könnte wie folgt aussehen:

- Aufbau und Installation der notwendigen Hardwarekomponenten
- Einspielen der Systemsoftware
- Einspielen der Anwendungssoftware
- Bereitstellen der notwendigen Daten einschließlich Konfigurationsdateien
- Wiederanlauf [Bund13]

Maßgeblich für die Geschäftstätigkeiten sind die Kundenbetreuung, die Verwaltung und der Betrieb, Geschäftsinformationen und Geschäftsdokumente, eine grundlegende Ausstattung sowie Räumlichkeiten. Als Teil der Risikominderungsstrategie sollte eine Analyse der aktuellen Informationstechnologien am Markt durchgeführt werden.

Eine Entscheidung über den Nutzen von alternativen Standorten ist zu treffen. Die teuerste und umfangreichste Strategie, jedoch gekennzeichnet durch die höchste Verfügbarkeit und Redundanz, ist die Wahl von „Fully Mirrored Sites“. Es werden alle Prozesse gespiegelt und zeitgleich synchronisiert. „Hot Sites“ sind Standorte, die von einem gewerblichen Verkäufer geleast werden und nur im Falle eines Notfalls verwendet werden. „Warm Sites“ sind Kombinationen aus „Hot Sites“ und „Cold Sites“. Diese sind teilweise ausgestattete Räumlichkeiten mit den notwendigsten Geräten für kritische Operationen. „Mobile Sites“ sind in sich abgeschlossene Einheiten, welche zu spezifischen Standorten transportiert werden, um neue, alternative Rechenzentren zu errichten. Die billigste Strategie, jedoch verbunden mit einer sehr langen Zeitspanne der Wiederinbetriebnahme der Prozesse, ist die Wahl von „Cold Sites“. Erst nach einer Unterbrechung werden alle Prozesse wieder neu in Betrieb genommen. Bei der „Reciprocal Site“ werden Vereinbarungen mit anderen Unternehmen, zur gegenseitigen Unterstützung während einer Unterbrechung, getroffen. [SnRi14]

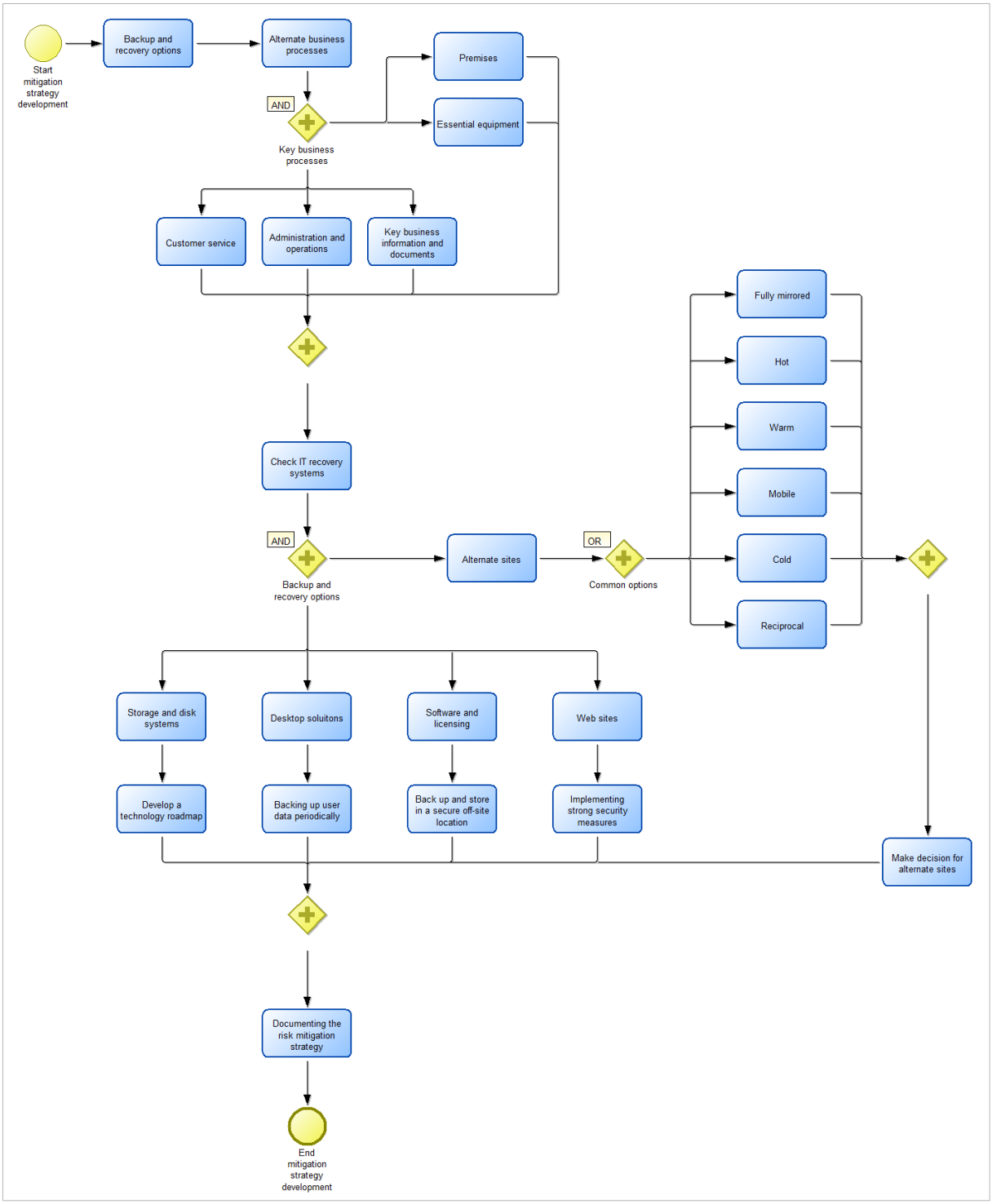

Abbildung 43: Schadensminderungsstrategie Entwicklung

Der nächste große Schritt ist die Überprüfung und Analyse des IT Recovery Systems und die Erstellung eines Technologieplans. Jede Institution sollte regelmäßig Sicherungskopien von allen kritischen Benutzerdaten erstellen und diese außerhalb des Standortes speichern. Software, Bewilligungsdaten wie auch Lizensierungen von Betriebssystemen, Benutzern und Applikationen sollten gesichert werden und ebenfalls außerhalb des Standortes gespeichert werden. Strategien für die Verwendung von

Webseiten sind die Umsetzung von Sicherheitsmaßnahmen, Auditierung und Überwachung des Webservers wie auch eine Dokumentation der Sicherheits- und Konfigurationseinstellungen. Als Abschluss dieses Prozesses werden alle gewählten Strategien und Informationen zusammengefasst und dokumentiert. [SnRi14]

5.1.5 Business Continuity und Disaster Recovery Plan

Der Business Continuity und Disaster Recovery Plan, zu sehen in Abbildung 44, startet mit dem Prozess der Entwicklung von Risikominderungsstrategien und folgt mit den fünf Phasen des Business Continuity und Disaster Recoverys, der Entwicklung eines BC/DR Teams, eines Kommunikationsplans wie auch den Ereignisprotokollen, Änderungsmanagement und Anhängen.

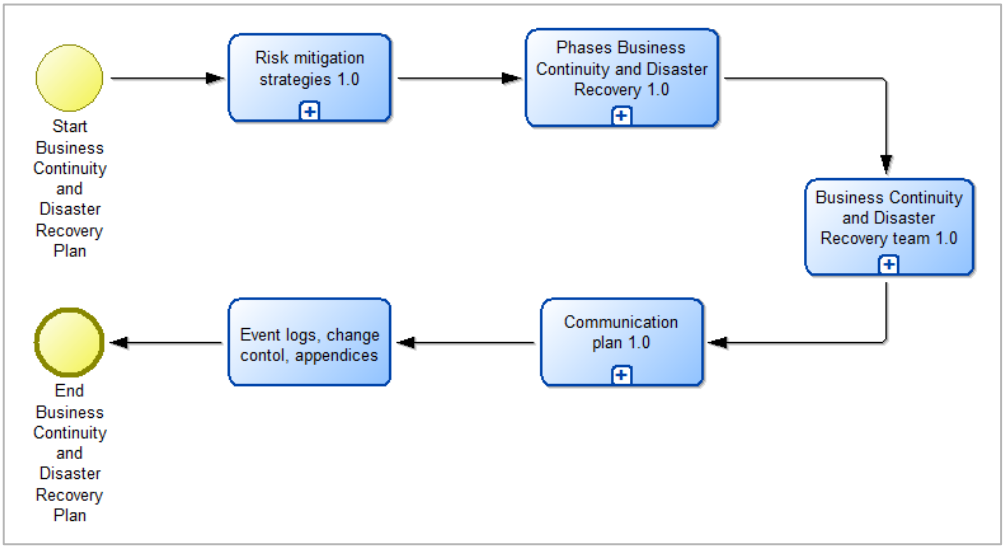

Abbildung 44: Business Continuity und Disaster Recovery Plan

5.1.5.1 Risikominderungsstrategien

Risikominderungstechniken, wie der Entwurf eines Prozesses zum Testen und Anwenden von Anti-Virus und Anti-Malware Software Updates und die Überprüfen der Firewalls, Log-Dateien und das Aufrüsten von Server-Patch Prozessen, sind grundlegend für eine erfolgreiche Informationssicherheitsstrategie. Weitere häufige Risikominderungstechniken, wie in Abbildung 45 zu sehen ist, sind die Einführen von einzelnen, verschlüsselten administrativen Datenbankkennwörter für verschiedene Rollen, wie physische Sicherheitskontrollen für die gesamte Computerausrüstung, die Einführung von Strategien für den Ablauf von Passwörtern, zentralisierte Passwort- und Authentifikationsstrategien, die Installation eines alleinstehenden, nicht mit dem Internet verbundenen Computers zum Scannen von externen Speichermedien, die Sicherung von Systemen, die Verwendung einer Cloud oder die Verlagerung der IT-Hardware außerhalb

des Standortes und offizielle dokumentierte Informationssicherheits- und Notfallwiederherstellungstrainings für alle Mitarbeiter. [SnRi14]

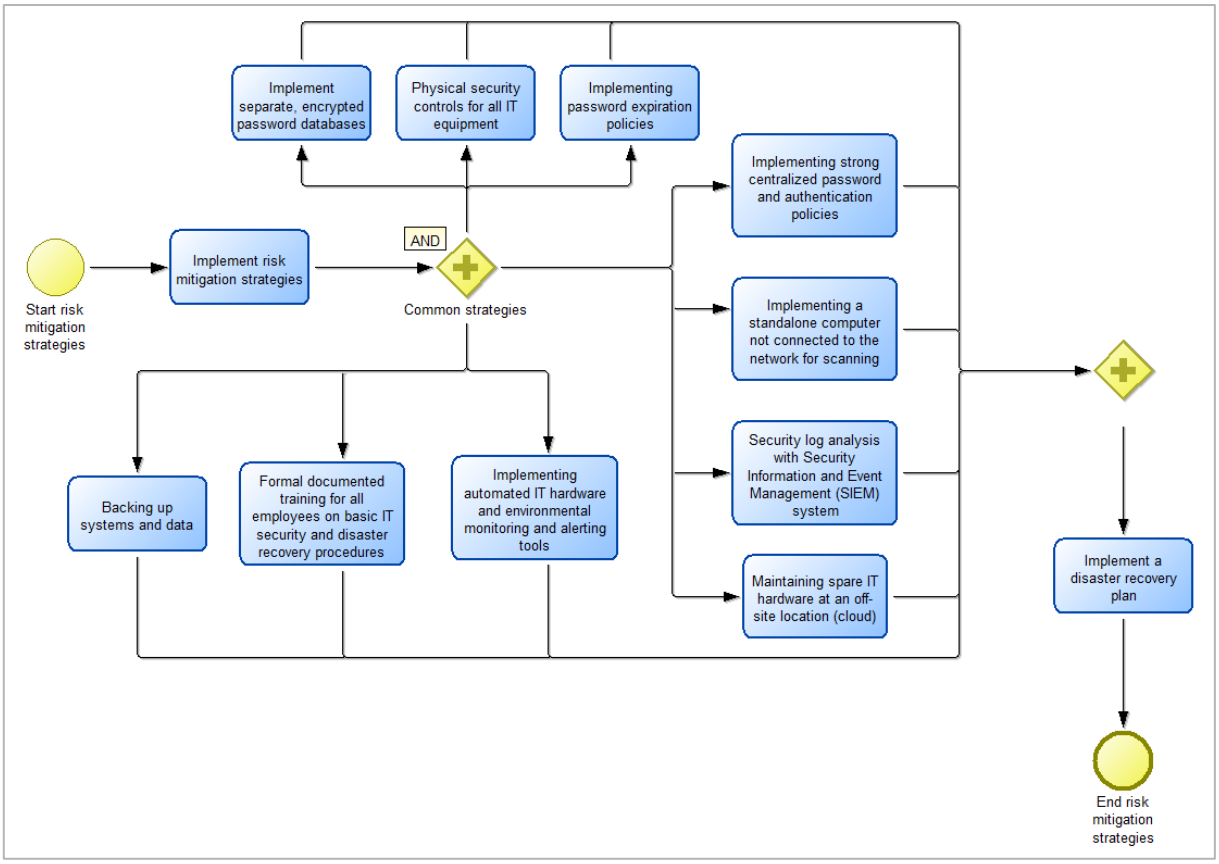

Abbildung 45: Risikominderungsstrategien

5.1.5.2 Business Continuity und Disaster Recovery Phasen

Abbildung 46 zeigt die Phasen des Business Continuity und des Disaster Recovery beginnend mit der Aktivierung und weiterführend dann die Notfallwiederherstellung, die Wiederaufnahme des Geschäfts wie auch der Übergang zu den normalen Operationen.

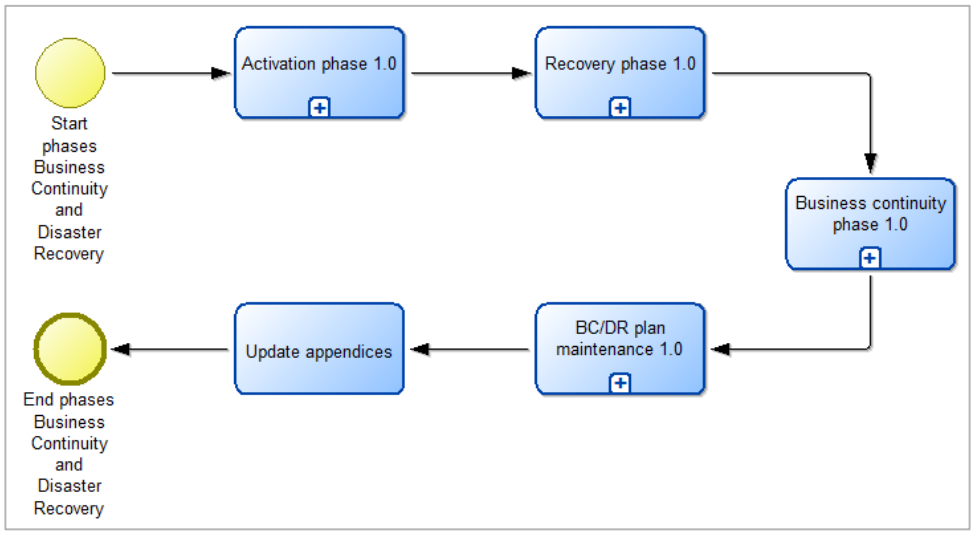

Abbildung 46: Business Continuity und Disaster Recovery Phasen

5.1.5.2.1 Aktivierungsphase

Die Aktivierungsphase, zu sehen in Abbildung 47, behandelt den Prozess während und unmittelbar nach einer Geschäftsunterbrechung wie auch die Definition der Aktivierung des Business Continuity und Disaster Recovery Plans. Die Aktivierung enthält die ersten Reaktionen und Ankündigungen, die Beurteilung und Eskalation, die Deklaration der Katastrophe wie auch die Umsetzung des Plans.

