



Hans-Peter Königs

IT-Risikomanagement mit System

Praxisorientiertes Management von
Informationssicherheits- und IT-Risiken

4. Auflage

Edition <kes>

Herausgegeben von

P. Hohl, Ingelheim, Deutschland

Mit der allgegenwärtigen Computertechnik ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes>-Zeitschrift für Informations-Sicherheit (s.a. www.kes.info), die seit 1985 im SecuMedia Verlag erscheint. Die <kes> behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz.

IT-Notfallmanagement mit System
von Gerhard Klett, Klaus-Werner Schröder und Heinrich Kersten

Der IT Security Manager
von Heinrich Kersten, Gerhard Klett, und Klaus-Dieter Wolfenstetter

Information Security Risk Management
von Sebastian Klipper

IT-Sicherheit kompakt und verständlich
von Bernhard C. Witt

Konfliktmanagement für Sicherheitsprofis
von Sebastian Klipper

Praxis des IT-Rechts
von Horst Speichert

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz
von Heinrich Kersten, Jürgen Reuter und Klaus-Werner Schröder

Security Awareness
von Michael Helisch und Dietmar Pokoyski

Rollen und Berechtigungskonzepte
von Alexander Tsolkas und Klaus Schmidt

Hans-Peter Königs

IT-Risikomanagement mit System

Praxisorientiertes Management von
Informationssicherheits- und IT-Risiken

4. Auflage

PRAXIS

 Springer Vieweg

Hans-Peter Königs
Olsberg, Schweiz

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

ISBN 978-3-8348-1687-0
DOI 10.1007/978-3-8348-2165-2

ISBN 978-3-8348-2165-2 (eBook)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Vieweg

© Springer Fachmedien Wiesbaden 2013

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer Vieweg ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-vieweg.de

Die Unternehmenspraxis – insbesondere in der derzeitigen Euro-Krise – zeigt, wie eng die Chancen unserer Unternehmen mit Risiken aller Art verbunden sind. Aufgrund der Ereignisse in den letzten Jahren unternehmen die Gesetzgeber und Regulatoren immer neue Anläufe und Verbesserungen, um die Risiken sowohl für die Volkswirtschaft, als auch für das einzelne Unternehmen und letztlich den Bürger in einem erträglichen Mass zu halten.

Bei den wesentlichen Neuerungen denken wir beispielsweise an die Datenschutzgesetze, an die neuen Anforderungen des „Basler Ausschusses für Bankenaufsicht“ (Basel II und III) oder an die Anforderungen von Solvency II für Versicherungen. Solche und auch andere Vorgaben stellen nebst den Anforderungen an das Risikomanagement bzgl. der finanziellen Risiken auch jeweils Anforderungen hinsichtlich der Beherrschung der Informationssicherheits- und IT-Risiken.

Die Möglichkeiten der IT aufgrund der globalen Vernetzungen, die Anonymität von Angreifern im Internet sowie die Geschwindigkeit und Komplexität der Arbeitsprozesse und Systeme bieten neben den unbestreitbaren Chancen immer neue und leider auch grössere und schwer fassbare Risiken. Die Risikobeurteilung und -behandlung muss sich dabei an der Wesentlichkeit für die Erreichung der Geschäftsziele orientieren. Deshalb sind neben den Angriffspotentialen aus dem „Cyber Space“ auch Risiken, resultierend aus Verstössen gegen gültiges Recht, mangelhafte Verträge oder schlecht abgestimmtes und überwachtes Outsourcing zu berücksichtigen, um einige Beispiele zu nennen.

Das vorliegende Buch nimmt sich diesen aktuellen Anforderungen in einer für die praktische Umsetzung geeigneten Weise unter Berücksichtigung der aktuellen internationalen Standards an. So werden die unter dem Sammelbegriff „Management-Systeme“ die im Unternehmen zu integrierenden Unternehmensprozesse für das Risikomanagement (ISO 31000) wie auch für die Informationssicherheit (ISO/IEC 2700x-Reihe) und die Geschäftskontinuität (neuer Standard ISO 22301) behandelt.

Ein eigenes neues Kapitel ist dem „Cloud-Computing“ mit entsprechenden Lösungsansätzen für das Management der Risiken zugeschrieben. Die Mitarbeit des Autors in den relevanten Stan-

dardisierungs-Gremien der Schweizerischen Normenvereinigung lässt ihn aus einem reichen Fundus für die Entwicklung und den Einsatz solcher Standards schöpfen. Im Sinne einer ganzheitlichen Betrachtung der Leistung und Sicherheit der IT und der Informationen im Unternehmen geht das Buch auch auf das neue Rahmenwerk CobiT 5 ein.

Wie in den vorherigen Auflagen dieses Buches hat es der Autor wiederum sehr gut verstanden, die zum Teil komplexen Zusammenhänge in einer mit Beispielen und auf das Wesentliche beschränkten Darstellung anschaulich zu behandeln. Dabei kommen dem Autor zweifellos seine langjährigen didaktischen Erfahrungen aus seiner Tätigkeit als Dozierender für verschiedene Fächer des Risikomanagements an der Hochschule für Wirtschaft Luzern zugute.

Wir wünschen auch der vierten, in vielen Aspekten überarbeiteten und ergänzten Auflage den guten Erfolg der vorangegangenen Auflagen.

Dr. Thomas Siegenthaler, Präsident CSI Consulting AG

Vorwort zur 4. Auflage

Die Auflagen dieses Buches spiegeln den Kreislauf einer ständigen Anpassung an neue Gegebenheiten und einer kontinuierlichen Verbesserung wider. So hat sich seit der ersten Auflage im Jahr 2005 nicht nur die Risikolandschaft mit ihren Anforderungen, sondern, neben den gesetzlichen und regulativen Vorgaben, auch die Verfügbarkeit von Standards, Rahmen- und Regelwerken erheblich erweitert. Beispiele solcher Rahmen- und Regelwerke über Aspekte des Risikomanagements sind der ISO Standard 31000:2009 über Prinzipien und Richtlinien eines Risikomanagements, die zahlreichen ISO/IEC-Standards der 2700x-Reihe über Informationssicherheit, der internationale Standard ISO 22301:2012 über Geschäftskontinuität sowie die deutschen BSI-Standards 100-x oder die österreichischen Standards der Reihe ONR 4900x in diesen Themen. Erwähnenswert sind auch die neuerlichen Bemühungen zur Vereinheitlichung der ISO-Standards über Management-Systeme auf der Basis des neuen „ISO Guide 83“.

Auch verwundert nicht, dass die Informationssicherheits-Risiken, beispielsweise bei der Verwendung von „Cloud-Computing“ sowie bei der steigenden Ernsthaftigkeit von „Cyber-Threats“, aber auch bei neuen gesetzgeberischen und regulatorischen Anforderungen in den letzten Jahren eine neue Relevanz erhalten haben. Die derzeit laufenden Standardisierungen, an denen ich in den relevanten Normen-Komitees der Schweizerischen Normenvereinigung mitarbeite, tragen solchen aktuellen Aspekten Rechnung. Doch ist es, trotz der starken Anlehnung an solche Standards, nicht Zweck dieses Buches, diese Standards zu interpretieren oder gar zu ersetzen. Vielmehr sollen für den Leser die wesentlichen praktischen Aspekte eines Risikomanagements aus der Sicht des Unternehmens sowie der IT und der Informationssicherheit herausgearbeitet werden. Somit ist das Buch Alternative und Ergänzung zu den heute vielfältig vorhandenen und in den Literaturhinweisen erwähnten Standardisierungs-Dokumenten. Selbstverständlich wird in dieser neuen Buchaufgabe die in den neueren Standards verwendete Terminologie des Risikomanagements, vor allem die des „ISO Guide 73:2009“ angewandt.

Wie im erweiterten Titel des Buches erkennbar ist, beschränkt sich das Buch weder alleine auf die Risiken der Informationssi-

cherheit* noch alleine auf die Risiken der Informationstechnologie, sondern soll im Rahmen eines Unternehmens-Risikomanagements für beide Risiko-Felder Gültigkeit haben.

Somit verfolgt das Buch das Ziel, den derzeitigen Stand des Informationssicherheits-Risikomanagements und des IT-Risikomanagements in einer für den Anwender in der Praxis notwendigen Übersicht und Ausführlichkeit zu behandeln. Um dabei den Fokus eines „Leitfadens“ nicht zu verlieren, wurden beispielsweise aufwändige quantitative Assessment-Methoden, welche hohe Anforderungen an das statistische Datenmaterial und an ihre praktische Umsetzung stellen, mit entsprechenden Hinweisen weniger umfassend und tief behandelt. Stattdessen wurden, insbesondere in den beiden ersten Buchteilen, die Möglichkeiten des Risiko-Assessments und der Risiko-Behandlung, wie sie für operationelle Risiken auf der Ebene des Gesamtunternehmens allenfalls in Betracht kommen, in den wesentlichen Grundzügen vorgestellt. Wie aktuelle Beispiele zeigen, können die Informationssicherheits-Risiken und IT-Risiken große Risiken für Unternehmen bedeuten. Man denke beispielsweise an den Ausfall wichtiger Produktionssysteme oder den Diebstahl geheimer Unternehmensdaten mittels Attacken über das Internet. Demzufolge bezweckt der Aufbau dieses Buches die Integration des Informationssicherheits-Managements und des IT-Risikomanagements in ein in das Führungssystem des Unternehmens integriertes Gesamt-Risikomanagement. So erweist sich die Strukturierung in die folgenden vier Buchteile als nützlich:

Teil A: Grundlagen erarbeiten

Teil B: Anforderungen aus Unternehmenssicht berücksichtigen

Teil C: Informations-Risiken erkennen und bewältigen

Teil D: Unternehmensprozesse meistern

Damit erklärt sich auch, dass in den ersten beiden Buchteilen die Grundlagen und die Anforderungen in einer für das Unternehmen allgemeinen Weise behandelt werden. Hingegen werden die für die IT- und Informations-Risiken spezifischen Inhalte im dritten Teil des Buches und die Umsetzung und die Integration des Informationssicherheits- und IT-Risikomanagements in die Unternehmensprozesse im vierten und letzten Teil des Buches behandelt.