Katstrophen werden in drei Kategorien eingeteilt. Kleine Unterbrechungen kennzeichnen sich dadurch, dass sich die Auswirkungen auf eine Komponente beziehen. Operationen wie auch Unternehmensfunktionen können sehr oft während eines bestimmten Zeitraumes weitergeführt werden und der Ausfall eines Systems kann während des normalen Geschäftsbetriebs behoben werden. Mittlere Unterbrechungen haben auf eine oder mehrere, jedoch nicht auf alle Unternehmensfunktionen Auswirkungen. Mehrere Systeme, aber nicht alle, können Versagen oder nicht verfügbar sein. Durch Hochwasser oder Feuer können bauliche Schäden an Gebäuden verursacht werden, wobei hier mit einer beschränkten Auswirkung und einer längeren Wiederherstellungsdauer zu rechnen ist. Die dritte Kategorie, große Unterbrechungen, definiert sich durch die Unterbrechung der gesamten Geschäftstätigkeiten, dem Ausfall und die Unzugänglichkeit aller Systeme und Geräte wie auch die Zerstörung des gesamten Gebäudes und der Einrichtungen. [SnRi14]

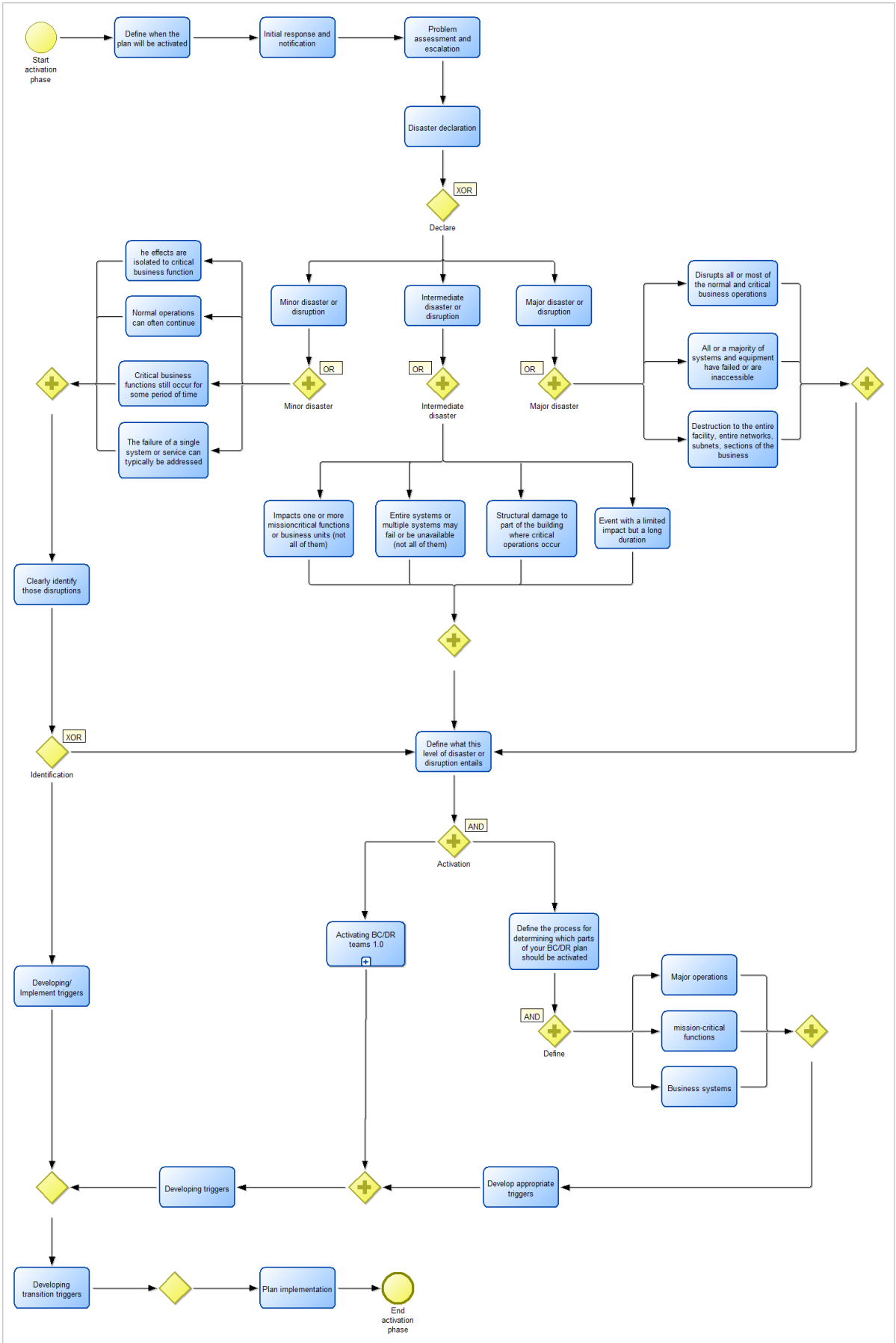

Abbildung 47: Aktivierungsphase

5.1.5.2.1.1 Aktivierung der Business Continuity und Disaster Recovery Teams

Nach der Klassifikation der Katastrophe wird ein BC/DR Team (zu sehen in Abbildung 48) aktiviert, welches für die Abwicklung der Betriebsstörung und die Umsetzung der weiteren Vorgehensweise unterschiedlicher Bereiche im BC/DR Plan zuständig ist. Die Mitglieder dieses Teams befassen sich mit den Bereichen Krisenmanagement, Schadensfeststellung, Benachrichtigung, Notfall, Risikobewertung, Betriebsmittel und Versorgung wie auch der Krisenkommunikation. Eine Business Continuity Führung und ein Koordinator halten das ganze Team zusammen. [SnRi14]

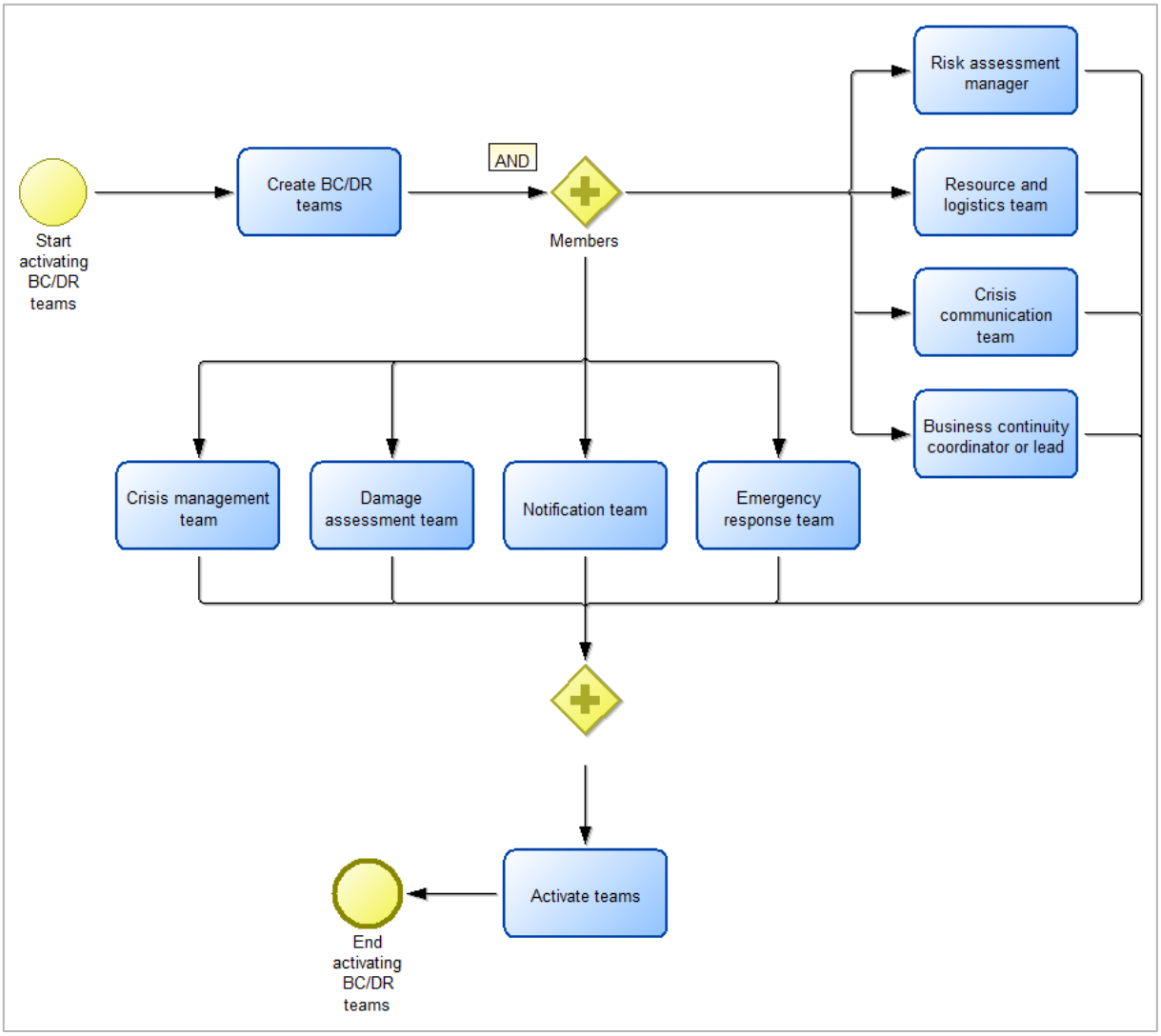

Abbildung 48: Aktivierung der Teams

5.1.5.2.2 Wiederherstellungsphase

Die Erarbeitung einer Aktivierungs-, Notfalls- und Wiederherstellungskontrollliste, die Entwicklung von IT-Wiederherstellungsaufgaben wie auch Computersicherheitsstrategien gehören zu den Prozessen der Wiederherstellungsphase (vergleiche Abbildung 49). [SnRi14]

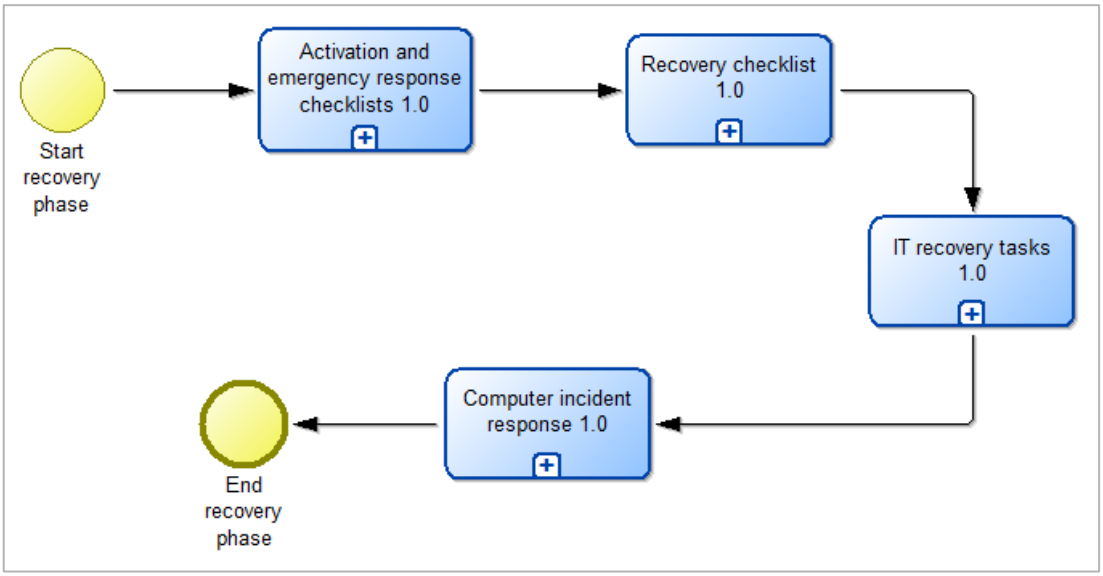

Abbildung 49: Wiederherstellungsphase

5.1.5.2.2.1 Aktivierungs- und Notfallmaßnahmencheckliste

In Abbildung 50 ist der Prozess der Erstellung einer Aktivierungs- und Notfallmaßnahmencheckliste dargestellt. Teil der Aktivierungscheckliste sind die Benachrichtigung des BC/DR Teams wie auch die Bestimmung zur Aktivierung des BC/DR Plans. Die Notfallmaßnahmencheckliste beinhaltet die unmittelbaren Nachwirkungen einer Katastrophe auf die menschliche Sicherheit. [SnRi14]

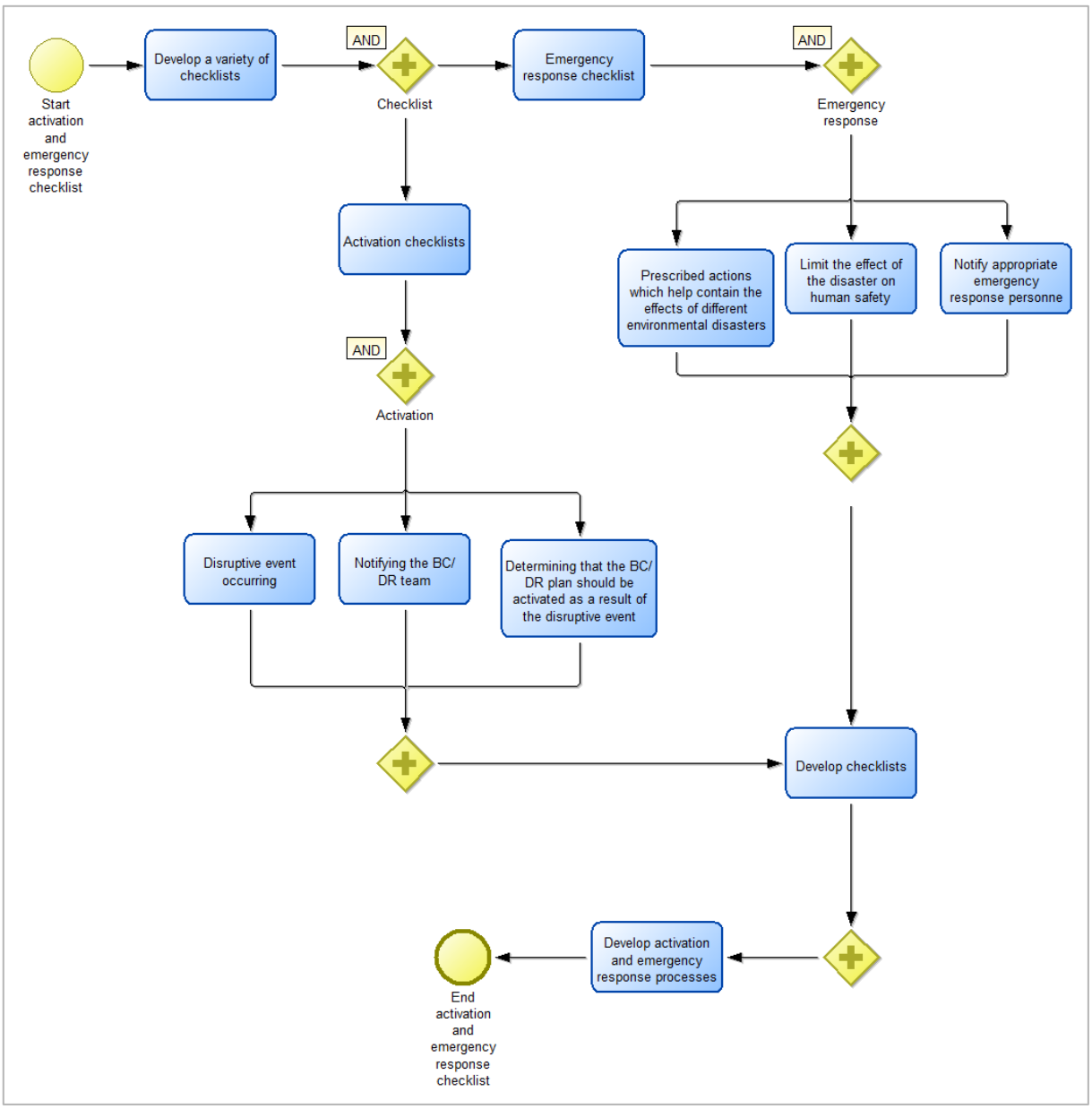

Abbildung 50: Aktivierungs- und Notfallmaßnahmencheckliste

5.1.5.2.2.2 Wiederherstellungscheckliste

Der BC/DR Plan beinhaltet eine Wiederherstellungscheckliste (siehe Abbildung 51) mit Informationen über die Mitarbeiter und Lieferanten (Kontaktliste), den System- und Netzwerkaufbau, das Vorhandensein einer Geräteliste, die Standorte der Sicherungskopien, alternativen Zugangsinformationen, das Vorgehen zur Erneuerung von Gebäuden und Einrichtungen, die Vorgehensweisen der physischen Sicherheit, die Zahlungen, Passwörter und Zugangscodes. [SnRi14]

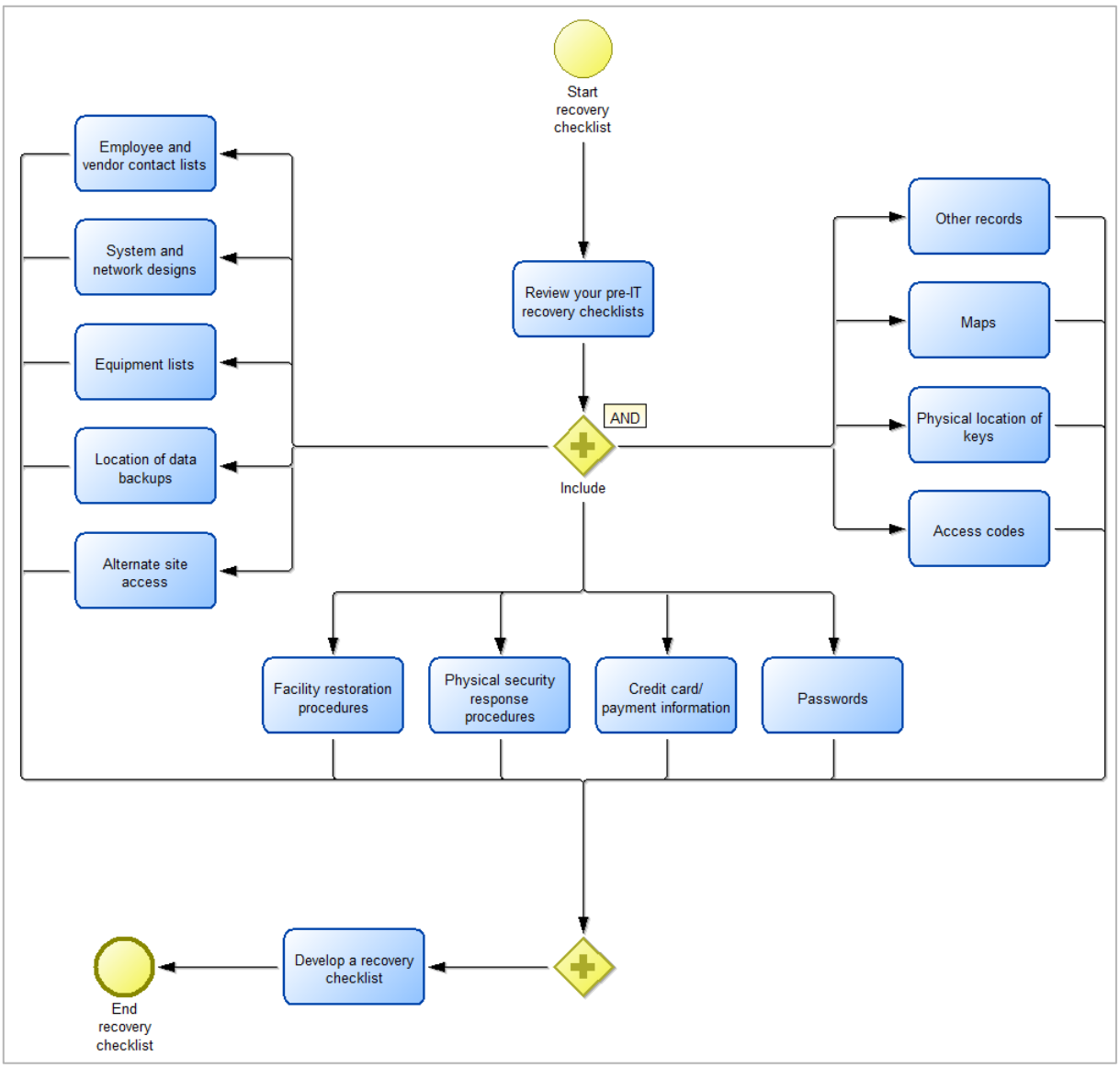

Abbildung 51: Wiederherstellungscheckliste

5.1.5.2.2.3 IT-Wiederherstellungsschritte

Die Wiederherstellungsphase beinhaltet auch den Prozess der Erstellung einer IT-Wiederherstellungscheckliste (siehe Abbildung 52). Die Wiederherstellung der IT-System- und Netzwerkinfrastruktur steht zu Beginn der Wiederherstellungscheckliste, gefolgt von den Bereichen Büro, technische Ausstattung der Benutzer, Geschäftsprozesse, Herstellungsprozesse und Produktion. Informationen über jegliche Anwendungen wie Netzwerkstandorte, Kontaktlisten der Anwendungsanbieter, Anzahl der Kunden Workstations, Server, Datenbanken, virtuelle Personal Computer, Netzwerkservices, Dateninputs, mobile Endgeräte sind ebenfalls in der Checkliste enthalten. [SnRi14]

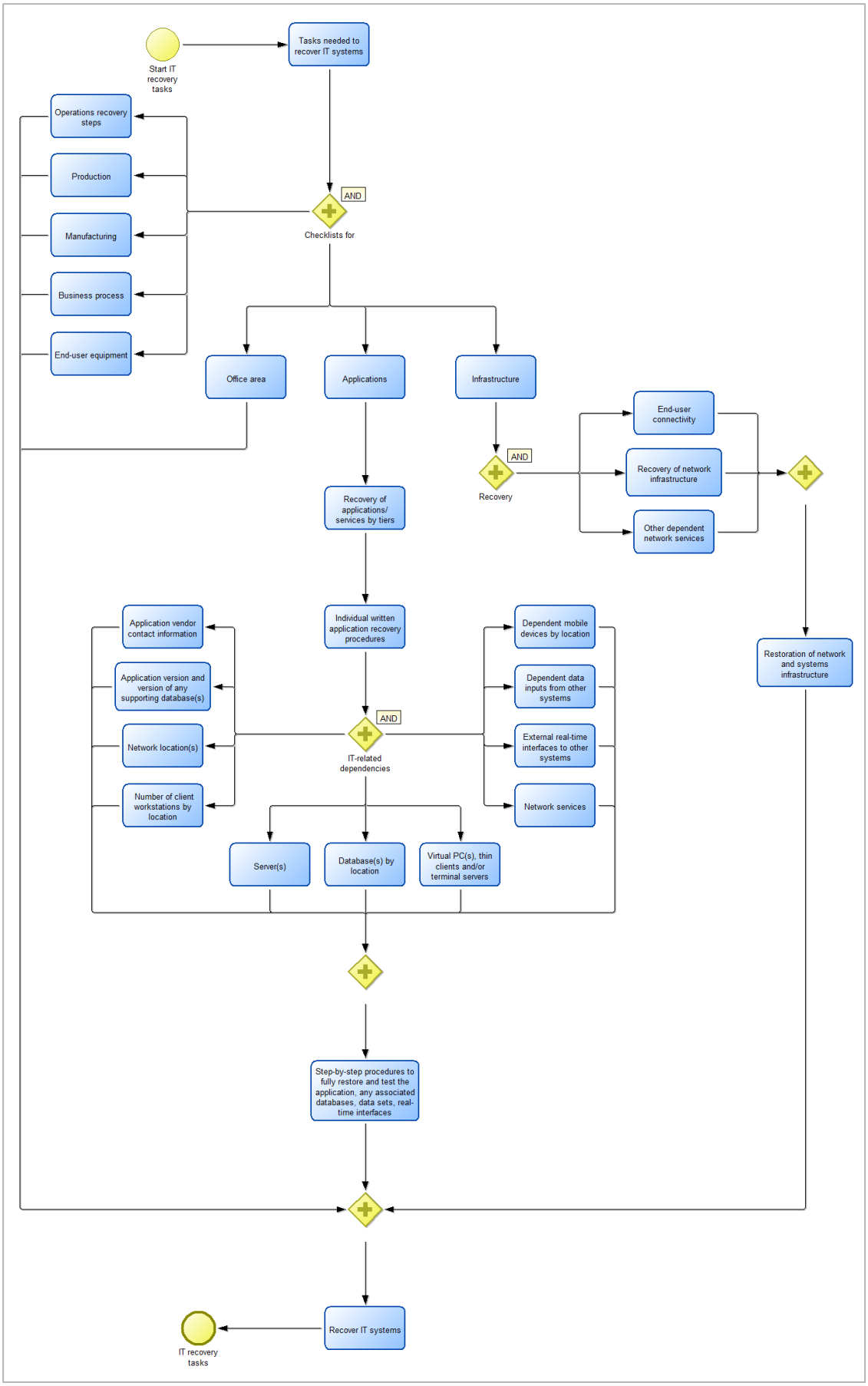

Abbildung 52: IT-Wiederherstellungsschritte

5.1.5.2.2.4 Computer incident response

Die IT Wiederherstellung befasst sich auch mit der Behebung von Problemen, verursacht durch Systemausfälle, Sicherheitslücken oder vorsätzliche Datenkorruption und Datenzerstörung. Es ist ratsam, ein CIR-Team zu aktivieren mit den Zuständigkeitsbereichen Kontrolle, Alarmbereitschaft und Mobilisierung, Beurteilung und Stabilisierung wie auch Entschluss und Überprüfung zu aktivieren, um Computerzwischenfälle schnellstmöglich zu bewältigen (siehe Abbildung 53). [SnRi14]

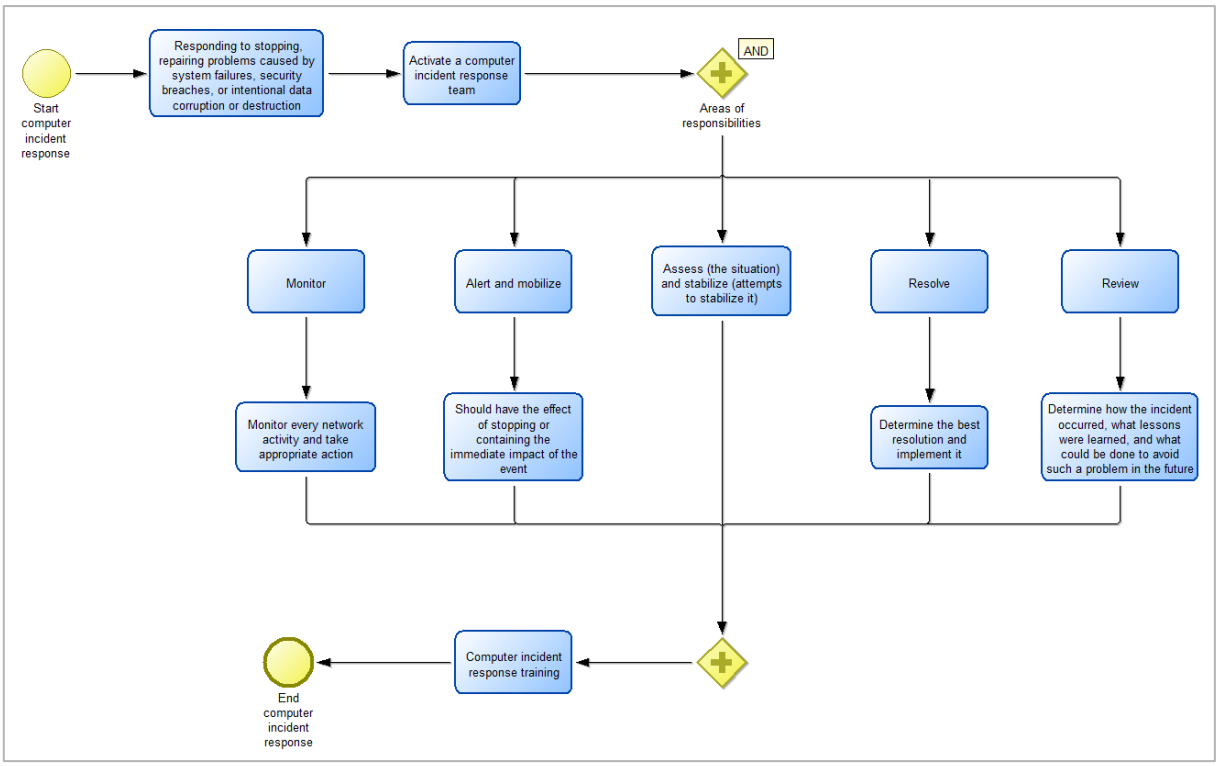

Abbildung 53: Computer incident response

5.1.5.2.3 Business continuity Phase

Die Business Continuity Phase, zu sehen in Abbildung 54, startet mit der Festlegung, welche Prozesse wiederhergestellt, gerettet und ersetzt werden sollen. Diese Schritte beinhalten das Managen der Geschäftsprozesse wie auch das Beurteilen und Normalisieren des Betriebs. Die Business Continuity Checkliste beinhaltet Informationen über die Führungskräfte, die Verwaltung, den Geschäftsbetrieb, die IT Infrastruktur und IT Benutzer, den Kommunikationsbereich wie auch die Ausstattungen und Sicherheit. [SnRi14]