* Sicherheit der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen

Am Ende eines jeden Kapitels finden sich eine Zusammenfassung sowie einige Kontrollfragen und Aufgaben. Die Musterlösungen für die Kontrollfragen und Aufgaben können über den Online-Service im Internet abgerufen werden. Die URL dafür ist:

<http://www.koenigs-media.ch/viewegbuch/>

Fragen, fachliche Hinweise oder gar einen über den Online-Service möglichen Dialog sind mir herzlich willkommen.

Dank

Wie die neuen Auflagen des Buches unterliegen auch die Ausbildungsgänge zum „Bachelor of Information Security“ und zum „Master of applied Studies in Information Security“ an der Hochschule Luzern, wo ich neben meiner Beratertätigkeit als Dozierender für Risikomanagement tätig bin, einem kontinuierlichen Verbesserungsprozess. Für die aus dieser Tätigkeit erhaltenen wertvollen Anregungen meiner Studierenden und Dozenten-Kollegen möchte ich mich an dieser Stelle herzlich bedanken.

Für die vielen Diskussionen und wertvollen Ratschläge zu den Erweiterungen in der vierten Auflage danke ich meinem langjährigen Berufskollegen Domenico Salvati und meinem Beraterkollegen Daniel Farner der Firma CSI Consulting AG für die stete Bereitschaft, einzelne Themen und deren Praxistauglichkeit zu diskutieren. Mein Dank gilt auch dem Lektorat des Springer Vieweg-Verlags für seine Unterstützung und seine wertvollen Hinweise.

Mein besonderer Dank geht an meine Tochter Nicole Königs Balfry für das sorgfältige Korrekturlesen sowie an meine Frau Diemuth Königs, Autorin historischer Bücher, die mir in allen Belangen mit Rat und Tat zur Seite steht.

Olsberg im September 2012

Hans-Peter Königs

Inhaltsverzeichnis

1	Einführung	1
1.1	Warum beschäftigen wir uns mit Risiken?	1
1.2	Risiken bei unternehmerischen Tätigkeiten	3
1.3	Inhalt und Aufbau dieses Buchs	3
	Teil A: Grundlagen erarbeiten	5
2	Elemente für die Durchführung eines Risikomanagements	7
2.1	Fokus und Kontext Risikomanagement	9
2.2	Definition des Begriffs „Risiko“	9
2.3	Risiko kombiniert aus Wahrscheinlichkeit und Konsequenz	13
2.4	Probleme bei Risikobestimmung mittels einfacher Multiplikation	17
2.5	Subjektivität bei Einschätzung und Bewertung der Risiken	18
2.6	Hilfsmittel zur Analyse, Aufbereitung und Darstellung der Risiken	19
2.6.1	Risiko-Bewertungs-Matrix	19
2.6.2	Kriterien zur Schadenseinstufung	21
2.6.3	Risiko-Landkarte, Akzeptanz-Kriterien und Risiko-Portfolio	24
2.6.4	Risiko-Katalog	25
2.7	Risiko-Aggregation und Abhängigkeiten	27
2.8	Beschreibung der Risiken mit Risikomasszahlen	29
2.8.1	Stochastische Methoden zur Bestimmung des Risikos	31
2.8.2	Risiko-Analyse und -Überwachung mit Indikatoren	35
2.9	Risiko-Organisation, Kategorien und Arten von Risiken	36
2.9.1	Bedrohungslisten	39
2.9.2	Beispiele von Risiko-Arten	39
2.10	Zusammenfassung	41
2.11	Kontrollfragen und Aufgaben	42
3	Risikomanagement als Prozess	43
3.1	Kommunikation und Konsultation	45
3.2	Festlegung Risikomanagement-Kontext	46

3.3	Durchführung Risiko-Assessment	47
3.4	Risiko-Identifikation	48
3.5	Risiko-Analyse	50
3.5.1	Teil-Analysen	51
3.5.2	Bedrohungs-Analyse	51
3.5.3	Schwächen-Analyse	52
3.5.4	Impact-Analyse	54
3.6	Risiko-Bewertung	55
3.7	Risiko-Assessment Methoden	57
3.7.1	Such-Methoden	59
3.7.2	Szenarien-Analyse	60
3.8	Risiko-Behandlung	61
3.9	Akzeptanz- und Iterationsentscheide	64
3.10	Überwachung und Überprüfung	65
3.11	Universeller Risikomanagement-Prozess	66
3.12	Zusammenfassung	67
3.13	Kontrollfragen und Aufgaben	69
Teil B: Anforderungen aus Unternehmenssicht berücksichtigen		71
4	Risikomanagement, ein Pflichtfach der Unternehmensführung	73
4.1	Risikomanagement integriert in das Führungssystem	73
4.2	Corporate Governance	76
4.3	Anforderungen von Gesetzgebern und Regulatoren	78
4.3.1	Gesetz KonTraG in Deutschland	78
4.3.2	Obligationenrecht in der Schweiz	79
4.3.3	Swiss Code of best Practice for Corporate Governance	82
4.3.4	Rahmenwerke Basel II und Basel III	83
4.3.5	Sarbanes-Oxley Act (SOX) der USA	90
4.3.6	EuroSOX	94
4.3.7	Datenschutz: Eine wichtige Unternehmensanforderung	95
4.4	Risikomanagement: Anliegen der Kunden und Öffentlichkeit	99
4.5	Hauptakteure im unternehmensweiten Risikomanagement	100
4.6	Zusammenfassung	103
4.7	Kontrollfragen und Aufgaben	105
5	Risikomanagement integriert in das Management-System	107
5.1	Integrierter unternehmensweiter Risikomanagement-Prozess	108
5.2	Normatives Management	110

5.2.1	Unternehmens-Politik.....	111
5.2.2	Unternehmens-Verfassung.....	111
5.2.3	Unternehmens-Kultur.....	112
5.2.4	Mission und Strategische Ziele.....	112
5.2.5	Vision als Input des Strategischen Managements	113
5.3	Strategisches Management.....	113
5.3.1	Strategische Ziele.....	115
5.3.2	Strategien	119
5.4	Strategie-Umsetzung	119
5.4.1	Strategie-Umsetzung mittels Balanced Scorecards (BSC)	119
5.4.2	Unternehmensübergreifende BSC	124
5.4.3	Balanced Scorecard und CobiT für die IT-Strategie.....	124
5.4.4	IT-Indikatoren in der Balanced Scorecard.....	126
5.4.5	Operatives Management (Gewinn-Management)	130
5.4.6	Policies und Pläne.....	130
5.4.7	Risikopolitische Grundsätze	132
5.5	Umsetzung von Anforderungen mit Management-Systemen.....	133
5.5.1	Management-Systeme.....	134
5.5.2	Vereinheitlichung Management-System-Standards durch ISO	136
5.6	Zusammenfassung.....	137
5.7	Kontrollfragen und Aufgaben	139
Teil C: Informations-Risiken erkennen und bewältigen.....		141
6	Informationssicherheits- und IT-Risiken	143
6.1	Veranschaulichung der Risikozusammenhänge am Modell.....	143
6.2	Informationen – die risikoträchtigen Güter.....	146
6.3	System-Ziele für Risiken Informationssicherheit und IT	148
6.4	Informationssicherheit versus IT-Sicherheit	150
6.5	Informationssicherheits-Risiken versus IT-Risiken.....	151
6.6	Grundschutz und Informationssicherheits-Risikomanagement.....	152
6.7	Zusammenfassung.....	153
6.8	Kontrollfragen und Aufgaben	154
7	Informationssicherheits- und IT-Governance	155
7.1	Management von Informations- und IT-Sicherheit.....	155
7.1.2	IT-Governance versus Informationssicherheits-Governance.....	156
7.1.3	IT-Governance nach ITGI der ISACA	158
7.1.4	Informationssicherheits-Governance nach ITGI der ISACA	160
7.2	Organisatorische Funktionen für Informations-Risiken.....	164