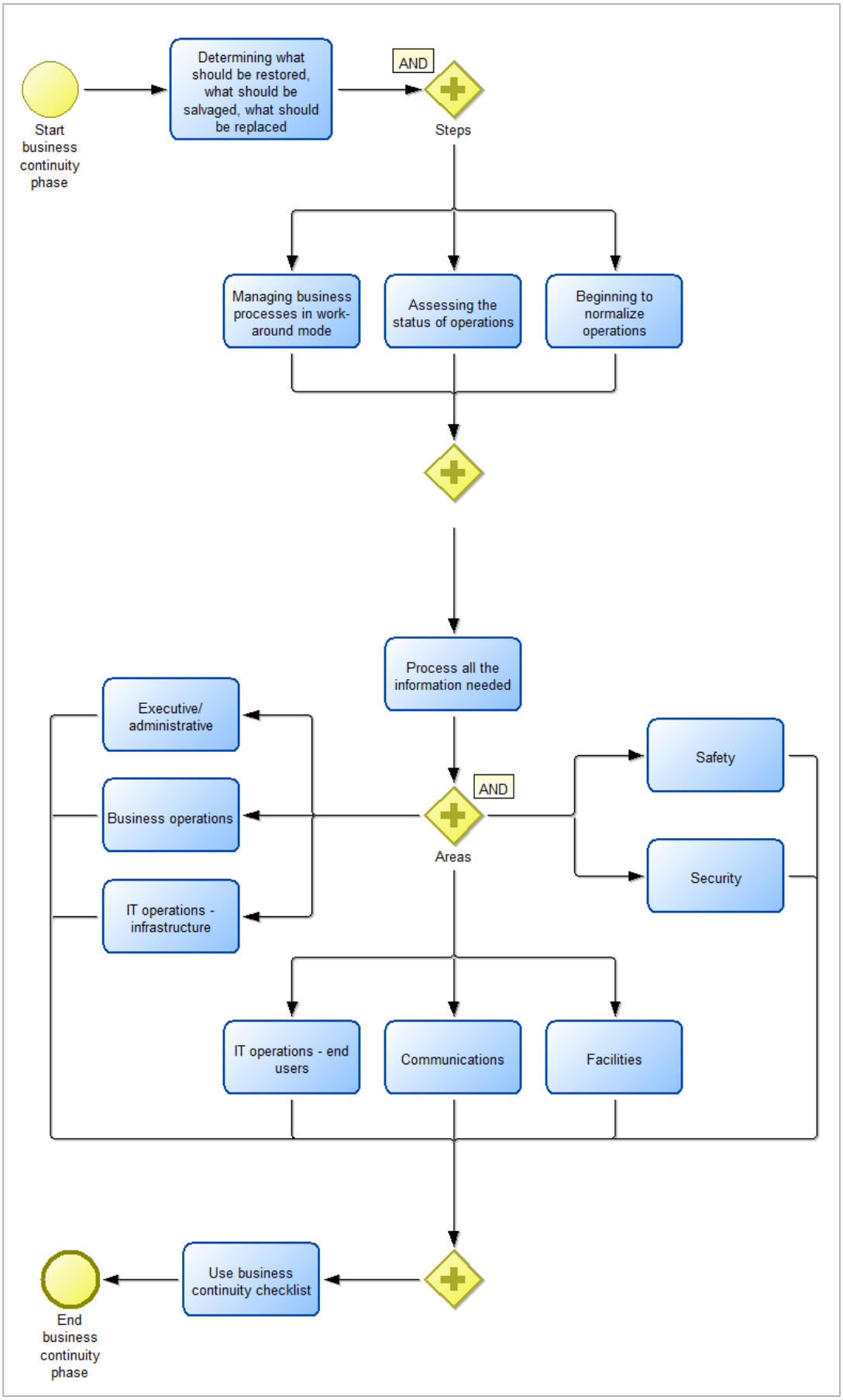

Abbildung 54: Business continuity Phase

5.1.5.2.4 Aufrechterhaltung des Business Continuity und Disaster Recovery Plans

Auf den Prozess der Aufrechterhaltung des BC/DR Plans wird näher in Kapitel 5.1.7 eingegangen.

5.1.5.3 Business Continuity und Disaster Recovery Team

Die Mitglieder des BC/DR Teams (siehe Abbildung 55) sind aus den Bereichen Krisenmanagement, aus dem Management, der Schadenabschätzung, des Betriebs, der Informationstechnologie, der Verwaltung, dem Transportwesen und Standortwechseln, der Medien, dem Personalwesen, dem Personal für rechtliche Angelegenheiten, dem Sicherheitspersonal und der Beschaffung. Richtlinien wie auch Kontaktinformationen sind für eine erfolgreiche Zusammenarbeit notwendig. [SnRi14]

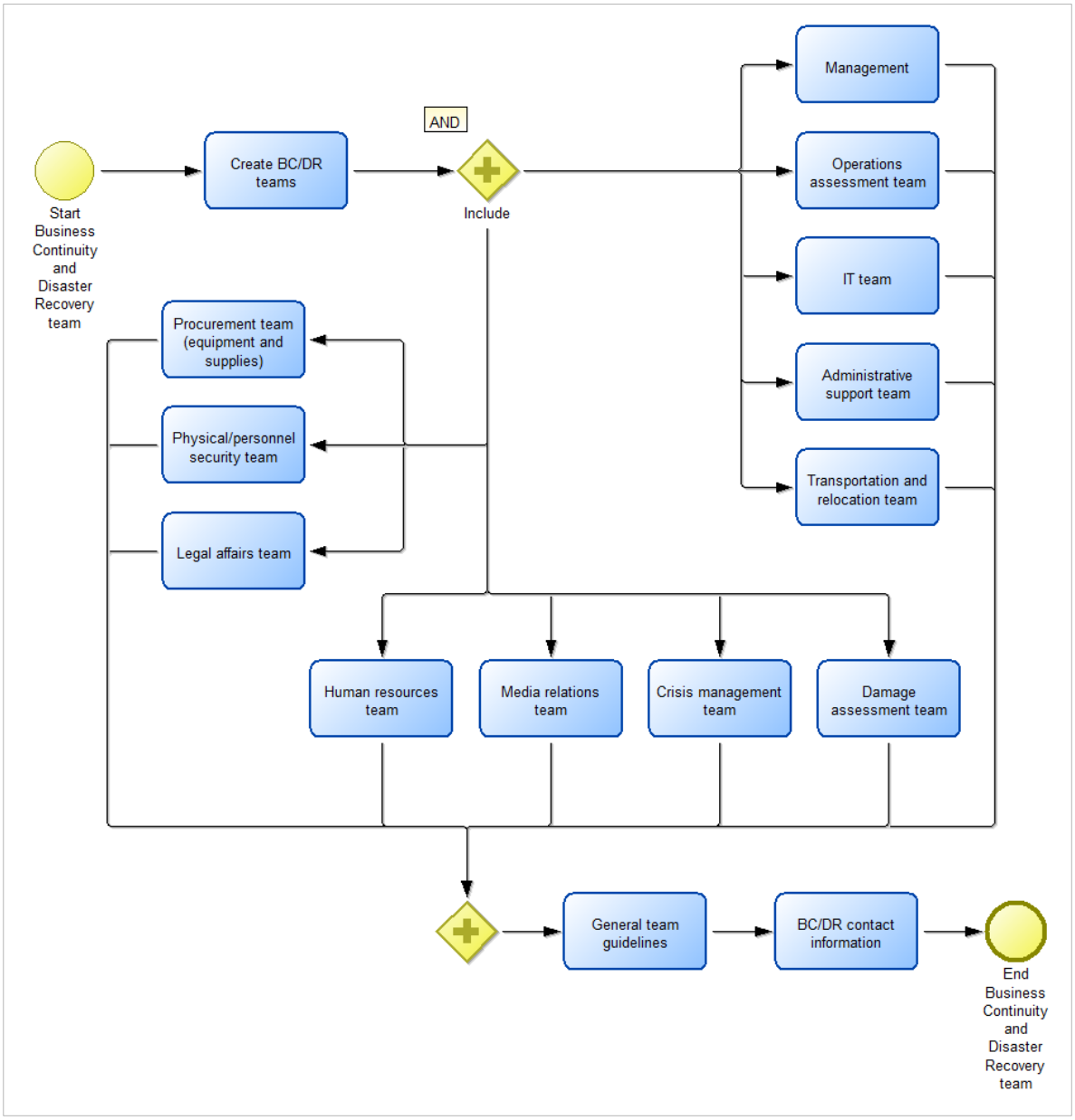

Abbildung 55: BC/DR Team

5.1.5.4 Kommunikationsplan

Der Kommunikationsplan, zu sehen in Abbildung 56, beinhaltet konkrete Informationen über den Namen, die Mitglieder, die Führung und die Befehlskette des Kommunikationsteams, die Verantwortlichkeiten und ihre Grenzen, die Leistungen, die Zeitplanung und die Koordination der Nachrichten, den Eskalationspfad sowie andere entsprechenden Informationen. Ein interner Kommunikationsplan, wie auch die Kommunikation mit den ArbeitnehmerInnen, mit Kunden und Verkäufern, mit Gesellschafter sowie mit der Community und der Öffentlichkeit sind ein wesentlicher Teil des BC/DR Plans. [SnRi14]

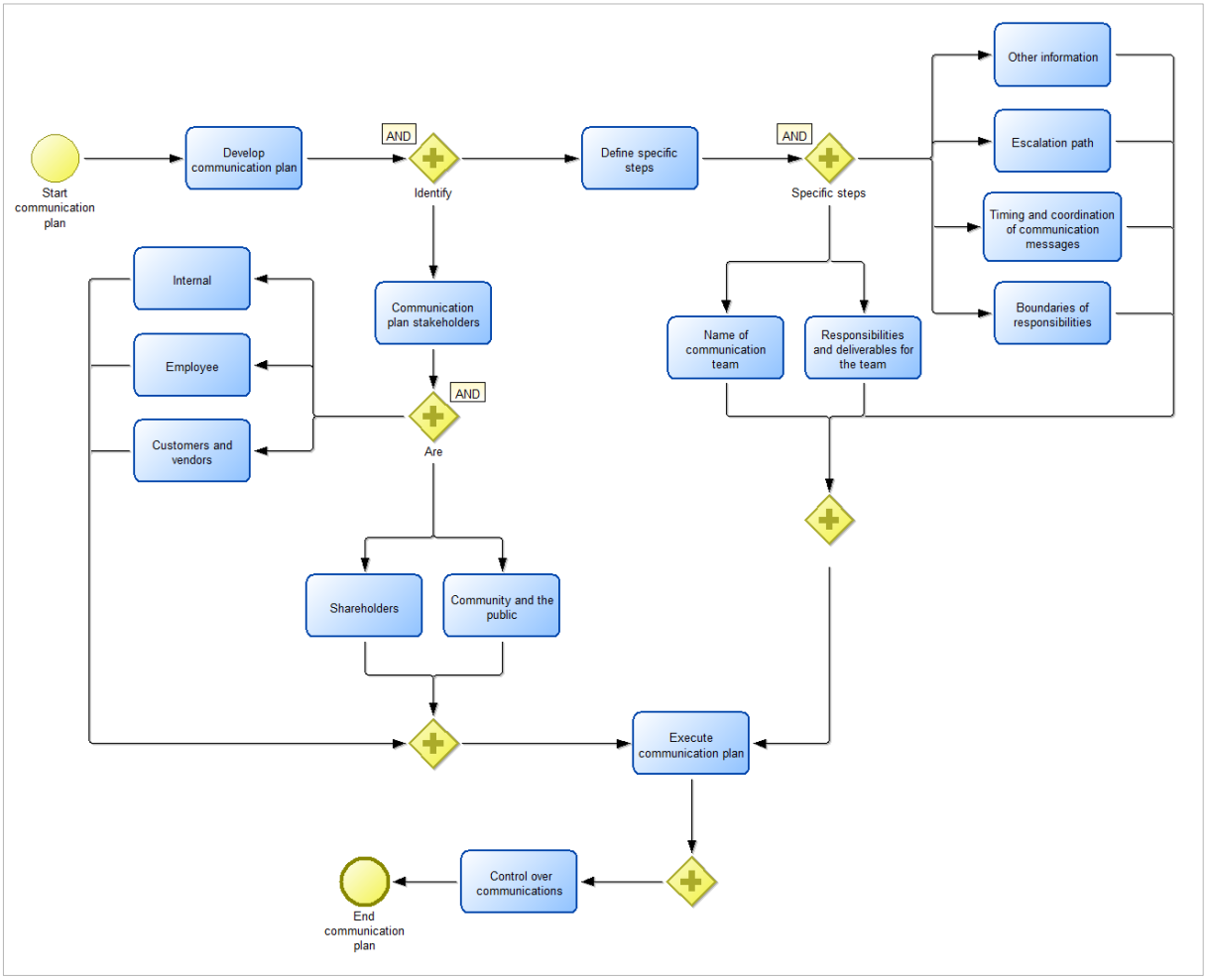

Abbildung 56: Kommunikationsplan

5.1.6 Training, Testen, Prüfen

Das Training von Personal und deren Rollen und Verantwortungen in Bezug auf den BC/DR Plan, das Testen des BC/DR Plans wie auch das Prüfen der IT Systeme sind die nächsten Schritte im Projektstrukturplan (vergleiche Abbildung 57). [SnRi14]

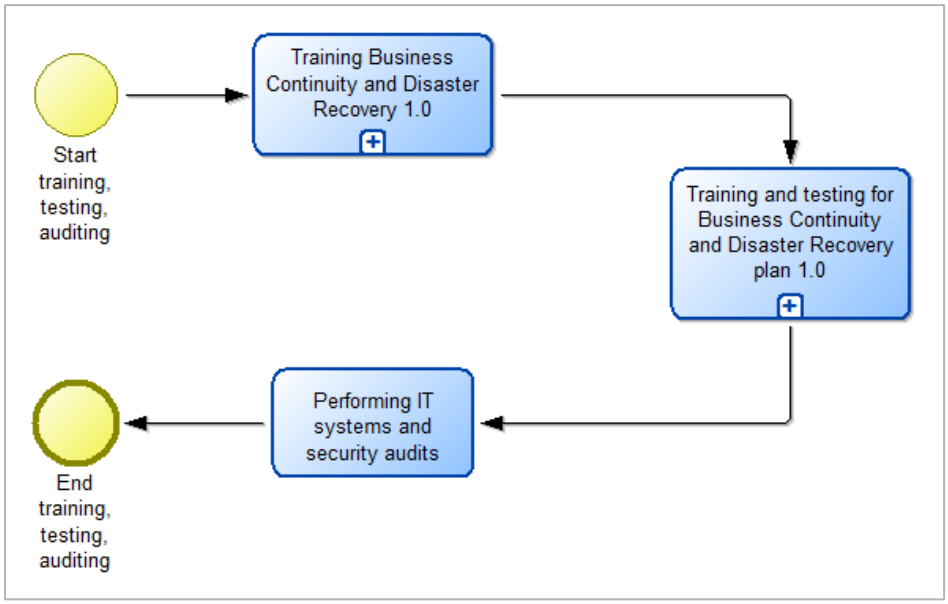

Abbildung 57: Training, Testen, Prüfen

Mögliche verwendete Test- und Übungsarten können sein:

- **Funktionstest** Die Prozeduren, Teilprozesse und Systemgruppen werden auf ihre Funktionalität überprüft.
- **Plan-Reviews** Überprüfung einzelner Pläne der Notfalls- und Krisenbewältigung.
- **Planbesprechungen** Mögliche Szenarien werden vorgegeben und theoretisch durchgespielt.
- **Kommunikations- und Alarmierungsübungen** Überprüfung der Kommunikationsmittel und der nutzenden Technologien.
- **Simulation von Szenarien** Prozeduren und Maßnahmen werden für die Bewältigung von Notfallszenarien auf ihre Funktionalität getestet.
- **Ernstfall- oder Vollübungen** Alle Hierarchieebenen und auch Externe werden bei den Ernstfall- und Vollübungen miteinbezogen. [Bund08a]

5.1.6.1 Training Business Continuity und Disaster Recovery

Vorsorgemaßnahmen, organisatorische Strukturen und unterschiedliche Pläne sind durch regelmäßige Tests und Übungen zu überprüfen. Jeder Betrieb sollte Schulungen und Trainings in den Bereichen Erste Hilfe und Reanimation wie auch Möglichkeiten zu Zertifizierungen und Auffrischungskursen für jeden Mitarbeiter anbieten. Die ideale Herangehensweise als Unterstützung für Trainings ist die Entwicklung eines Trainingsprojektplans (siehe Abbildung 58). [SnRi14]

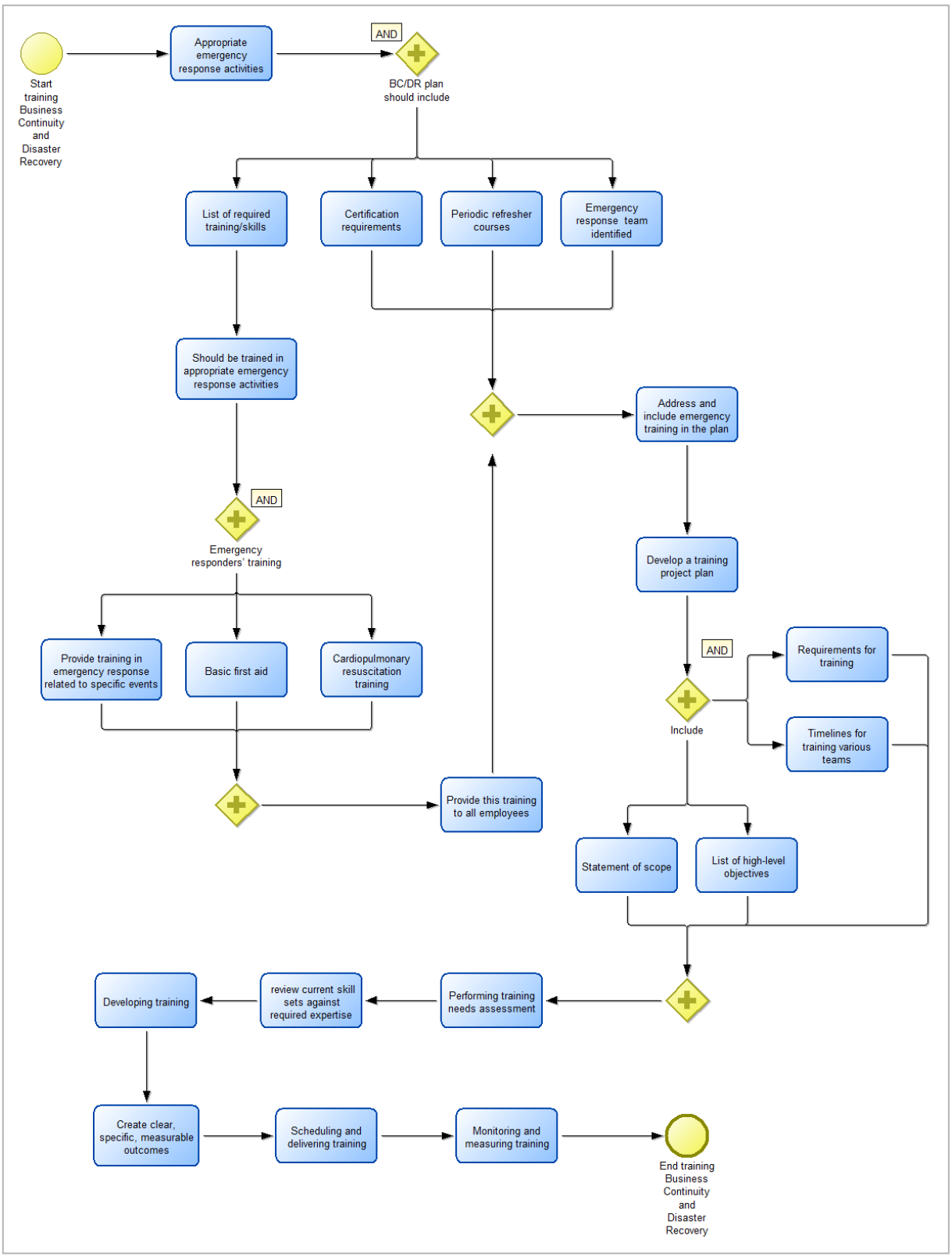

Abbildung 58: Training BC und DR

5.1.6.2 Training und Test des Business Continuity und Disaster Recovery Plans

Wie in Abbildung 59 zu sehen ist, wird nach dem allgemeinen Training der Business Continuity und Disaster Recovery, Training und Tests des BC/DR Plans durchgeführt.

Der sogenannte Trainingsstrukturplan beinhaltet Methoden zur Identifikation notwendiger Trainings, den Entwurf realistischer Szenarien und die Verwendung von Checklisten. [SnRi14]

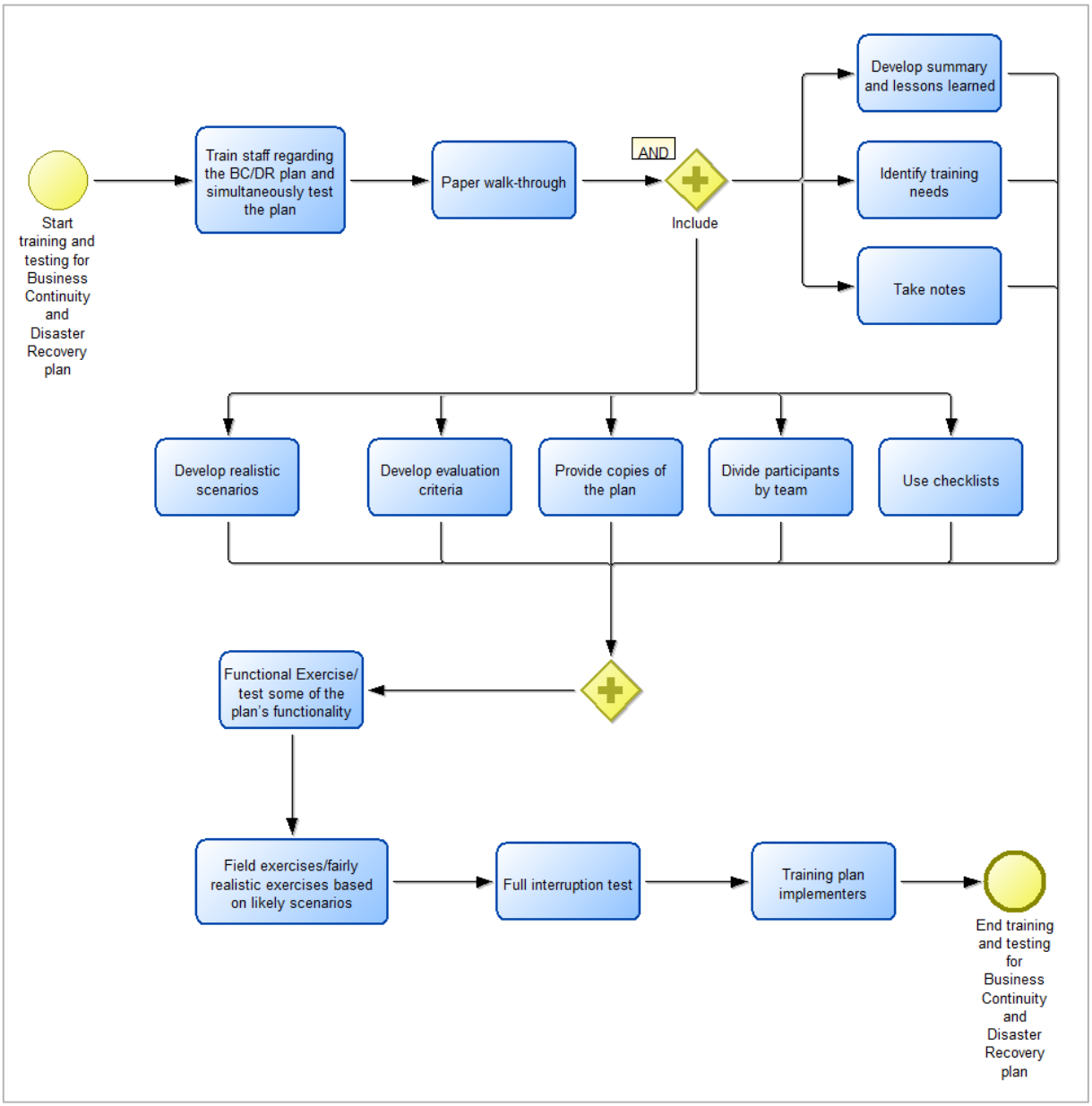

Abbildung 59: Training und Test des BC und DR Plans

5.1.7 Aufrechterhaltung des BC/DR Plans

Die Abbildung 60 stellt den Prozess der Aufrechterhaltung des BC/DR Plans dar. Der Notfallmanagement Prozess muss regelmäßig auf seine Wirksamkeit und Effizienz überprüft werden, Vorsorgemaßnahmen müssen umgesetzt werden und Dokumente fortlaufend aktualisiert werden. Das Management sollte regelmäßig Kontrollen und Bewertungen der Prozesse durchführen. [Bund08a]

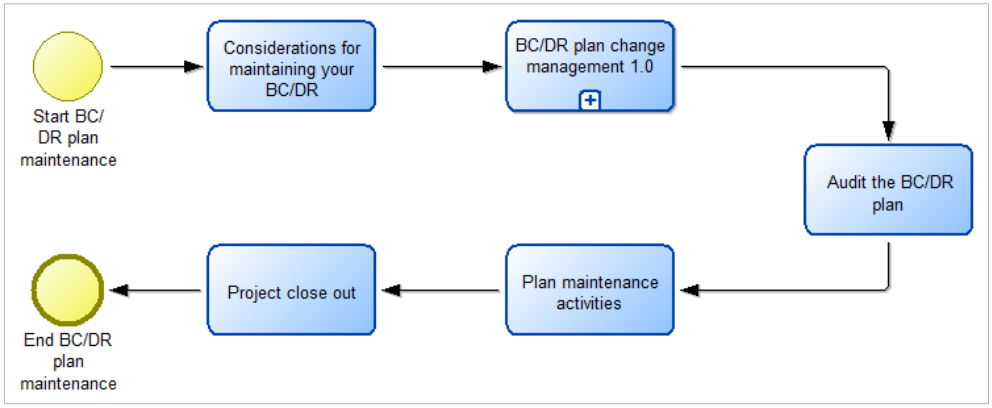

Abbildung 60: Aufrechterhaltung des BC/DR Plans

5.1.7.1 BD/DR Plan Change Management

Regelmäßige Veränderungen müssen durch das Change Management (siehe Abbildung 61) dokumentiert werden. Veränderungen in den Bereichen der Informationstechnologie, des Betriebs und der Geschäftsprozesse wie auch gesetzliche und strategische Veränderungen müssen bewertet, und in den gesamten Geschäftsprozess neu eingearbeitet werden. [SnRi14]

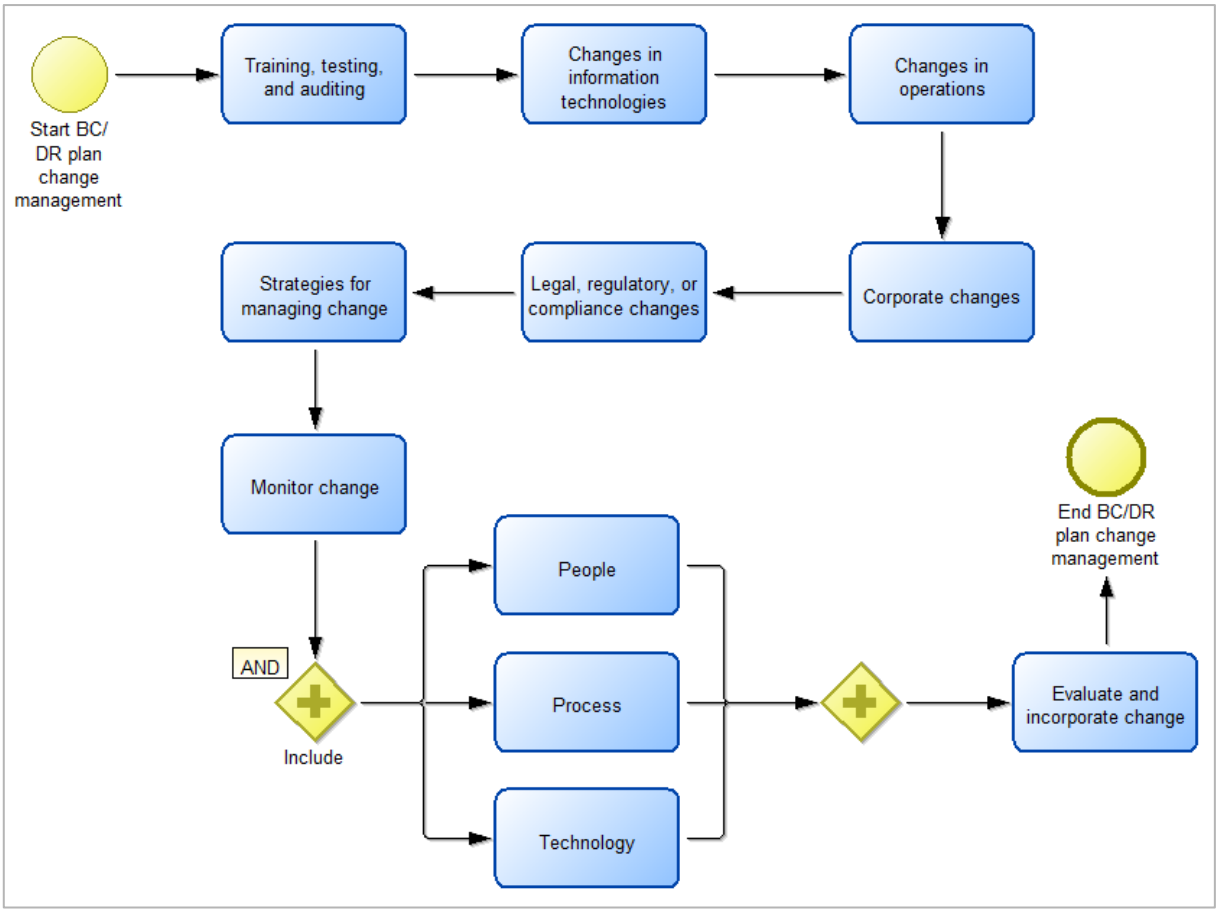

Abbildung 61: BC/DR Plan Change Management

5.2 IT-Infrastrukturlösungen

IT-Unternehmen fokussieren sich mittlerweile schon vermehrt auf die Entwicklung von Technologielösungen für kleine und mittlere Unternehmen in den Bereichen Business Continuity Management und Disaster Recovery. Das entwickelte Business Continuity Management Modell kann mit vorhandenen IT-Infrastrukturlösungen, dienend als Unterstützung, durchgeführt und angewendet werden. In den kommenden Unterkapiteln werden vier IT-Unternehmen und ihre Servicevorschläge für Business Continuity Management dargestellt, um einen Einblick zu geben, wie Vielfältig solche Angebote sein können.

5.2.1 Fujitsu Technology Solutions

Die Fujitsu Technology Solutions GmbH entwickelte eine virtualisierte Lösung für den Betrieb von SAP IT-Infrastrukturen, das sogenannte Flex Frame Compact for SAP (siehe Abbildung 62).