7.2.1	Chief Information Officer (CIO).....	165
7.2.2	Chief (Information) Security Officer	165
7.2.3	Business-Owner, IT-Owner und IT-Administratoren.....	167
7.2.4	Information Security Steering Committee	168
7.2.5	Checks and Balances durch Organisations-Struktur	168
7.3	Zusammenfassung.....	171
7.4	Kontrollfragen und Aufgaben	172
8	Informationssicherheits-Risikomanagement in der Führungs-Pyramide.....	173
8.1	Ebenen der Führungspyramide.....	174
8.1.1	Risiko- und Sicherheits-Politik auf der Unternehmens-Ebene	174
8.1.2	Informationssicherheits-Politik und ISMS-Politik	175
8.1.3	Weisungen und Ausführungsbestimmungen.....	177
8.1.4	Informationssicherheits-Architektur und -Standards	179
8.1.5	IT-Sicherheitskonzepte.....	183
8.2	Zusammenfassung.....	184
8.3	Kontrollfragen und Aufgaben	186
9	Informations-Risikomanagement mit Standard-Regelwerken	187
9.1	Bedeutung der Standard-Regelwerke	187
9.2	Übersicht über wichtige Regelwerke.....	189
9.3	Risikomanagement mit der Standard-Reihe ISO/IEC 2700x.....	195
9.3.1	Informationssicherheits-Management nach ISO/IEC 27001.....	197
9.3.2	Code of Practice ISO/IEC 27002.....	205
9.3.3	Informationssicherheits-Risikomanagement mit ISO/IEC 27005	209
9.4	CobiT Framework	212
9.4.1	CobiT 4.1.....	213
9.4.2	IT-Risikomanagement mit CobiT 4.1.....	219
9.5	BSI-Standards und Grundschutzkataloge	221
9.6	Zusammenfassung.....	224
9.7	Kontrollfragen und Aufgaben	225
10	Methoden und Werkzeuge zum IT-Risikomanagement	227
10.1	IT-Risikomanagement mit Sicherheitskonzepten.....	227
10.1.1	Kapitel „Kontextbeschreibung“	231
10.1.2	Kapitel „Risiko-Assessment“.....	235
10.1.3	Kapitel „Risiko-Analyse“.....	238
10.1.4	Schwachstellen-Analyse anstelle einer Risiko-Analyse	240
10.1.5	Kapitel „Bewertung und Anforderungen an Massnahmen“	242

10.1.6	Kapitel „Definition und Beschreibung Massnahmen“	245
10.1.7	Kapitel „Umsetzung Massnahmen“	246
10.1.8	Kommunikation und kooperative Ausarbeitung der Kapitel	249
10.1.9	Risiko-Akzeptanz, Konzept-Abnahme und -Anpassung	249
10.1.10	Überwachung und Überprüfung	250
10.2	Die CRAMM-Methode	250
10.3	Fehlermöglichkeits- und Einfluss-Analyse	257
10.4	Fehlerbaum-Analyse	259
10.5	Ereignisbaum-Analyse	264
10.6	Zusammenfassung	265
10.7	Kontrollfragen und Aufgaben	268
11	Kosten/Nutzen - Relationen der Risikobehandlung	273
11.1	Formel für “Return on Security Investments” (ROSI)	275
11.2	Ermittlung der Kosten für die Sicherheitsmassnahmen	277
11.3	Ermittlung der Kosten der behandelten Risiken	280
11.4	Massnahmen-Nutzen ausgerichtet an Unternehmenszielen	281
11.4.1	Grundzüge von Val IT	283
11.4.2	Grundzüge von Risk IT	285
11.5	Fazit zu Ansätzen der Sicherheit-Nutzen-Bestimmung	288
11.6	Zusammenfassung	288
11.7	Kontrollfragen und Aufgaben	291
Teil D: Unternehmens-Prozesse meistern	293	
12	Risikomanagement-Prozesse im Unternehmen	295
12.1	Verzahnung der RM-Prozesse im Unternehmen	296
12.1.1	Risiko-Konsolidierung	297
12.1.2	Subsidiäre RM-Prozesse	298
12.1.3	Informations-RM und Rollenkonzepte im Gesamt-RM	300
12.2	Risikomanagement im Strategie-Prozess	302
12.2.1	Risikomanagement und IT-Strategie im Strategie-Prozess	303
12.2.2	Periodisches Risiko-Reporting	306
12.3	Zusammenfassung	306
12.4	Kontrollfragen und Aufgaben	307
13	Geschäftskontinuitäts-Management und IT-Notfall-Planung	309
13.1	Einzelpläne zur Unterstützung der Geschäftskontinuität	310
13.1.1	Geschäftskontinuitäts-Plan (Business Continuity Plan)	311

13.1.2	Betriebskontinuitäts-Plan (Continuity of Operations Plan)	313
13.1.3	Ausweichplan (Disaster Recovery Plan)	313
13.1.4	IT-Notfall-Plan (IT Contingency Plan)	314
13.1.5	Vulnerability- und Incident Response-Plan	314
13.2	BCMS im Unternehmens-Risikomanagement	315
13.3	Planung Kontinuitäts-System	318
13.3.1	Kontext des Unternehmens	318
13.3.2	Führung	319
13.3.3	Planung	321
13.3.4	Unterstützung	322
13.4	Operation	325
13.5	Geschäfts-Impact-Analyse und Risiko-Assessment	326
13.5.1	Geschäfts-Impact-Analyse	326
13.5.2	Risk-Assessment	330
13.6	Geschäftskontinuität-Strategien	331
13.7	Geschäftskontinuitäts-Verfahren und Pläne	334
13.7.1	Krisenmanagement	334
13.7.2	Kriterien für Plan-Aktivierungen	338
13.7.3	Ressourcen und externe Abhängigkeiten	339
13.7.4	Plan-Zusammenstellung	340
13.7.5	Kommunikationskonzept für Ereignisfall	341
13.8	Tests, Übungen und Plan-Unterhalt	342
13.8.1	Tests	343
13.8.2	Übungsvorbereitungen und -Durchführungen	343
13.8.3	Wartung und Überprüfung der Pläne	344
13.9	Leistungsbewertung	345
13.9.1	Überwachung und Überprüfung	345
13.9.2	Internes und externes Audit	346
13.9.3	Überprüfung durch Management	347
13.10	Kontinuierliche Verbesserungen und Wiederholungen	349
13.11	IT-Notfall-Plan, Vulnerability- und Incident-Management	349
13.11.1	Organisation eines Vulnerability- und Incident-Managements	352
13.11.2	Behandlung von plötzlichen Ereignissen als RM-Prozess	355
13.12	Zusammenfassung	356
13.13	Kontrollfragen und Aufgaben	358
14	Risikomanagement im Lifecycle von Informationen und Systemen	359
14.1	Schutz von Informationen im Lifecycle	359
14.1.1	Einstufung der Informations-Risiken	359

14.1.2	Massnahmen für die einzelnen Schutzphasen	360
14.2	Risikomanagement im Lifecycle von IT-Systemen.....	361
14.3	Synchronisation RM mit System-Lifecycle	363
14.4	Zusammenfassung.....	365
14.5	Kontrollfragen und Aufgaben	366
15	Risikomanagement in Outsourcing-Prozessen.....	369
15.1	IT-Risikomanagement im Outsourcing-Vertrag.....	370
15.1.1	Sicherheitskonzept im Sourcing-Lifecycle.....	372
15.1.2	Sicherheitskonzept beim Dienstleister.....	375
15.2	Zusammenfassung.....	377
15.3	Kontrollfragen	378
16	Risikomanagement bei Nutzung und Angebot Cloud-Computing	379
16.1	Prinzip und Definitionen Cloud-Computing	379
16.1.1	Wesentliche Charakteristiken	382
16.1.2	Service-Modelle	382
16.1.3	Deployment-Modelle.....	383
16.2	Informationssicherheitsrisiken beim Cloud-Computing	384
16.3	Cloud-Sourcing als Service aus der Kundenperspektive.....	384
16.3.1	Phase 1: Cloud-Sourcing-Strategie.....	388
16.3.2	Phase 2: Evaluation und Auswahl.....	389
16.3.3	Phase 3: Vertragsentwicklung.....	391
16.3.4	Phase 4: Cloud-Sourcing-Management	392
16.4	Risikomanagement für Cloud-Computing aus Kundensicht	393
16.4.1	Kontext im Sicherheitskonzept für Cloud-Computing-Einsatz	394
16.4.2	Risiko-Assessment	396
16.5	Cloud-Sourcing-Lifecycle auf der Provider-Seite.....	403
16.6	Zusammenfassung.....	404
16.7	Kontrollfragen und Aufgaben	407
Anhang.....		409
A.1	Beispiele von Risiko-Arten.....	411
A.2	Beispiele von „Cyber Threats“	415
A.3	Muster Ausführungsbestimmung für Informationsschutz	417
A.4	Formulare zur Einschätzung von IT-Risiken.....	421
A.5	Beispiele zur Aggregation von operationellen Risiken	425

Literatur	429
Abkürzungsverzeichnis.....	436
Stichwortverzeichnis	438

„Erstens kommt es anders und zweitens als man denkt“. Dieses von Wilhelm Busch geprägte Prinzip wird im vorliegenden Buch nicht widerlegt. Doch warum beschäftigen wir uns denn überhaupt mit Risiken? Diese Frage und wie wir uns mit den Risiken im Allgemeinen und mit den Informationssicherheits- und den IT-Risiken im Unternehmen im Besonderen auseinandersetzen können, sollte spätestens nach dem Lesen dieses Buches beantwortet werden können.