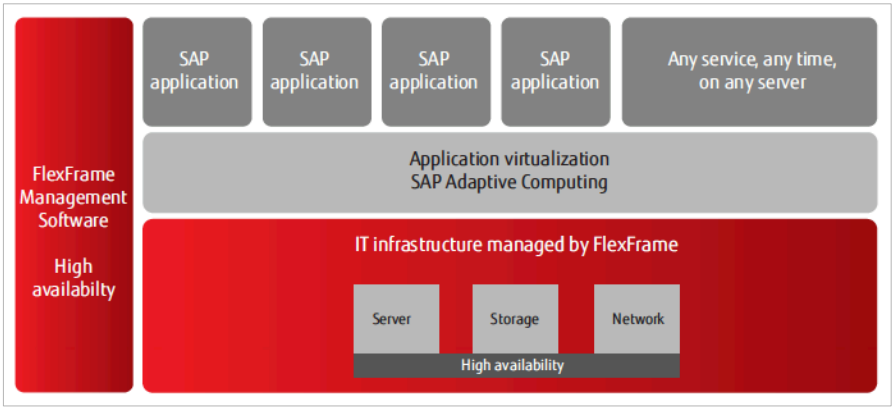

Abbildung 62: Flex Frame Compact for SAP [Fuji00]

Die IT-Infrastrukturlösung Flex Frame von Fujitsu Technology Solutions unterstützt die Virtualisierung von Services, Applikationen und Datenbank Services, um eine bessere und flexiblere Serverauslastung zu erreichen. Flex Frame zeichnet sich durch die Komponenten Control Center, Application Nodes, Switches und Storage Area Network aus. [Fuji00]

5.2.2 Hewlett Packard

HP bietet Business Continuity Services wie Beratungsleistungen durch Experten (Business Continuity Consulting, IT-Service Continuity Management und High Availability Consulting), Managed Services und cloudbasierten Services (Data Center Continuity Services, Data Protection Services und Workplace Continuity Services) wie auch Recovery as a Service an. Der Fokus von HP liegt hauptsächlich im Bereich des

Cloudcomputings, verständlich dargestellt in der HP-Infografik über die angebotene cloudbasierte Disaster Recovery Lösung, wie zu sehen in Abbildung 63. [Hewl15a]

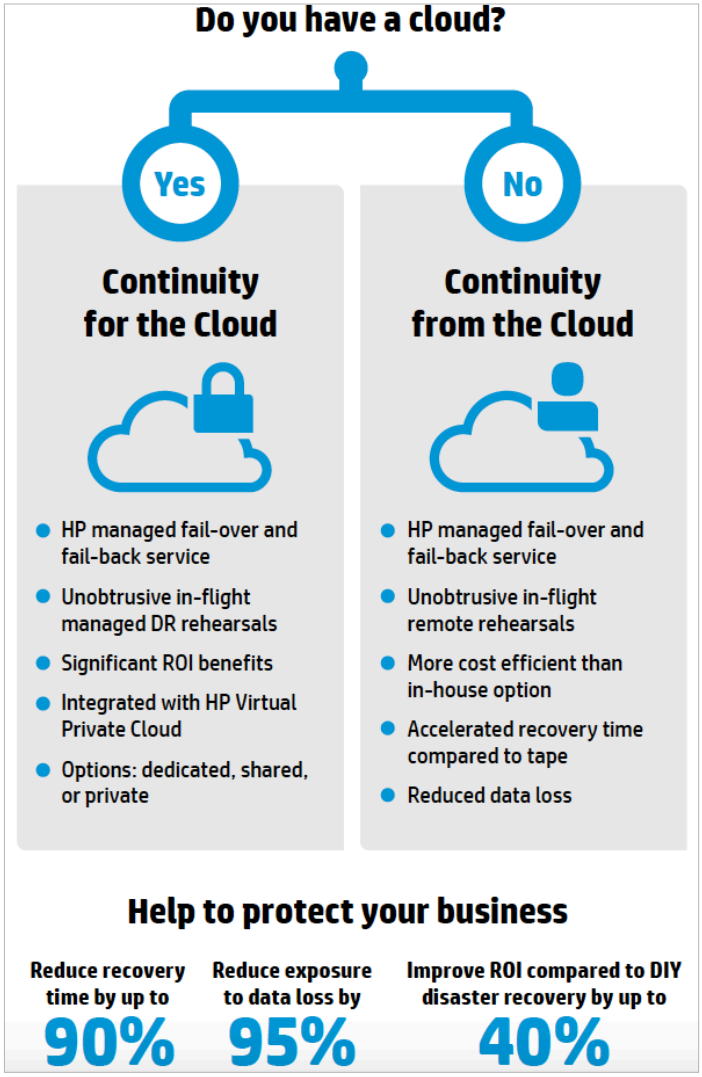

Abbildung 63: Continuity for the Cloud und from the Cloud [Hewl15b]

5.2.3 IBM

IBM Österreich hat ein breites Business Continuity Angebotsspektrum und bietet folgende Resiliency Services an:

- **Beurteilung** Die Ermittlung der Prozesse und Funktionen mit Hilfe einer Business Impact Analyse, einer Risikobeurteilung, einer Beurteilung der Wiederherstellbarkeit, einer Verfügbarkeitsbeurteilung und der Beurteilung von Ausfallsicherheitsprogrammen.
- **Beratung** Entwurf einer Ausfallsicherheitsstrategie mit IBM Business Continuity Consulting.

- **Planung und Design** Services wie der Strategieentwurf, die Entwicklung von Plänen und der Architekturentwurf für Ausfallsicherheit sowie der Entwurf von Ausfallsicherheitsprogrammen und die Entwicklung technischer Verfahren.
- **Implementierung und Test** Business Continuity Tests (Test, Prüfung und Optimierung)
- **Business Continuity Management** Angebot eines Verfügbarkeitsmanagements und Managed Services für die Ausfallsicherheit
- **Disaster Recovery** Services wie IT-Recovery, Wiederherstellung des Arbeitsbereiches und eine schnelle Wiederherstellung von Technologien.
- **Disaster Recovery mit Hilfe der Cloud** Als Cloud-Backup und virtualisierter Serverwiederherstellung verfügbar.
- **Standort- und Gebäudemanagement** Angebote der Strategiefindung für das Rechenzentrum, Gestaltung und Aufbau des Rechenzentrums, vordefiniertes modulares Rechenzentrum, Konsolidierung und Umzug des Rechenzentrums wie auch Facilities Cabling Services. [Ibmö15]

5.2.4 Microsoft

Microsoft bietet für kleine und mittlere Unternehmen die eigens entwickelte Cloudtechnologie Azure an (siehe Abbildung 64). Diese Lösung bietet ein flexibles Backup wie auch die Speicherung von Daten und die Datenwiederherstellung in und aus der Cloud an. [Micr14]

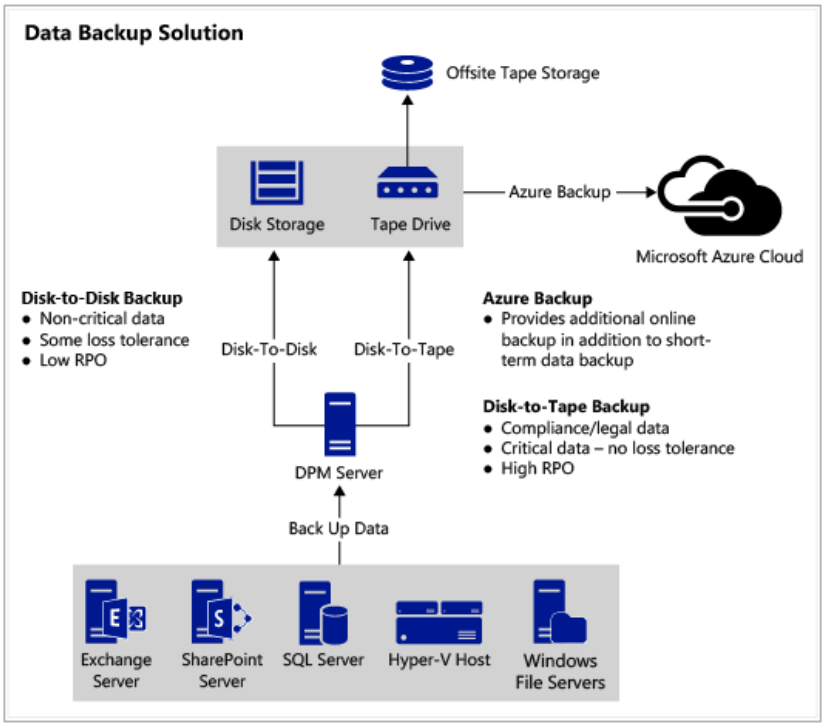

Abbildung 64: Microsoft Azure [Micr14]

6 Anwendung des Modells

Die Anwendung des Modells erfolgt durch eine Vergleichsanalyse mit der IT Infrastructure Library (ITIL). Dies bedeutet, dass der Business Continuity Management Prozess auf den ITIL Service Delivery Prozess abgebildet wird, um den funktionsfähigen Einsatz des Modells in der Praxis bei klein- und mittleren Unternehmen zu garantieren. In den nächsten Unterkapiteln wird ein Überblick über das IT-Service Management wie auch ITIL geschaffen und darauf aufbauend der Vergleich der Modelle durchgeführt.

6.1 IT Infrastructure Library (ITIL)

Die IT Infrastructure Library (ITIL) wird von [Beim10] als ein Standard für das IT-Service Management definiert mit dem Ziel, Services optimal auf die Anforderungen aus dem Business abzustimmen und regelmäßig auf optimale Unterstützung der Geschäftsprozesse zu überprüfen. Die aktuelle Version 3 orientiert sich an einem IT-Service Lifecycle und beschreibt den Lebenszyklus des IT-Services von der Erfassung der Anforderungen über die Gestaltung, Implementierung und den Betrieb bis hin zur kontinuierlichen Anpassung der Servicequalität.

6.1.1 IT-Service Management

Das IT Service Management wird laut ITIL [Olbr08] als ein Prozess und eine Vorgehensweise definiert, um IT-Dienstleistungen zielgerichtet, kundenfreundlich und kostenoptimiert zu erbringen, zu planen, zu steuern und zu überwachen. Bei ITIL steht der Kunde mit seinen Anforderungen und Bedürfnissen im Vordergrund und er wird einerseits in der Rolle des Vertragspartners und andererseits in der Rolle des Anwenders gesehen. Das IT-Servicemanagement gliedert sich, wie in Abbildung 65 zu sehen ist, in zwei Bereiche, dem Service Support Prozess und Service Delivery Prozess. Der Prozess des Service Supports ist auf die operativen Prozesse ausgerichtet, wohingegen der Prozess des Service Deliverys sich mit den planungs-, entwicklungs- und bereitstellungsrelevanten sowie vertragsrechtlichen, strategischen, taktischen und kostenseitigen Themen auseinandersetzt.

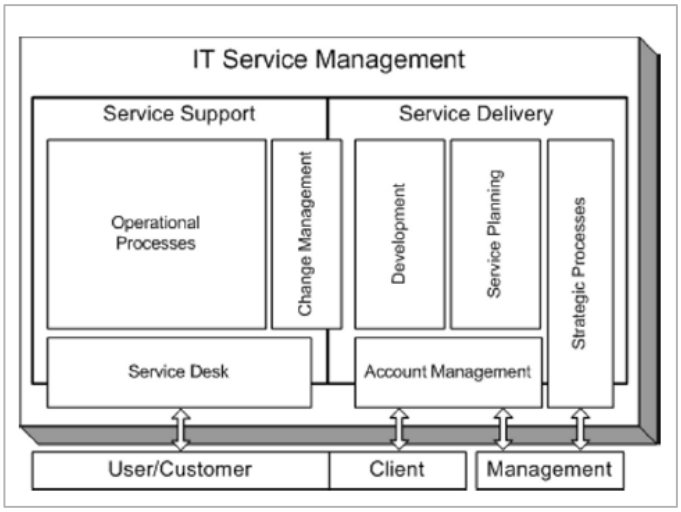

Abbildung 65: IT Service Management [Olbr08]

6.1.1.1 Service Delivery

Der Prozess Service Delivery, zu sehen in Abbildung 66, besteht aus fünf Bereichen, dem Service Level Managament, dem Availability Management, dem Capacity Management, dem Finance Management und dem Continuity Management. [Olbr08]

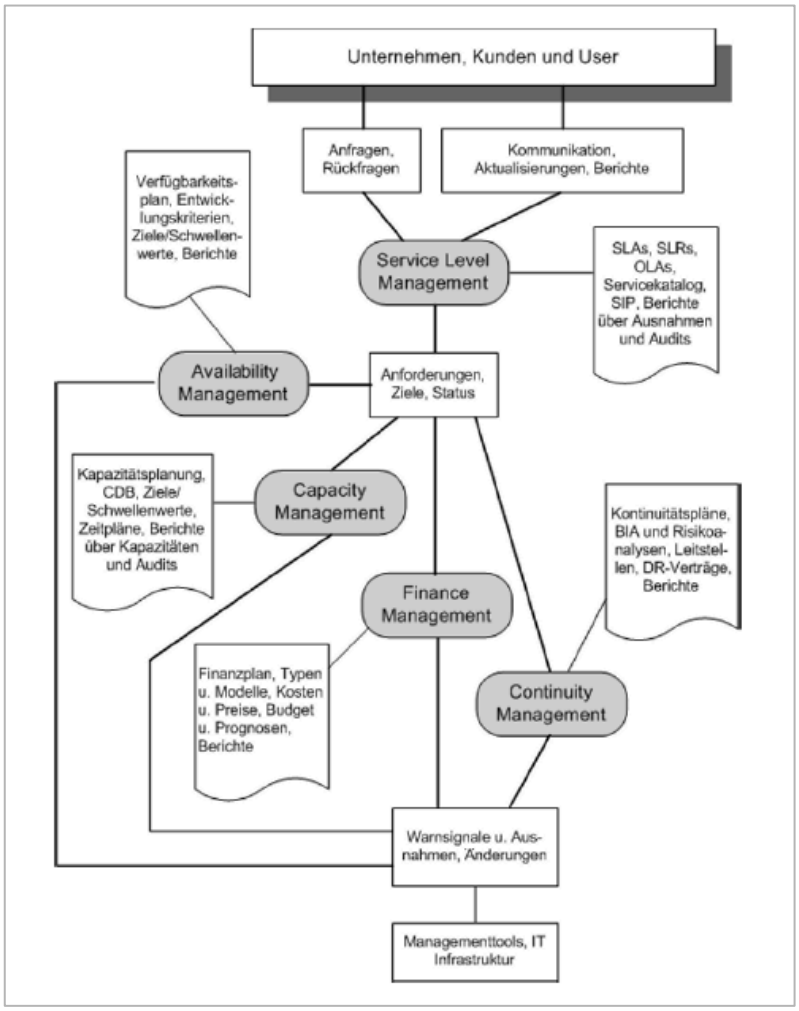

Abbildung 66: Service Delivery Prozess [Olbr08]

6.1.2 IT-Service Lifecycle

Der IT-Service Lifecycle, zu sehen in Abbildung 67, besteht aus fünf Prozessschritten, der Service Strategy, dem Service Design, der Service Transition, der Service Operation und dem Continual Service Improvement. [Beim10]

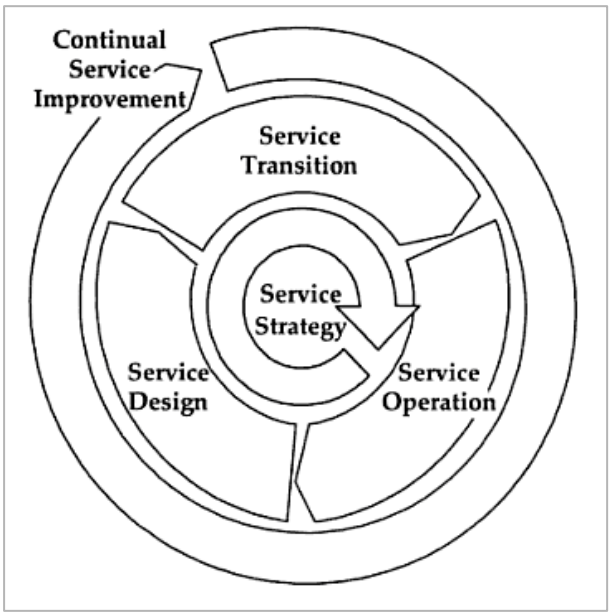

Abbildung 67: ITIL Service Lifecycle [BVGM08]

Der Service Delivery Prozess ist in der neuen Version 3 der IT Infrastructure Library in der Phase des Service Designs wiederzufinden.

6.1.2.1 Service Design

Das Service Design beschäftigt sich mit dem Entwurf und der Entwicklung von Services und den zugehörigen Prozessen mit dem Ziel der Einführung in eine Produktivumgebung. Der Prozess des Entwurfs effektiver und effizienter IT-Services beinhaltet die Funktionalität, die Verfügbarkeit von Ressourcen sowie die verfügbare Zeit. Die Service Design Phase im Lebenszyklus beginnt mit der Nachfrage nach neuen oder geänderten Anforderungen des Kunden und endet mit einem Entwurf für eine Servicelösung. [JKPT08] Dieser Entwurfsprozess besteht aus folgenden Schritten und gleicht dem Projektstrukturplan des Business Continuity Management Modells in der Vorgehensweise bei der Entwicklung des Lösungsansatzes:

- **Service Lösung** Der Entwurf von Service Lösungen erfolgt durch die Analyse und Entwicklung zugehöriger Anforderungen, Ressourcen und Kapazitäten.
- **Serviceportfolio** Der Entwurf des Serviceportfolios dient als Unterstützung aller Prozesse hinsichtlich Systemen und Werkzeugen.