1.1**Warum beschäftigen wir uns mit Risiken?**

Unsere tagtäglichen Erfahrungen zeigen an einfachen Beispielen, dass wir mit geeigneten Vorkehrungen und Massnahmen das Auftreten von negativen Ereignissen oder auch die Konsequenzen solcher Ereignisse vermindern können. Wem es je passiert ist, dass kurz vor der Fertigstellung einer umfangreichen Schreiarbeit am PC die Informationen unwiederbringlich gelöscht waren, wird die Nützlichkeit einer regelmässigen Informationensicherung auf ein anderes Speicher-Medium kaum in Frage stellen.

*Häufigkeiten
reduzieren oder
negative Konse-
quenzen mildern*

Negative Ereignisse (z.B. Unfälle) können mit noch so weiser Voraussicht und entsprechenden Massnahmen nie gänzlich vermieden werden. Doch können mit entsprechenden Vorkehrungen entweder die Häufigkeiten solcher Ereignisse reduziert oder ihre negativen Konsequenzen gemildert werden.

Das am 11. März 2011 stattgefundene Erdbeben in Japan und die nachfolgende Tsunami- und Atomreaktor-Katastrophe haben uns in eklatanter Weise vor Augen geführt, wie den Verhältnissen angemessene vorsorgliche Massnahmen den Tsunami zwar nicht hätten verhindern, aber die Auswirkungen – vor allem die nachfolgende Reaktorkatastrophe – wesentlich hätten reduzieren können. So kam auch der am 5. Juli 2012 veröffentlichten Bericht einer eingesetzten parlamentarischen Untersuchungskommission zum Schluss, dass die „von Menschen verursachte Katastrophe“ der Kernschmelze „vermeidbar“ gewesen wäre.

Auch denken wir sofort an mögliche Unterlassungen, wenn wir, wie am 15. Januar 2009, lesen: „Die elektronischen Fahrpläne und das Buchungssystem der Deutschen Bahn waren in ganz Deutschland stundenlang ausgefallen. Der Computerausfall hatte am Mittwoch bundesweit zu Verspätungen im Bahnverkehr geführt.“

Ähnliches, aber in umgekehrter Richtung, gilt für die positiven Ereignisse, die wir selbstverständlich herbeiwünschen und für die wir uns einen möglichst positiven Effekt erhoffen. Solche ungewissen wünschbaren positiven Ereignisse bezeichnen wir als Chancen.

Für solche Ereignisse ergreifen wir Massnahmen, um den positiven Effekt mit grösstmöglicher Wahrscheinlichkeit oder mit möglichst günstigen Ergebnissen herbeizuführen. So soll beispielsweise die Fernsehwerbung für ein Kosmetikprodukt dafür sorgen, dass das Produkt möglichst häufig gekauft wird. Oder ein Softwareprodukt wird so angeboten, dass es zum einen möglichst häufig gekauft wird und zum anderen einen möglichst hohen Preis erzielt.

Risiken und Chancen

Sowohl für die Risiken als auch die Chancen gibt es Massnahmen, die das gewünschte Resultat besser oder schlechter herbeiführen können. Ein zentraler Aspekt des Umgangs mit Risiken und Chancen ist, unter den massgeblichen Bedingungen, die optimal geeigneten Massnahmen herauszufinden und zu realisieren.

Die eben skizzierte Beschäftigung mit Risiken ist grob vereinfacht das, was wir unter „Risikomanagement“ verstehen. Um mit allen und zum Teil hoch abstrakten Aspekten zu den gewünschten optimalen Ergebnissen zu kommen, braucht es ein grosses Mass an Systematik. Gerade wenn es um hohe Risiken und hohe Massnahmenkosten geht, die den Unternehmen durch die Informations-Technologie entstehen, ist es wichtig, diese ganzheitlich, systematisch und transparent zu behandeln.

„Risikomanagement“ mit systemischen Modellen

Die dafür in diesem Buch verwendeten Modelle sind als „systemische“ Modelle zu verstehen. Dabei kann eine Risiko-Ursache verschiedene Auswirkungen und eine Auswirkung verschiedene Ursachen haben. Um die meist „komplexe“ Wirklichkeit möglichst gut zu modellieren, enthalten daher die Problemlösungsprozesse des Risikomanagements entsprechende Rückkopplungen und Iterationen ([Ulri91], S. 114). Mit diesem „systemischen“ Ansatz findet auch der Titel dieses Buches „IT-Risikomanagement mit System“ seine Erklärung.

1.2

Risiken bei unternehmerischen Tätigkeiten

Risiken und Chancen sind in jedem Unternehmen – wenn auch nicht immer offensichtlich – vorhanden. Es gilt der Grundsatz, dass mit dem Ergreifen von Chancen auch immer Risiken eingegangen werden müssen. Dabei ist es eine normale menschliche Eigenschaft, die Risiken aus dem Bewusstsein zu verdrängen. Dennoch ist der sorgfältige Umgang mit Risiken, gleichermassen wie das Wahrnehmen von Chancen, eine der wichtigsten unternehmerischen Verantwortlichkeiten und muss in der Unternehmens-Politik, in der Unternehmens-Strategie sowie in allen unternehmerischen Handlungen gepflegt werden. Ist es doch das Wohl des Unternehmens und gar sein Überleben, das vom richtigen Umgang mit den Risiken abhängig ist.

Leidtragende

Die Leidtragenden der Risiken sind auch nicht alleine die Eigentümer des Unternehmens, sondern alle an einem Unternehmen beteiligten Kreise, die sog. Anspruchsgruppen (Stakeholders), wie Beschäftigte, Kapitalgeber, Verbände, Partner, Lieferanten, Behörden, Kommunen und der Staat. So haben die in den letzten Jahren aufgetretenen Schadensereignisse bewirkt, dass das Risikomanagement in den meisten Industriestaaten zu einer vom Gesetzgeber verordneten „Muss-Disziplin“ der Unternehmensführung geworden ist.

1.3

Inhalt und Aufbau dieses Buchs

Die unterschiedlichen Risiken in einem Unternehmen sind in ihrer Art und Entstehung stark voneinander abhängig und tragen letztendlich zum Erfolg oder Misserfolg eines Unternehmens in entscheidendem Masse bei. Deshalb muss die Steuerung und Überwachung der Risiken bereits auf der obersten Ebene der Unternehmensführung erfolgen. Das Buch behandelt zwar speziell die Informationssicherheits- und IT-Risiken, dennoch müssen die Bedrohungen, Massnahmen und Prozesse zum Management dieser Risiken in einem ganzheitlichen Zusammenhang zur Unternehmenssicht und dessen Zielen, Anforderungen und Management-Prozessen gesehen werden. Demzufolge wird vor der detaillierten Behandlung der Informationssicherheits- und IT-Risiken im Teil C des Buches der dazu notwendige Vorspann in den Teilen A und B behandelt.

Teil A: Grundlagen erarbeiten

Somit werden in **Teil A** des Buches die für ein ganzheitliches Risikomanagement in einem Unternehmen allgemeinen Grundlagen und Instrumente aufgezeigt.

*Teil B:
Anforderungen
aus Unterneh-
menssicht
berücksichtigen*

Im Teil B werden die an das Unternehmen gestellten heute aktuellen Anforderungen an ein Risikomanagement und die Voraussetzungen und Prozesse für die in die Management-Prozesse des Unternehmens integrierten Risiko-Aspekte beleuchtet. Die dazu zusammengestellten Konzepte, Methoden und Instrumente haben zum Ziel, ein möglichst effektives Risikomanagement mit vertretbarem Aufwand aufzubauen und zu betreiben.

*Teil C:
Informations-
Risiken erkennen
und bewältigen*

Im Teil C werden die Risiken der Informationen und der Informationstechnologie detailliert behandelt und entsprechende Methoden und Verfahren speziell zum Management der Informationssicherheit- und IT-Risiken beschrieben. Der gebräuchliche aber unscharfe Begriff der „Informations-Risiken“ schliesst dabei die Informationssicherheits-Risiken wie die Risiken im Zusammenhang mit der Leistungserbringung der Informatik ein.

*Teil D:
Unternehmens-
prozesse meistern*

Im Teil D wird sodann gezeigt, wie sich die verschiedenen Risiken, darunter die operationellen Risiken der Informationssicherheit und der Informations-Technologie, in einen gesamten Risikomanagement-Prozess des Unternehmens einfügen lassen und wie unternehmenswichtige Risikomanagement-Prozesse wie die Geschäftskontinuitäts-Planung im Risikomanagement-Prozess verankert werden können.

Teil A

Grundlagen erarbeiten

2

Elemente für die Durchführung eines Risikomanagements

*Akzeptable
Restrisiken*

*Risikomanage-
ment*

Die Beschäftigung mit den Risiken dient vor allem ihrer Erkennung und Bewertung sowie der Erarbeitung von Massnahmen und deren Umsetzung. Durch die Massnahmen sollen die Risiken auf akzeptable „Restrisiken“ reduziert werden.

Auf der Basis von Art, Quantität und Qualität der Risiken sowie einiger weiterer Kriterien sollen möglichst optimale Massnahmen-Lösungen gefunden und umgesetzt werden, aber auch akzeptable Restrisiken toleriert und ohne weitere Behandlung bewusst getragen werden können. Die koordinierten Aktivitäten zur Steuerung von Risiken im Unternehmen werden als „Risikomanagement“ bezeichnet. Die in Abbildung 2.1 gezeigten hauptsächlichen Aktivitäten eines Risikomanagements werden vorteilhaft in einer prozessorientierten Weise durchgeführt.

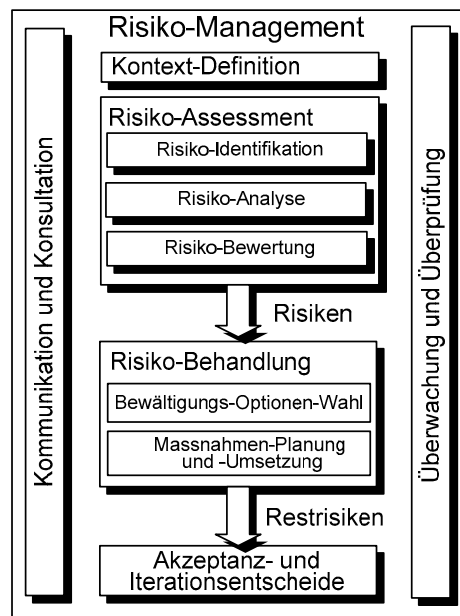


Abbildung 2.1: Aktivitäten für das Risikomanagement

Das „Risikomanagement“, wie es in diesem Buch sowohl generell aus Unternehmenssicht als auch spezifisch für die Gebiete der Informationssicherheit und der Informationstechnologie behandelt wird, ist eine wichtige Teil-Disziplin der Unternehmensführung.

*Interdisziplinäre
Vernetzung Risiko-
management*

Eine solche Anwendung des Risikomanagements hat zudem einen hohen interdisziplinären Stellenwert, können doch beispielsweise die „Informationssicherheits-Risiken“ grosse andere Risiken in der Volkswirtschaft, im Gesundheitswesen, im Kommunikations-, Energie-, Verkehrs- und Transportwesen sowie ganz allgemein in der Gesellschaft nach sich ziehen. Beispiele: Datendiebstahl bei Sony von Namen, Passwörtern und Kreditkartennummern, undurchschaubare Funktionen bei sozialen Netzwerken, Cyber-Attacken mit Trojanern, mit denen Kriminelle die Computer von Privatpersonen und Unternehmen zu Betrugszwecken ausspionieren bis hin zu Staats- und Wirtschaftsspionage und dem heute zur Realität gewordenen „Cyber-Krieg“.

*Terminologie und
Standards*

Die im Zusammenhang mit „Risikomanagement“ in den einzelnen Disziplinen verwendete Terminologie ist vielfältig und teilweise noch uneinheitlich. Auf diesem Hintergrund sind die Standardisierungen einer Terminologie im ISO Guide 73 [Isog09] sowie die Standards ISO 31000:2009 [Isor09] und ISO/IEC 27005:2011 [Isoi11] oder des US-amerikanischen „Committee of Sponsoring Organizations of the Treadway Commission“ [Cose04] als sehr begrüßenswert anzusehen. Doch weisen solche Standards, trotz der Harmonisierungsbestrebungen durch die ISO, im näheren Detail immer noch Unterschiede auf, die wahrscheinlich, aufgrund der spezifischen Anforderungen für einen bestimmten Kontext und der nationalen Präferenzen bei den Abstimmungen, nie vollständig harmonisiert werden können. Die Standards über Risikomanagement haben somit meist lediglich Empfehlungscharakter. Dieses Buch orientiert sich bezüglich Risikomanagement, wo immer angezeigt, an der im ISO Guide 73:2009 festgelegten Terminologie und den darauf abgestimmten „generischen“ Grundsätzen und Richtlinien des Standards ISO 31000:2009. Doch in einigen wichtigen Details finden auch Ergänzungen aus der Praxis des Autors sowie anderen Standards wie der Österreichischen Standardreihe ONR 49000:2008 ff (vgl. [Onri08]) oder des Standards ISO/IEC 27005:2011 über ein „Information Security Risk Management“ Verwendung.

2.1

Fokus und Kontext Risikomanagement

Fokussierung auf Betroffene

Die aus dem Risikomanagement resultierenden Massnahmen bezwecken, die Gefahrensituationen oder die Folgen von Schadensereignissen für die „Betroffenen“ zu beseitigen oder zu vermindern.

Je nachdem wie die Aufgabenstellung für das durchzuführende Risikomanagement lautet, können die Betroffenen, Einzelpersonen, Gruppen von Personen oder auch, wie in diesem Buch, Unternehmen sein. Die Risiken, die wir im Rahmen dieses Buches betrachten, fallen bei einzelnen Produkten oder Dienstleistungen, bei einzelnen Organisationseinheiten oder auf der Ebene des Gesamtunternehmens an.

Neben der Fokussierung auf die Betroffenen ist die Bezeichnung und Abgrenzung der Gegenstände* für die möglichen Schadensereignisse nötig. Auch das Umfeld der betrachteten Gegenstände bedarf der Definition und Abgrenzung. Diese Definitionen und Abgrenzungen sind aus den Blickwinkeln der Gefahrensituationen, der an der Risikobeurteilung und Behandlung beteiligten Stellen sowie der massgeblichen funktionalen Zusammenhängen notwendig.

Massgeblicher Kontext

Bereits zu Beginn einer Risikomanagement-Aufgabe ist die Fokussierung und die Bestimmung des massgeblichen Kontextes unabdingbare Voraussetzung. Mehr über die Inhalte des „Kontexts“ sowie die Aktivitäten bei den einzelnen Management-Aktivitäten sind im Kapitel 3 dargelegt.

2.2

Definition des Begriffs „Risiko“

Im Hinblick auf eine möglichst breite Anwendung lautet die ISO-Definition ISO/IEC Guide 73:2009 [IsoV09]:

Risiko ist die Auswirkung von Unsicherheit auf Ziele.

Diese grobe Definition, schliesst zwar objektive und subjektive Betrachtungen mit ein, ist aber in der Praxis nicht allzu hilfreich.

* Der Begriff „Gegenstand“ wird in diesem Buch synonym zu „Objekt“ sowohl für greifbare als auch für abstrakte Güter, Objekte und Strukturen verwendet und schliesst den in der englischsprachigen Standardisierung oft verwendeten Begriff „Asset“ ein.

In der Praxis sind deshalb je nach Anwendungsgebiet aussagekräftigere Definitionen anzutreffen*.

So werden für betriebswirtschaftliche Fragestellungen, wie sie in diesem Buch vorkommen, Verluste oder Schäden als die negativen Folgen von „**Zielabweichungen**“ eines vorgängig definierten Ziels verstanden. Mit den ursächlichen Bedrohungen, welche Schäden mit einer gewissen Häufigkeit hervorrufen können, ergibt sich folgende für den Praxiseinsatz sinnvolle Risiko-Definition (vgl. [Brüh01]):

Risiko-Definition

Risiko ist eine nach Wahrscheinlichkeit (Häufigkeit) und Auswirkung bewertete Bedrohung eines zielorientierten Systems[†]. Das Risiko betrachtet dabei stets die negative, unerwünschte und ungeplante Abweichung von System-Zielen und deren Folgen.

Risiko / Chance

Dem Risiko steht meist eine Chance gegenüber, welche ein positives Ergebnis in Aussicht stellt. Bei den in diesem Buch betrachteten „Operationellen Risiken“ besteht jedoch meist keine unmittelbare Verknüpfung des Risikos mit einer Ertragsquelle. Daher lassen sich die Risiken und die dazugehörige Chancen solcher Risiken meist auch nicht mit dem gleichen Lösungsansatz behandeln, was das Abwägen der Risiken mit den Chancen entsprechend schwierig gestaltet.

Die obige Risiko-Definition lässt ein breites Anwendungsspektrum zu. So können die mit Unsicherheit behafteten Ziele in der Form elementarer Eigenschaften, aber auch in der Form komplexer qualitativer oder quantitativer Anforderungen formuliert werden. Von der Zieldefinition hängt es primär ab, was als Abweichung vom Ziel und deren Folgen (Konsequenzen) und damit als Risiko erklärt werden kann. So bestehen auch zur Ana-

* In einer der fünf Fussnoten zum Begriff Risiko bemerkt der ISO/IEC Guide 73:2009 [IsoV09] beispielsweise, dass Risiko oft als „Kombination von Likelihood eines Ereignisses und seiner Konsequenzen“ ausgedrückt wird.

† Unter System wird in diesem Zusammenhang ein allgemeines System verstanden, das beispielsweise ein ökonomisches, ein gesellschaftliches oder ein technisches System mit zielorientierten Werten sein kann. Systeme mit ihren Subsystemen interagieren untereinander und werden für eine Risikobetrachtung entsprechend definiert und abgegrenzt.

lyse und Bewertung der Abweichungen von Zielen vielzählige Möglichkeiten, z.B. in der Form technischer Risikoassagen, wie Mass über Anzahl und Ausmass von technischen Fehlern oder in der Form stochastischer Risikomassen in zeit- und geldwerter Skalierung oder gar in der Form von Indikatoren (s. Abschnitte 2.8 und 2.8.2).