- **Architektur** Eine Unternehmensarchitektur mit den Elementen Service Architektur, Anwendungsarchitektur, Informationsarchitektur und IT Infrastruktur Architektur wird entworfen.
- **Prozesse** Aktivitäten, Inputs und Outputs werden durch den Entwurf von Prozessen definiert.
- **Systeme und Metriken zur Messung** Regelmäßige Bewertungen müssen durchgeführt werden, um den Entwicklungsprozess erfolgreich führen zu können. Der Fortschritt, die Erfüllung, die Effektivität wie auch die Effizienz der Prozesse muss regelmäßig überprüft werden. [JKPT08]

Die verantwortlichen Prozesse und Aktivitäten für den Entwurf einer neuen oder geänderten Service Lösung werden in den nächsten Punkten näher beschrieben. Jedoch wird nur auf die Prozesse eingegangen, welche als Vergleich für das Business Continuity Management Modell verwendet werden können.

6.1.2.1.1 IT Service Continuity Management

Das IT-Service Continuity Management (ITSCM) leitet sich direkt vom Business Contiunity Management des Kunden ab und stellt sicher, dass der Kunde im Katastrophenfall mit einem definierten Minimum an Services arbeiten kann. Die Ressourcen sind so zu gestalten, dass die Services zur Unterstützung der Geschäftsprozesse nach einer Katastrophe in der vorgegebenen Zeit wiederhergestellt werden können. [Beim10]

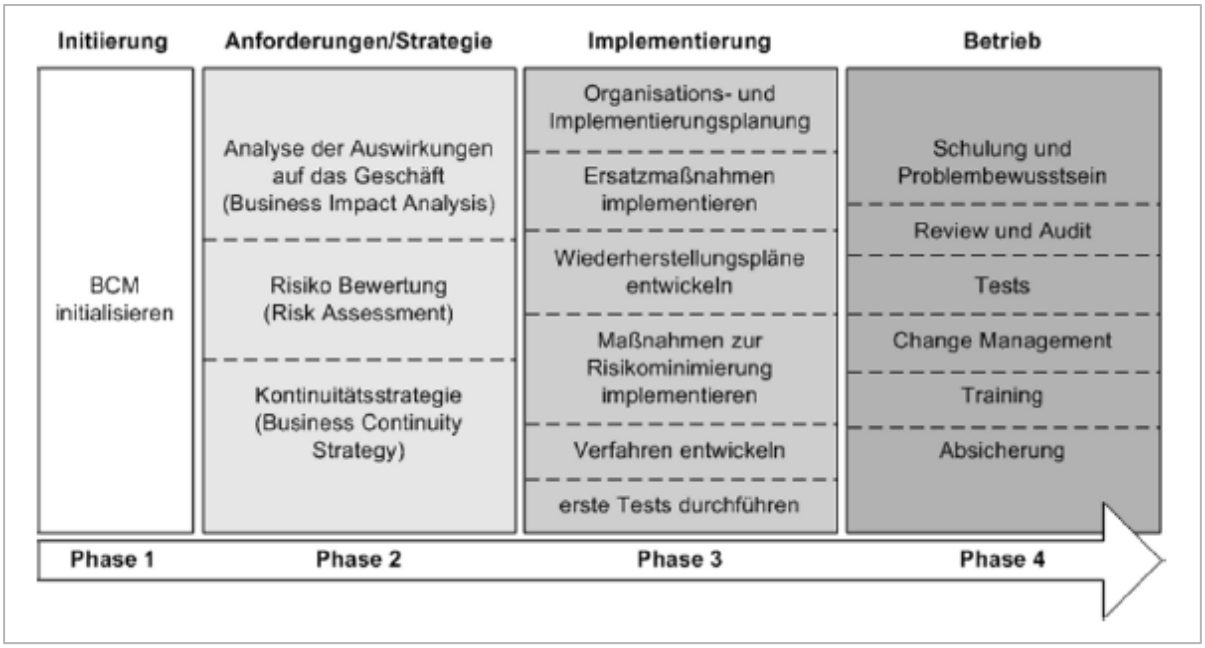

Abbildung 68: ITSCM Phasenmodell [Olbr08]

Der ITSCM-Plan gliedert sich, wie in Abbildung 68 zu sehen ist, in 4 Phasen:

- I**nitiierung** Policies werden definiert, um die Ziele für die Prozesse zu definieren. Dies beinhaltet unter anderem die Definition von Kriterien für die Bewertung einer Katastrophe.
- **Anforderungen und Strategie** Um die Anforderungen zu Erkennen und die Strategie zu gestalten wird eine Business Impact Analyse und ein Risk Assessment durchgeführt wie auch eine IT-Service Continuity Strategy entworfen.
- **Implementierung** Geplante Maßnahmen in der Produktivumgebung werden mit der Erstellung von Notfall-Kommunikationsplänen, Schadensermittlungs- und Bewertungsplänen, Bergungs- und Rettungsplänen, Beschaffungsplänen für die wichtigsten Daten sowie Krisenmanagement- und Public-Relations Plänen implementiert.
- **Operativer Betrieb** Die Prozesse werden durch Ausbildungen und Trainings, regelmäßigen Reviews, Tests und Change Management im Unternehmen etabliert. [Beim10]

6.1.2.1.2 Service Level Management

Das Service Level Management (SLM) hat die Aufgabe, verbindliche Vereinbarungen und Regelungen für die Erbringung von IT Serviceleistungen in Form von Vertragswerken zu erstellen und zu dokumentieren. [Olbr08]. Der Fokus wird sowohl auf die Betrachtung und Verbesserung bestehender Services wie auch auf die Umsetzung neuer oder veränderter Kundenanforderungen in neue Services gelegt. Anforderungen des Kunden werden erfasst, dokumentiert und bei der Gestaltung der Services umgesetzt sowie Service Level Agreements (SLA) definiert, dokumentiert und vereinbart. [Beim10]

6.1.2.1.3 Service Catalogue Management

Das Service Catalogue Management (SCM) hat als Ziel einen aktuellen Servicekatalog mit definierten Quellen für konsistente Informationen aller vereinbarten Services bereitzustellen und zu pflegen. [Beim10]

6.1.2.1.4 Capacitiy Management

Das Capacity Management (CM) befasst sich mit der Bereitstellung der Ressourcen und der Kapazität und Performance von Services. [Beim10] Es werden aktuelle und künftige Anforderungen an die Organisation und die IT-Infrastruktur betrachtet, der Fokus liegt auf der gesamten Hardware und Software innerhalb der IT-Infrastruktur. [Olbr08]

6.1.2.1.5 Availability Management

Das Availability Management (AM) ist ein Prozess zur Optimierung der Nutzung und der Leistungsfähigkeit der IT-Infrastruktur. Es wird dafür gesorgt, dass die IT-Services im Normalbetrieb stets verfügbar sind (technische Verfügbarkeit aller IT-Komponenten). Dabei sind Kontinuität, Wartbarkeit und Fehlertoleranz die wichtigsten Qualitätsmerkmale. [Olbr08]

6.1.2.1.6 Information Security Management

Das Information Security Management (ISM) befasst sich mit der Identifizierung von Risiken bezüglich der Informationssicherheit und deren Maßnahmen. Die zentralen Ziele des ISM sind die Garantie der Verfügbarkeit, Vertraulichkeit und Integrität der Informationen. [Beim10]

6.2 Vergleich Business Continuity Modell – ITIL Framework

Der Vergleich des Business Continuity Modells mit der Phase Service Design des ITIL Frameworks hat ergeben, dass alle modellierten Prozesse des Business Continuity Modells im ITIL Framework wiederzufinden sind (vergleiche Tabelle 9). Alle Prozesse des IT Service Continuity Managements sind im Projektstrukturplan des Modells detailliert dargestellt. Der Business Continuity und Disaster Recovery Plan beinhalten alle restlichen Phasen des Service Designs.

Tabelle 9: Vergleich des Business Continuity Modells mit dem ITIL Framework

ITIL Framework (Service Design)		**Business Continuity Modell**	
IT Service Continuity Management • Initiierung • Anforderungen und Strategie • Implementierung • Operativer Betrieb	✓	Projektstrukturplan • Projektvorbereitung • Business Impact Analyse Risikoanalyse Schadensminimierungsstrategie • Business Continuity und Disaster Recovery Plan • Training, Testen, Prüfen Aufrechterhaltung des BC/DR Plans	✓
Service Level Management	✓	Business Continuity und Disaster Recovery Plan	✓
Service Catalogue Management	✓		
Capacitiy Management	✓		
Availability Management	✓		
Information Security Management	✓		

7 Conclusio

Diese Abschlussarbeit befasst sich mit der Entwicklung einer Architektur, die die Resilience für Informationssysteme im Katastrophenschutzeinsatz gewährleistet. Es wurde den Fragen nachgegangen: Was ist Business Continuity Management? Sind Informationssysteme resilient? Wie kann eine resiliente Architektur aussehen?

Das Business Continuity Management ist Teil eines Notfallplans, kann im Notfallmanagementprozess wiedergefunden werden und dient als Grundlage bei der Entwicklung der Architektur und der anschließenden Entwicklung des Modells. Die wichtigsten Notfallmanagementprozessschritte sind die Analyse des Unternehmens, die Feststellung der Risiken, die Entwicklung einer Strategie wie auch die Erstellung und Erprobung des Plans. Diese Prozessschritte können mit Hilfe eines Maßnahmenkatalogs in kleinen und mittleren Unternehmen umgesetzt werden, um die Geschäftsfortführung und den Wiederanlauf vor, während und nach einer Katastrophe zu gewährleisten. Resiliente Management Systeme mit den Prozessschritten Erkennen, Diagnose und Evaluierung, Bearbeitung und Wiederherstellung, wie auch Eskalation und Institutionalisierung dienen als Unterstützung bei der Umsetzung eines widerstandsfähigen Business Process Managements. Um resiliente Informationssysteme einzuführen oder bestehende Systeme resilienter zu machen, kann das CERT Resilience Management Model mit dem Fokus auf das Technologiemanagement eingesetzt werden. IT Infrastruktur Resilience Techniken wie Cloud Computing und Virtualisierung, aber auch Internet Resilience Techniken wie Protection Switching und Multiprotocol Label Switching, sind Ansätze, die Informationssysteme resilienter machen können.

Um nun eine Architektur unter Berücksichtigung der Business Continuity und Resilience zu entwickeln, wurde als Grundlage das IS Architekturplanungskonzept mit allen Ebenen von der Strategie, der Organisationsstruktur, der Informationsstruktur, der IS-Infrastruktur bis hin zur IT-Infrastruktur verwendet. Um anschließend ein Modell zu entwickeln, wurden Teile des Zachmann Frameworks mit dem Boeing Information Service Modell kombiniert und ein Projektstrukturplan erstellt. Dieser Projektstrukturplan ist Schritt für Schritt durchzuführen und dient als Leitfaden für kleine und mittlere Unternehmen bei der Einführung eines Business Continuity Managements. Zusätzlich zu diesem Modell können vorhandene IT-Infrastrukturlösungen als Unterstützung eingesetzt werden. Das entwickelte Business Continuity Modell wurde anschließend mit der Phase des Service Designs des ITIL Frameworks verglichen um festzustellen, ob dieses Modell auch in der Praxis bei einem Unternehmen einsetzbar wäre. Das Ergebnis zeigte, dass alle relevanten Prozesse des ITIL Frameworks im Business Continuity Management Modell

wiederzufinden sind und somit der erfolgreiche praxisnahe Einsatz in einem Unternehmen garantiert ist.

7.1 Diskussion der Ergebnisse

Business Continuity Management und Disaster Recovery sind zwei noch weiterhin zu erforschende Bereiche. Die theoretische Aufarbeitung der Literatur zeigte, dass es wenige wissenschaftliche Quellen gibt und oft Begriffe wie „...noch im Entstehen...“ zu finden sind. Was sich jedoch aus den aktuellen literarischen Quellen zeigt ist, dass konzeptuell und prozessorientiert ein weites Spektrum vom Projektmanagement und Krisenmanagement bis hin zur Systemarchitektur gegeben ist. Große Unternehmen haben meistens selbst entwickelte Business Continuity Management Lösungen implementiert wohingegen kleine und mittlere Unternehmen auf externe kostspielige Lösungen angewiesen sind. Die in dieser Abschlussarbeit modellierten Prozesse des Business Continuity Managements können als Leitfaden, wie auch als Maßnahmenkatalog angesehen werden, und dienen kleinen und mittleren Unternehmen zur Unterstützung bei der Einführung eines internen Business Continuity Managements. Zusätzlich können Angebote, wie zum Beispiel das IT-Infrastrukturangebot des IT-Unternehmens IBM, als Unterstützung durch umfangreiche IT-Services im Bereich Business Continuity Management und Disaster Recovery verwendet werden.
Ein Teil dieser Arbeit (Business Continuity Management und das Modell) wurde im Rahmen eines Forschungsprojektes in Kooperation mit der BMLVS/LVAk Landesverteidigungsakademie Wien, der Universität für Bodenkultur Wien, dem BMI, der h2 projekt.beratung KG wie auch der ingentus decision support KG erarbeitet und getestet. Um jedoch aussagekräftige Ergebnisse zu liefern, müsste das Modell in einem kleinen und mittleren Unternehmen eingesetzt und getestet werden. Durch den Vergleich des Business Continuity Management Modells, mit einer Phase des ITIL Frameworks, konnte ein Praxisbezug hergestellt werden. Es kann jedoch dadurch nicht hundertprozentig garantiert werden, dass dieses Modell die Resilience für Informationssysteme im Katastrophenschutzeinsatz gewährleistet. Dies zeigt, dass wissenschaftlich und literarisch eine Definition, wie auch eine theoretische Vorgehensweise für die Umsetzung eines Business Continuity Managements gegeben sind.

7.2 Schlussfolgerung

Business Continuity Management und Resilience sind Themen, die zu dieser Zeit ein großes Interesse wecken. Daten in großen Mengen müssen gespeichert werden,

jederzeit verfügbar sein und gegen äußere Einwirkungen geschützt sein. Ein Hacker Angriff, ein Stromausfall oder ein Erdbeben können mehrere oder alle Geschäftsprozesse unterbrechen und langfristige Geschäftsunterbrechungen zur Folge haben. Unternehmen sind abhängig von ihren Daten, um am globalen Markt wettbewerbsfähig zu bleiben. Dementsprechend sollten Notfallmanagementprozesse in jedem Unternehmen im Management verankert sein. Diese Verankerung ist jedoch für kleine und mittlere Unternehmen kostspielig und mit dem Einsatz von mehr Personal verbunden. Das Modell dieser Abschlussarbeit kann als kostengünstige Lösung als Unterstützung bei der Umsetzung eines Business Continuity Managements in Unternehmen verwendet werden.
Eine kostspieligere Lösung könnte der Einsatz von Cloud Computing sein, um Daten zu speichern und zu verwalten. Jedoch ist dieses Konzept noch sehr umstritten und wird mit großer Skepsis betrachtet. Datensicherheit, Compliance, und Datenschutz sind sicherheitsrelevante Aspekte, die den Einsatz von Cloud Computing in Unternehmen verlangsamen. Eine weitere unterstützende Lösung kann der Einsatz eines Business Continuity Standards (zum Beispiel der BSI-Standard 1000-4 des Bundesamts für Sicherheit in der Informationstechnik) sein, um die wichtigsten unternehmensrelevanten Prozesse in einem Unternehmen einzuführen.
Unternehmen werden in Zukunft durch den Einsatz von Business Continuity Management Konzepten konkurrenzfähiger, wie auch gewinnmaximierender arbeiten können, da alle Geschäftsprozesse vor, während und nach einer Katastrophe verfügbar sein können. Zusätzlich sollte jedoch noch der Fokus auf die Themen Business Contunity Management wie auch Resilience, in Kombination mit Datensicherheit und Datenschutz, gelegt werden. Wie kann Business Continuity Management kostengünstig in Unternehmen eingeführt werden und sowohl die Sicherheit wie auch den Schutz der Daten garantieren?