*Folgen der Ziel-
Abweichungen*

Wird die obige Risiko-Definition beispielsweise auf Projektrisiken angewendet, dann sind hauptsächlich die Folgen der Ziel-Abweichungen bezüglich „Dauer“, „Budget“ und „Qualität“ zu betrachten. Wenden wir die oben angegebene Definition auf Informationen und IT-Gegenstände an, dann resultieren die Sicherheits-Risiken und deren Folgen aus Abweichungen von den elementaren System-Zielen, „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“. Benützen wir die obige Definition bezüglich der Einhaltung einer gesetzlichen Vorschrift, dann könnte die aus einer Abweichung (Nichteinhaltung) resultierende Konsequenz beispielsweise der Verlust einer Banklizenz mit den entsprechenden Vermögensverlusten bedeuten. Solche auf der Erfüllung komplexer Anforderungen beruhenden Risiken werden oft unter dem Begriff „Compliance-Risiken“ zusammengefasst.

*Unerwünschte
Zielabweichungen*

Die „unerwünschten Ziel-Abweichungen“ können eintreten, wenn entsprechende Bedrohungen vorhanden sind. So kann beispielsweise die Bedrohung „Krankheit Mitarbeiter“ eine negative Abweichung vom Ziel: „Fertigstellungs-Termin“ eines Projekts bewirken.

Bedrohungen

Eine Bedrohung wirkt sich umso häufiger und stärker aus, als geeignete Massnahmen fehlen. Eine geeignete Massnahme im gerade gegebenen Beispiel wäre, den krank gewordenen Mitarbeiter kurzfristig durch eine andere gleichermassen geeignete Person ersetzen zu können. Ist eine solche Massnahme nicht vorhanden, sprechen wir von einer Schwäche, Verletzlichkeit oder Schwachstelle des Systems.

*Schwäche /
Schwachstelle /
Verletzlichkeit*

*Wahrscheinlich-
keit von möglichen
Folgen*

Aus den Bedrohungen und den Schwächen des Systems ergibt sich die Wahrscheinlichkeit, mit der eine Abweichung vom gesetzten Ziel mit bestimmten negativen Folgen eintritt. Eine solche Abweichung kann plötzlich, aber auch schleichend oder intermittierend, d.h. mit einer gewissen Zeitabhängigkeit, eintreten. Als Beispiel einer zeitabhängig eintretenden Abweichung vom Ziel „Vertraulichkeit der Daten“, könnte ein über längere Zeit unentdeckt wiederholter Datendiebstahl genannt werden.

	Die Folgen (Konsequenzen)* der Abweichungen vom Ziel bezeichnen wir als Schaden (auch Tragweite oder Verlust).
<i>Folgen einer Ziel-Abweichung</i>	So kann die Abweichung von einem geplanten Projekttermin finanzielle Einbussen zur Folge haben und/oder das Ansehen der Firma auf dem Markt beeinträchtigen (Reputations-Schaden). Die Folgen einer Ziel-Abweichung, wie die Abweichung selbst, können entweder ein zeitunabhängiges oder ein mit der Zeit veränderliches Ausmass aufweisen. So bedürfen die Ereignisse mit zeitlich anwachsendem Ausmass, z.B. Brandschäden, auch einer der Schadensentwicklung entsprechenden Risikobewältigung.
<i>Keine Möglichkeiten von Zielabweichungen = „sicher“</i>	Bestehen hingegen keine Möglichkeiten von Ziel-Abweichungen, so resultiert definitionsgemäss auch kein Schaden, wir sind also „sicher“. Bei bestimmten Zielen (z.B. Fertigstellungstermin in einem Projekt) kann eine Zielabweichung durchaus auch positive Folgen aufweisen. In diesem Falle haben wir es definitionsgemäss mit einer Chance zu tun. Bei den Massnahmenentscheidungen zur Bewältigung eines Risikos sind die möglichen Chancen ebenfalls in geeigneter Weise zu berücksichtigen.†
<i>„System-Ziel“ / „Sicherheits-Ziel“</i>	Da wir die Vorgänge um ein Risiko systemisch betrachten (Ursachen, Auswirkungen etc.), verwenden wir für diese Art von Zielen den Begriff „System-Ziel“. In der Informationssicherheit wird statt System-Ziel oft auch der Begriff „Sicherheits-Ziel“ verwendet.
<i>Risiko-Ziel</i>	Ein System-Ziel bei der Risikobestimmung ist wiederum nicht zu verwechseln mit einem „Risiko-Ziel“, bei dem es um eine Vorgabe geht, eine bestimmte Risikohöhe nicht zu überschreiten. Risiko-Ziele werden oft auch in der Form von akzeptierbaren „Risiko-Toleranzen“ ausgedrückt.

* Die Auswirkung eines Ereignisses wird auch als „Impact“ bezeichnet. Die gesamthaften Konsequenzen können aus mehreren Impacts resultieren. Die negativen Konsequenzen eines Ereignisses bezeichnen wir in diesem Buch als Schaden oder Verlust.

† Die Analyse von Chancen sowie die Massnahmen zur deren Realisierung werden im Rahmen dieses Buches über Informationssicherheits- und IT-Risikomanagement nicht speziell behandelt.

Beispiel:

Es besteht das Ziel, das Produktionssystem „FabriStock“ am 1. November 2012 in Betrieb nehmen zu können. Das System-Ziel heisst somit „Einhaltung des Einführungstermins“. Hingegen könnte ein mögliches Risiko-Ziel heissen: Die Kostenfolge durch eine Terminabweichung, multipliziert mit der Wahrscheinlichkeit ihres Auftretens, darf nicht mehr als 20' 000 € betragen (=Risiko). Bei einem Risiko von 10' 000 € ist das Risiko-Ziel noch bestens eingehalten, wir befinden uns sozusagen noch im „grünen Bereich“. Das Beispiel zeigt, dass erst mit der Einführung eines „Risiko-Ziels“ die Nichteinhaltung eines System-Ziels relativiert werden kann. Wir sehen später, dass wir diese Relativierung mit der Aufgabe „Risiko-Bewertung“ (risk evaluation) durchführen.

2.3

Risiko kombiniert aus Wahrscheinlichkeit und Konsequenz

Die oben angeführten verbalen Definitionen des Risikos liefern noch keine „messbaren“ Ergebnisse. Messbare Ergebnisse sind aber für viele Massnahmen-Entscheide oder für die Vergleichbarkeit von Risiken untereinander und mit anderen Risiken wichtig.

Eine einfache Möglichkeit, das Risiko messbar auszudrücken, besteht gemäss der untenstehenden Formel in der Multiplikation von Wahrscheinlichkeit und Schadensausmass. Es gilt jedoch vorweg zu bemerken, wie im Abschnitt 2.4 noch näher erläutert, dass solche Berechnungen problematisch sind und nur unter bestimmten Bedingungen zielführend sein können.

$$R = p_E \times S_E$$

R: Risiko;

p_E : Wahrscheinlichkeit, dass ein Schadensereignis mit dem Schaden S_E eintritt;

S_E : Ausmass des Schadensereignisses (auch Tragweite oder Verlust).

Anstelle der „theoretischen Wahrscheinlichkeit“ p_E wird meist die empirisch bestimmbare „relative Häufigkeit“ H_E des Schadeneintritts eingesetzt.

Eine solche Formel zeigt zwar rudimentär, dass das Risiko grösser wird, wenn die Wahrscheinlichkeit (relative Häufigkeit) eines

Schadensereignisses oder dessen Schadensausmass zunimmt. Doch gilt es zu bedenken, dass in der Realität mehrere Schadensereignisse in unterschiedlichen Zeitabständen mit meist unterschiedlichen Schadenshöhen eintreten, wobei sowohl die „Schadenseintritte“ als auch die „Schadenshöhen“ statistisch verteilt eintreten und sich daraus eine kombinierte statistische Schadensverteilung* ergibt. Die obige Formel nimmt auch keineswegs darauf Bezug, welche Kombination von Wahrscheinlichkeit und Schaden einer statistischen Verteilung dem zu berechnenden Risiko zugrunde liegen soll.

Eine für viele betriebswirtschaftliche Entscheidungen zweckmässigere Variante ist es daher, den für eine bestimmte Zeitperiode, z.B. ein Jahr, zu „erwartenden“ Schaden aus der Multiplikation† der in dieser Zeitperiode zu „erwartenden“ Anzahl der Schadenseintritte mit der „erwarteten“ Schadenshöhe zu berechnen:

$$R_T = H_T \times S$$

R_T : In der Zeitperiode T „erwarteter“ Schaden;

H_T : In der Zeitperiode T erwartete Anzahl (Häufigkeit) der Schadenseintritte;

S : erwartete (durchschnittliche) Schadenshöhe der eintretenden Schadensereignisse.

Eine derartige Risiko-Darstellung beruht auf der Kumulation (Aggregation) mehrerer, statistisch verteilter Schadensereignisse und wird auch als „erwarteter Verlust“‡ bezeichnet. Ihre Anwendung macht mit gewissen Einschränkungen Sinn und wird beispielsweise bei der Berechnung eines „Return on Security Investments (ROSI)“ eingesetzt (s. Abschnitt 11.1). Aber auch diese Variante, bestehend aus einer einfachen Multiplikation einer mittleren, auf eine definierte Zeitperiode (z.B. ein Jahr),

* Die statistische Verteilung setzt sich aus einer statistischen Verteilung der Schadenseintritte und der Schadenshöhen zusammen.

† Die Multiplikation der Erwartungswerte (Mittelwerte) der beiden Wahrscheinlichkeits-Verteilungen setzt voraus, dass das Auftreten der Ereignisse und die Schadenshöhen stochastisch voneinander unabhängig sind.

bezogenen Häufigkeit mit einer mittleren Schadenshöhe gibt lediglich ein Mass für ein „mittleres“ Risiko* wieder. Inwiefern einzelne „unerwartete“ Schadensereignisse zu einem, den Mittelwert wesentlich übersteigenden, Schadensvolumen führen könnten, wird mit dieser Berechnung nicht in adäquater Weise berücksichtigt. Für die Erfassung dieser „unerwarteten“ Risikoereignisse müssen andere Risikomasse (z.B. dem Value-at-Risk, Expected Shortfall oder Extremwerttheorie) herangezogen werden (s. Abschnitte 2.8 und 2.8.1).

Eine praktische Anwendung obiger Risikoformel soll an folgendem Praxisbeispiel aus der IT veranschaulicht werden:

Beispiel:

Ein IT-Plattform-Provider berechnet den „erwarteten Verlust“ der an Kunden zu richtenden Malus-Zahlungen infolge von Ausfällen seiner Server-Plattformen. Zu dieser Berechnung registriert er über die Dauer von einem Jahr die jeden Monat aufgrund von Ausfällen fällig werdenden Zahlungen (s. Abbildung 2.2). Wie die Tabelle in Abbildung 2.2 zeigt, ist in einem Monat kein Ausfall zu verzeichnen; hingegen weisen sechs Monate einen Ausfall, drei Monate zwei Ausfälle und zwei Monate drei Ausfälle mit jeweils unterschiedlichen Kostenfolgen auf.

* Anm.: Bei einer regulatorisch geforderten Eigenkapitalhinterlegung wird der Erwartungswert definitionsgemäss nicht als Risiko behandelt.

		Eingetretene Schadenshöhen in Tausend €					
		0	1	2		3	
Anzahl	Monat						
1			10				
2				30	20		
3			20				
4		0					
5						10	20
6			30				30
7				10	40		
8						20	30
9				20	40		
10			30				
11			40				
12			20				

Abbildung 2.2: Beispiel registrierter Ausfälle und Schadenshöhen

In Abbildung 2.3 sind sodann die resultierenden Tabellen für die statistischen Verteilungen sowohl der Anzahl der Schadensereignisse als auch der Schadenshöhen aufgezeigt.

Anzahl Schadensereignisse in einem Monat	Rel. Häufigkeit [%] der Anzahl	Schadenshöhe [Tausend €]	Rel. Häufigkeit [%] der Schadenshöhen
0	8.3	10	16.7
1	50	20	33.3
2	25	30	27.8
3	16.7	40	22.2
Erwartete Häufigkeit $H = 1.5$ (pro Monat)		Erwartete Schadenshöhe $S = 25.6$ T. €	

$$H_T = (0 \times 0.083) + (1 \times 0.5) + (2 \times 0.25) + (3 \times 0.167) = 1.5$$

$$S = (10 \times 0.167) + (20 \times 0.333) + (30 \times 0.278) + (40 \times 0.222) = 25.6 \text{ [T. €]}$$

Abbildung 2.3: Verteilungen Schadensanzahl und Schadenshöhe

Aus den Erwartungswerten (Mittelwerten) ergibt sich sodann gemäss der Formel der pro Monat zu erwartende Schaden (Verlust):

$$R_T = H_T \times S = 1.5 \times 25.6 \text{ T. €} = 38.3 \text{ T. €}$$

Durch Multiplikation mit 12 kann der monatlich erwartete Schaden auf ein Jahr umgerechnet werden. Das Ergebnis des erwarteten Schadens pro Jahr hätte natürlich für dieses Beispiel viel einfacher durch Summation aller eingetretenen Schäden über das Jahr errechnet werden können. Auch gilt zu erwähnen, dass die alleinige Berechnung des erwarteten Verlusts* für dieses Anwendungsbeispiel dann nicht besonders aussagekräftig ist, wenn noch die selten auftretenden langanhaltenden Ausfälle berücksichtigt werden müssen, die zusätzlich zu hohen Verlusten, infolge von Reputationsschäden oder Haftung, führen können. Für solche Risikosituation müssen die entsprechenden Verteilungen der Schadensanzahl und der Schadenshöhe zur Berechnung von aussagekräftigeren Risiko-Massen (z.B. dem „Value-at-Risk“ und dem „Expected Shortfall“) herangezogen werden, wie dies im Abschnitt 2.8.1 noch näher behandelt wird.

2.4

Probleme bei Risikobestimmung mittels einfacher Multiplikation

Die oben angeführten „einfachen“ Multiplikations-Formeln liefern bei relativ häufig eintretenden Ereignissen, wenn die Einzelschäden nicht übermässig gross sind, plausible Risikowerte. Die Ereignisse mit sehr grossen und für das Unternehmen schmerzlichen Schäden kommen in der Regel eher selten und mit schlecht quantifizierbaren Wahrscheinlichkeiten (Häufigkeiten) vor. Falls auch solche Ereignisse bei der Risikobestimmung berücksichtigt werden müssen, befinden sie sich in der absteigenden Flanke der Wahrscheinlichkeitsverteilung oder gar als „Ausreisser“ mit geringer Wahrscheinlichkeit im sog. „Schwanz“ der Wahrscheinlichkeitsverteilung. Für solche verhältnismässig hohen oder gar sehr hohen Schäden, die zwar mit geringer Wahrscheinlichkeit auftretenden, ist es daher nicht sinnvoll, das Risiko mittels einer einfachen Multiplikations-Formel zu bestimmen, da die arithmetische Multiplikation eines grossen Schadens mit einer geringen Wahrscheinlichkeit (Häufigkeit) im Schwanz der Verteilung ein für das Unternehmen zu geringes und damit allenfalls „tragbares Risiko“ vortäuschen würde.

Vorsicht mit den einfachen Multiplikations-Formeln ist auch geboten, wenn grobe Schätzwerte für Häufigkeit und Schadenshöhe in die Formel eingesetzt werden. Eine mit solchen Werten

* Der Erwartete Verlust wird in der Fachliteratur mehrheitlich nicht als eigentliches Risikomass verstanden

vorgenommene Multiplikation erweckt zwar den Eindruck eines genauen rechnerischen Ergebnisses; ein genaues Ergebnis ist aber bei geringen Eintrittswahrscheinlichkeiten (-Häufigkeiten) überhaupt nicht möglich.

Beispiel

Ereignet sich beispielsweise innert 10 Jahren in einem von hundert Computerräumen in der Schweiz ein Gross-Brand und zieht ein solcher Brand einen Schaden von 10 Millionen Franken nach sich, dann würde das mit obigen Multiplikations-Formeln* errechnete Risiko pro Jahr (bei einer errechneten Häufigkeit pro Computerraum und Jahr von $1/1'000$) gerade nur **10'000 Franken** betragen. Dieses über eine relativ kleine Wahrscheinlichkeit und einen grossen Schaden berechnete relativ geringe Risiko, könnte für ein Unternehmen mit einem Jahresumsatz von 10 Millionen Franken dazu verleiten, keine Vorkehrungen gegen das Brandrisiko zu treffen. Ein verantwortungsbewusstes Management wird hingegen – ungeachtet dieser offensichtlich falschen Risiko-Berechnung – den Brandrisiken im Rechenzentrum mit umfassenden Massnahmen begegnen, da bei einem tatsächlichen Brandereignis das Unternehmen ohne adäquate Massnahmen wahrscheinlich nicht überleben würde.

Seltene, aber sehr grosse Schadensereignisse

Dieses Beispiel zeigt, dass für seltene, aber grosse Schadensereignisse die Berechnungen mit den oben angeführten „einfachen Risikoformeln“ keine adäquaten Entscheidungsgrundlagen liefern. Hier helfen Risikomasse, wie sie im Abschnitt 2.8.1 näher dargelegt werden.

In einem alternativen pragmatischen Ansatz wird für die seltenen, aber sehr grossen Schadensereignisse vorrangig der mögliche Schaden und nicht ein über die Wahrscheinlichkeit rechnerisch ermitteltes Risiko als Entscheidungsgrundlage herbeigezogen. Bei der „Analyse“ und „Bewertung“ des Risikos kann diesem Umstand mit einer entsprechend ausgelegten Risiko-Bewertungs-Matrix Rechnung getragen werden (s. Abschnitt 2.5.1).

2.5

Subjektivität bei Einschätzung und Bewertung der Risiken

Die Einschätzung der beiden Risiko-Dimensionen „Wahrscheinlichkeit“ und „Schaden“ (Konsequenzen, Tragweite, Verlust) eines Schadensereignisses erfolgt einerseits aus den Erfahrungen

* Beispiel kann auch für die 2. Formel mit den Mittelwerten angewendet werden

und Aufzeichnungen aus der Vergangenheit (ex post) und/oder aus der Prognose für zukünftige Ereignisse (ex ante). Die Einschätzung für die Zukunft sowie die Einstellung zur Tragbarkeit der Risiken hängen stark von der Subjektivität der am Risikomanagement-Prozess beteiligten Personen ab.

*Risiko-Freudigkeit
/ Risiko-Aversion*

So neigen die einen Personen zur Risiko-Affinität*, andere wiederum zur Risiko-Aversion†.