8 Informationen über die Autorin

ANGABEN ZUR PERSON

Name	**PIA PATRICIA HOSCHEK, BSC**
Staatsangehörigkeit	**Österreich**
Geburtsdatum	**12.08.1989**

SCHUL- UND BERUFSBILDUNG

DEZEMBER 2012 – DEZEMBER 2015	Masterstudium Wirtschaftsinformatik Universität Wien Masterarbeit: „Architektur zur Gewährleistung der Resilience für Informationssysteme im Katastrophenschutzeinsatz“
OKTOBER 2008 – DEZEMBER 2012	Bachelorstudium Wirtschaftsinformatik Universität Wien Bachelorarbeit: „ITIL Security Compliance“
OKTOBER 2007 – SEPTEMBER 2008	Bachelorstudium Sportwissenschaften und Bachelorstudium Ernährungswissenschaften Universität Wien
SEPTEMBER 1999 – JUNI 2007	Sigmund Freud Gymnasium Wien 2

BERUFSERFAHRUNG

APRIL 2014 – MÄRZ 2015	Universität Wien, Fakultät für Informatik Forschungsgruppe Multimedia Information Systems Wissenschaftliche Projektmitarbeiterin im Rahmen des Forschungsprojektes „LMK-Muse“ (in Kooperation mit der BMLVS/LVAk, der Boku Wien, dem BMI, der h2 projekt.beratung KG wie auch der ingentus decision support KG)

9 Literaturverzeichnis

[Bank03] BANK OF JAPAN: Business Continuity Planning at the Bank of Japan (2003)

[Baye13] BAYER, FRANZ ; KÜHN, H. (Hrsg.): *Prozessmanagement für Experten. Impulse für aktuelle und wiederkehrende Themen*. Berlin Heidelberg : Springer Verlag Berlin Heidelberg, 2013

[BeFD10] BERL, ANDREAS ; FISCHER, ANDREAS ; DE MEER, HERMANN: Virtualisierung im Future Internet: Virtualisierungsmethoden und Anwendungen. In: *Informatik-Spektrum* Bd. 33 (2010), Nr. 2, S. 186–194

[Beim10] BEIMS, MARTIN: *IT-Service Management in der Praxis mit ITIL 3: Zielfindung Methoden Realisierung*. 2. Aufl. München : Carl Hansen Verlag, 2010

[BhDB11] BHAMRA, RAN ; DANI, SAMIR ; BURNARD, KEVIN: Resilience: the concept, a literature review and future directions. In: *International Journal of Production Research* Bd. 49 (2011), Nr. 18, S. 5375–5393

[Boci00] BOC INFORMATION TECHNOLOGIES CONSULTING AG: *ADONIS:Community Edition*. URL http://en.adonis-community.com/welcome/download/

[Bund08a] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 100-4, Notfallmanagement* (Nr. 1). Bonn, 2008

[Bund08b] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 100-2. IT-Grundschutz-Vorgehensweise* (Nr. 2). Bonn, 2008

[Bund13] BUNDESKANZLERAMT ÖSTERREICH UND A-SIT: Österreichisches Informationssicherheitshandbuch (2013)

[BVGM08] BUCHSEIN, RALF ; VICTOR, FRANK ; GÜNTHER, HOLGER ; MACHMEIER, VOLKER: *IT-Management mit ITIL V3: Strategie, Kennzahlen, Umsetzung*. 2. Aufl. Wiesbaden : Vieweg + Teubner Verlag | GWV Fachverlage GmbH, 2008

[CACW10a] CARALLI, RICHARD A. ; ALLEN, JULIA H. ; CURTIS, PAMELA D. ; WHITE, DAVID W. ; YOUNG, LISA R.: Improving Operational Resilience Processes. The CERT Resilience Management Model. In: *IEEE Second International Conference on Social Computing* (2010), S. 1165–1170

[CACW10b] CARALLI, RICHARD A. ; ALLEN, JULIA H. ; CURTIS, PAMELA D. ; WHITE, DAVID W. ; YOUNG, LISA R.: CERT® Resilience Management Model, Version 1.0. Improving Operational Resilience Processes. In: *Software Engineering Institute* (2010)

[CBFP04] CANDEA, GEORGE ; BROWN, AARON B. ; FOX, ARMANDO ; PATTERSON, DAVID: Recovery-oriented computing: building multitier dependability. In: *Computer* Bd. 37 (2004), Nr. 11, S. 60–67

[Cisc08] CISCO SYSTEMS, INC.: *Router Virtualization in Service Providers*. URL http://www.cisco.com/c/en/us/solutions/collateral/routers/carrier-routing-system/white_paper_c11-512753.pdf. - abgerufen am 2015-05-23

[Deut03] DEUTER, M. (Hrsg.): *Das große Oxford Wörterbuch mit Exam Trainer und CD-ROM*. Oxford : Oxford University Press, 2003

[Fiks03] FIKSEL, JOSEPH: Designing resilient, sustainable systems. In: *Environmental science & technology* Bd. 37 (2003), Nr. 23, S. 5330–5339

[Fuji00] FlexFrame Compact for SAP. In: FUJITSU TECHNOLOGY SOLUTIONS GMBH (Hrsg.)

[HaNe09] HANSEN, HANS ROBERT ; NEUMANN, GUSTAF: *Wirtschaftsinformatik 1*. 10. Aufl. Stuttgart : Lucius & Lucius, 2009

[HaVä03] HAMEL, GARY ; VÄLIKANGAS, LIISA: *The Quest for Resilience*. URL https://hbr.org/2003/09/the-quest-for-resilience. - abgerufen am 2015-05-31. — Harvard Business Review

[HeES04] HERBANE, BRAHIM ; ELLIOTT, DOMINIC ; SWARTZ, ETHNÉ M.: Business Continuity Management: time for a strategic role? In: *Long Range Planning* Bd. 37 (2004), Nr. 5, S. 435–457

[Hewl15a] HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.: *Continuity Services. Optimale Business Continuity, geringere Risiken und niedrigere Kosten*. URL http://www8.hp.com/de/de/business-services/it-services.html?compURI=1079081. - abgerufen am 2015-06-13

[Hewl15b] HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.: *Infographic: Continuity for the Cloud and from the Cloud*. URL http://www8.hp.com/h20195/V2/GetDocument.aspx?docname=c04164852&cc=us&lc=en. - abgerufen am 2015-06-13

[HoOr97] HOME, JOHN F. ; ORR, JOHN E.: Assessing behaviors that create resilient organizations. In: *Employment Relations Today* Bd. 24 (1997), Nr. 4, S. 29–39

[Ibmö15] IBM ÖSTERREICH: *Resiliency Services*. URL http://www-935.ibm.com/services/at/de/it-services/business-continuity/. - abgerufen am 2015-06-13

[Jack10] JACKSON, SCOTT: *Architecting Resilient Systems. Accident Avoidance and Survival and Recovery from Disruptions*. New Jersey : John Wiley & Sons, Inc., Hoboken, 2010

[Järv12] JÄRVELÄINEN, JONNA: Information security and business continuity management in interorganizational IT relationships. In: *Information Management & Computer Security* Bd. 20 (2012), Nr. 5, S. 332–349

[JKPT08] JONG, ARJEN DE ; KOLTHOF, AXEL ; PIEPER, MIKE ; TJASSING, RUBY ; VAN DER VEEN, ANNELIESE ; VERHEIJEN, TIENEKE ; VAN BON, J. (Hrsg.): *Foundations in IT Service Management basierend auf ITIL V3*. Zaltbommel, Niederlande : Van Haren Publishing, 2008

[JKSK00] JUNGINGER, STEFAN ; KÜHN, HARALD ; STROBL, ROBERT ; KARAGIANNIS, DIMITRIS: Ein Geschäftsprozessmanagement-Werkzeug der nächsten Generation - ADONIS: Konzeption und Anwendungen. In: *Wirtschaftsinformatik* Bd. 42 (2000), Nr. 5, S. 392–401

[KaFC10] KAMMENHUBER, NILS ; FESSI, ALI ; CARLE, GEORG: Resilience: Widerstandsfähigkeit des Internets gegen Störungen - Stand der Forschung und Entwicklung. In: *Informatik-Spektrum* Bd. 33 (2010), Nr. 2, S. 131–142

[KaNo96] KAPLAN, ROBERT S. ; NORTON, DAVID P.: Linking the Balanced Scorecard to Strategy. In: *California Managament Review* Bd. 39 (1996), Nr. 1, S. 53–79

[LaLS10] LAUDON, KENNETH C. ; LAUDON, JANE P. ; SCHODER, DETLEF: *Wirtschaftsinformatik: Eine Einführung*. 2. Aufl. München : Pearson Deutschland GmbH, 2010

[LeGi03] LEHMANN, MICHAEL ; GIEDKE, ANNA: Cloud-Computing - technische Hintergründe für die terretorial gebundene rechtliche Analyse. Cloudspezifische Serververbindungen und eingesetzte Virtualisierungstechnik. In: *Computer und Recht* Bd. 29 (2003), Nr. 9, S. 608–616

[LoNB03] LONDON FIRST ; NATIONAL COUNTER TERRORISM SECURITY OFFICE ; BUSINESS CONTINUITY INSTITUTE: *Expecting the unexpected: Business Continuity in an uncertain world*. England, 2003

[Mars13] MARSHALL, DAVID: *Bluelock provides VMware users with cloud-based disaster recovery*. URL http://www.infoworld.com/article/2614633/virtualization/bluelock-provides-vmware-users-with-cloud-based-disaster-recovery.html. - abgerufen am 2015-07-07. — Info World

[McSp02] MCNURLIN, BARBARA C. ; SPRAGUE, RALPH H.: *Information Systems Management in Practice*. 5. Aufl. Upper Saddle River, New Jersey : Prentice Hall, 2002

[MeGr11] MELL, PETER ; GRANCE, TIMOTHY: The NIST Definition of Cloud Computing. In: *National Institute of Standards and Technology* (2011)

[Micr14] MICROSOFT CORPORATION: *Deploy backup and recovery for business continuity*. URL https://technet.microsoft.com/en-us/library/dn621063.aspx. - abgerufen am 2015-06-16

[MüKA13] MÜLLER, GÜNTER ; KOSLOWSKI, THOMAS G. ; ACCORSI, RAFAEL: Resilience - A New Research Field in Business Information Systems? In: ABRAMOWICZ, W. (Hrsg.): *Business Information Systems Workshops*. Bd. 160. Deutschland : Springer Berlin Heidelberg, 2013, S. 3–14

[Olbr08] OLBRICH, ALFRED: *ITIL kompakt und verständlich: Effizientes IT Service Management - Den Standard für IT-Prozesse kennenlernen, verstehen und erfolgreich in der Praxis umsetzen*. 4. Aufl. Wiesbaden : Vieweg + Teubner Verlag | GWV Fachverlage GmbH, 2008

[PfLe12] PFLANZ, MARK ; LEVIS, ALEXANDER: An Approach to Evaluating Resilience in Command and Control Architectures. In: *Procedia Computer Science* Bd. 8 (2012), S. 141–146

[Pint11] PINTA, JAN: Disaster Recovery Planning as part of Business Continuity Management. In: *AGRIS on-line Papers in Economics and Informatics* Bd. 3 (2011), Nr. 4, S. 55–61

[Proj08] PROJEKT MANAGEMENT AUSTRIA: *pma baseline*. 3.0. Aufl. Österreich : pma, 2008

[Qual15] QUALITY AUSTRIA - TRAININGS, ZERTIFIZIERUNGS UND BEGUTACHTUNGS GMBH: *qualityaustria Erfolg mit Qualität*. URL http://www.qualityaustria.com/index.php?id=2431. - abgerufen am 2015-06-29

[SnRi14] SNEDAKER, SUSAN ; RIMA, CHRIS: *Business Continuity and Disaster Recovery Planning for IT Professionals*. 2. Aufl. Waltham : Elsevier, Inc., 2014

[StHu15] STREBENZ, JAMES P.G. ; HUTCHISON, DAVID: *ResiliNets Wiki*. URL https://wiki.ittc.ku.edu/resilinets/Main_Page. - abgerufen am 2015-01-05. — ResiliNets Wiki

[Thie14] THIEßEN, A. (Hrsg.): *Handbuch Krisenmanagement*. 2. Aufl. Wiesbaden : Springer Fachmedien Wiesbaden, 2014

[ThTh10] THIEL, CHRISTIAN ; THIEL, CHRISTOPH: Business Continuity Management für KMU. In: *Datenschutz und Datensicherheit - DuD* Bd. 34 (2010), Nr. 6, S. 404–407

[ThZa13] THORENZ, LYNN ; ZACHER, MATHIAS: Cloud Computing: Neue Chancen für das Outsourcing. In: RICKMANN, H. ; DIEFENBACH, S. ; BRÜNIG, K. T. (Hrsg.): *IT-Outsourcing: Neue Herausforderungen im Zeitalter von Cloud Computing*. Berlin, Heidelberg : Springer Berlin Heidelberg, 2013

[Tink11] TINKL, BERNHARD: *Vergleich unterschiedlicher Ansätze zur Implementierung eines Business Continuity Management*. Wien, Technische Universität Wien, Diplomarbeit, 2011

[Tüva15] TÜV AUSTRIA AKADEMIE GMBH: *Kursprogramm*. URL https://www.tuv-akademie.at/kursprogramm/detail/p/110.087/event/business-continuity-management-2.html. - abgerufen am 2015-06-29

[Ugav07] UGAVINA, NITHIYA: MDG Technology For Zachman Framework User Guide. In: SPARXSYSTEMS SOFTWARE GMBH (Hrsg.) (2007)

[VACI09] VOGEL, OLIVER ; ARNOLD, INGO ; CHUGHTAI, ARIF ; IHLER, EDMUND ; KEHRER, TIMO ; MEHLIG, UWE ; ZDUN, UWE: *Software-Architektur: Grundlagen - Konzepte - Praxis*. 2. Aufl. Heidelberg : Spektrum Akademischer Verlag, 2009

[WhMa14] WHITMAN, MICHAEL E. ; MATTORD, HERBERT J.: *Management of Information Security*. 4. Aufl. Stanford : Cengage Learning, 2014

10 Anhang mit Abkürzungsverzeichnis

A

AM · *Availability Management*

B

BC · *Business Continuity*
BCM · *Business Continuity Management*
BIA · *Business Impact Analyse*

C

CERT-RMM · *CERT Resilience Management Model*
CIR · Computer Incident Response
CM · *Capacity Management*

D

DDoS · *Distributed Denial of Service*
DNS · *Domain Name System*
DR · *Disaster Recovery*

I

IP · *Internet Protokoll*
IS · *Informationssysteme*
ISM · *Information Security Management*
IT · *Informationstechnologie*
ITIL · *IT Infrastructure Library*
ITSCM · *IT Service Continuity Management*

K

KMU · *Kleine und mittlere Unternehmen*

L

LAN · *Local Area Network*

M

MPLS · *Multiprotocol Label Switching*

S

SCM · *Service Catalogue Management*
SCTP · *Stream Control Transmission Protocol*
SLA · *Service Level Agreements*
SLM · *Service Level Management*

T

TCP · *Transmission Control Protocol*

V

VM · *Virtuelle Maschine*