Auch sind einer einzelnen Person kaum alle relevanten Fakten für die Beurteilung eines Risikos bekannt. Aufgrund der Subjektivität bei der Wahrnehmung (Perzeption), aber auch bei der Risikobehandlung empfiehlt es sich, die Analysen und Entscheidungen beim Risikomanagement möglichst unter vielen Gesichtswinkeln breit abzustützen. Es empfiehlt sich beispielsweise, die Analyse mit einem interdisziplinär zusammengestellten Risiko-Analyse-Team durchzuführen und die Handlungs- und Akzeptanzentscheide über grosse Risiken im Team (z.B. Geschäftsleitung, Sicherheitskommission) zu fällen.

2.6 Hilfsmittel zur Analyse, Aufbereitung und Darstellung der Risiken

2.6.1 Risiko-Bewertungs-Matrix

Das Dilemma mit der einfachen Risiko-Formel können wir mit einem pragmatischen, für viele Anwendungen hinreichenden Ansatz lösen, indem wir beispielsweise das „Produkt“ einiger Häufigkeitswerte und einiger Schadenswerte (als Funktion) in einer Risiko-Bewertungs-Matrix festlegen.

*Risiko-
Wahrnehmung*

Bei der Festlegung der „Produktwerte“ kann die Risiko-Wahrnehmung des Managements, insbesondere für grosse und seltene Schadensereignisse, berücksichtigt (vorprogrammiert) werden.

* Risiko-Affinität (Risiko-Freude) bewirkt ein Entscheidungsverhalten, bei dem die jeweils riskantere Handlungsalternative im Hinblick auf mögliche Chancen bevorzugt wird, auch wenn die Erfolgsaussichten ungewiss sind oder Misslingen droht.

† Risiko-Aversion bewirkt ein Entscheidungsverhalten, bei dem die jeweils weniger riskante Handlungsalternative bevorzugt wird.

*Risiko-Matrix für
„Wahrnehmung“
und „Bewertung“
der Risiken im
Unternehmen*

Die solchermassen entwickelte „Risiko-Bewertungs-Matrix“, oder kurz Risiko-Matrix genannt, werden wir sodann als Hilfsmittel für die „Analyse“ und „Bewertung“ der Risiken im Unternehmen einsetzen. Natürlich ist es in einem grösseren Unternehmen auch möglich, mit unterschiedlichen „Risiko-Matrizen“ für unterschiedliche Bereiche (z.B. für Tochtergesellschaften) zu arbeiten. Dabei sollte aber auf die Kompatibilität der Skalen geachtet werden. Das Beispiel einer solchen Risiko-Matrix ist in der nachfolgenden Abbildung 2.4 gezeigt.

Monetarisierte Risiko-Werte in Mio. €					
bis 0.1	0.1 - 0.3	0.3 - 1	1 - 3	3 - 10	über 10
sehr klein	klein	mittel	gross	sehr gross	katastrophal

Schadenshöhe pro Fall Häufigkeit der Fälle	E	D	C	B	A
	klein	mittel	gross	sehr gross	katastrophal
sehr oft (mehrmals pro Jahr)	mittel	gross	sehr gross	katastrophal	irreal (*)
oft (1 mal in 1 – 3 Jahren)	klein	mittel	gross	sehr gross	katastrophal
selten (1 mal in 3 – 10 Jahren)	sehr klein	klein	mittel	gross	katastrophal
sehr selten (1 mal in 10 – 30 Jahren)	sehr klein	klein	klein	mittel	katastrophal
unwahrscheinlich (1 mal in mehr als 30 Jahren)	sehr klein	sehr klein	klein	mittel	katastrophal (**)

(*) Risiken werden als „irreal“ bezeichnet, da mehrere „katastrophale“ Schäden im Jahr die Insolvenz des Unternehmens bedeuten würde.

(**) Für katastrophale Schäden wird das Risiko mit der Höhe des Schadens gleichgesetzt.

Abbildung 2.4: Risiko-Matrix mit Ordinalskala und monetarisierten Risiko-Werten

Im nächsten Abschnitt wird gezeigt, welche Voraussetzungen geschaffen werden müssen, um die Schäden einschätzen zu können.

2.6.2

Kriterien zur Schadenseinstufung

Kardinale und ordinale Skalen

Um ein Risiko bestimmen zu können muss, neben der Wahrscheinlichkeit (Häufigkeit), der zugrundeliegende Schaden ermittelt werden können. Der Schaden kann sich in verschiedenen Ausprägungen (Impacts) darstellen. Letztendlich ist der für das Unternehmen entstehende gesamte Schaden für die Bestimmung des Risikos massgebend. Die sich aus einem Schadensereignis ergebenden „direkten finanziellen Verluste“ werden oft mit rechenbaren Werten (z.B. Euro) eines „kardinalen“ Skalensystems eingeschätzt. Hingegen erfolgt die Einschätzung der sonstigen Schadensauswirkungen, die sich indirekt und oft erst in der langen Frist als finanzielle Schäden für das Unternehmen auswirken, vorzugsweise mit „ordinalen“ Werten (z.B. klein, mittel, gross). Um der Schadens- und Risiko-Wahrnehmung des Unternehmens gerecht zu werden, empfiehlt es sich jedoch, auch die direkten finanziellen Verluste mit ordinalen Werten mittels einer für das Unternehmen einheitlichen Ordinalskala einzustufen*. Zur Abstimmung der Ordinalskala mit tatsächlichen finanziellen Werten, werden den ordinalen Skalen-Werten noch unternehmensspezifische monetäre Werte (z.B. Eurobeträge) zugeordnet.

Schadens- Einstufungstabelle

Die Abbildung 2.5 zeigt wie eine solche Schadens-Einstufungstabelle (Schadensmetrik) aussehen könnte. Die Schadenseinstufungstabelle richtet sich nach der Grösse und der Branche des Unternehmens sowie nach den Besonderheiten seiner Risiko-Objekte.

Einstufungs- Kriterien

Für jede Schadensstufe dieser Metrik werden die „Einstufungskriterien“ der Schadensauswirkungen sowohl in qualitativer (ordinaler) als auch in quantitativer (kardinaler) Weise festgelegt.

* Eine ordinale Einstufung liegt auch den sog. „Scoring“- und „Rating“-Verfahren zugrunde. Die mit diesen Instrumenten erhobenen Daten werden auch als „Scorecard-Daten“ bezeichnet. Sollen die als „Scores“ erhobenen Risikodaten später quantitativ aggregiert werden, dann ist dies beim Aufbau und bei der Monetarisierung der Risiko-Matrix entsprechend zu berücksichtigen.

Impacts

* z.T. persönliche Haftung verantwortlicher leitender Personen

Abbildung 2.5: Beispiel der Schaden-Einstufungstabelle eines Unternehmens

Wie das Beispiel in Abbildung 2.5 zeigt, ist es sinnvoll, die möglichen Schadensauswirkungen (Impacts) grob zu unterteilen, z.B.:

- Direkte finanzielle Schäden;
- Schädigung der geschäftlichen und wirtschaftlichen Interessen;
- Verlust an Reputation und Goodwill;
- Nichteinhaltung gesetzlicher und regulativer Verpflichtungen;
- Beeinträchtigung der Gesundheit, Sicherheit und des Schutzes anderer Personen.

Für unterschiedliche Geschäftsprozesse wird es in der Regel auch unterschiedliche Kriterien geben. Die „Skalierung“ der Schadensmetrik sollte jedoch vorzugsweise, unter Berücksichtigung der wichtigsten Geschäftsprozesse, für das gesamte Unternehmen einheitlich festgelegt sein.

Monetäre Höhe für „sehr grosse“ Schäden

Für eine solche einheitliche Schadens-Metrik wird es die Aufgabe der Geschäftsleitung sein, zumindest für den als „sehr gross“ einzustufenden Schaden die monetäre Höhe festzulegen (z.B. Höhe eines durchschnittlichen jährlichen Betriebsgewinns über die letzten 5 Jahre). Sind die monetären Werte der Metrik für „direkte finanzielle Schäden“ einmal festgelegt, dann lassen sich diese monetären Werte auch als „Äquivalente“ für die Einstufung der „indirekten Schäden“* heranziehen.

Spezifische, aufeinander abgestimmte Schadens-Metriken

In einem grösseren Unternehmen sind u. U. für einzelne Risiko-Gebiete auch spezifische Schadens-Einstufungstabellen sinnvoll (z.B. für eine Tochtergesellschaft mit speziellen Geschäftsprozessen). Für ein integriertes Unternehmens-Risikomanagement müssen jedoch die verschiedenen Einstufungstabellen untereinander abgestimmt und ineinander überführbar sein.

Bewilligung und Inkraftsetzung Schadens-Einstufungstabelle

Die Festlegung und regelmässige Anpassung einer Schadens-Einstufungstabelle mit einer entsprechenden Metrik gehört zu den grundlegenden Voraussetzungen für ein nach rationalen Gesichtspunkten durchzuführendes Risikomanagement. Im Rahmen der Unternehmens-Governance werden die Vorgaben für die Schadenseinstufung auch durch die obersten Führungsgremien bewilligt und in Kraft gesetzt.

* Indirekte Schäden (z.B. Reputations-Schäden) wirken sich nicht unmittelbar auf das finanzielle Ergebnis aus.

Metrik zur Einschätzung der Wahrscheinlichkeit oder Häufigkeit

Die für die Einschätzung der Wahrscheinlichkeit oder Häufigkeit eines Schadensereignisses benötigte Metrik ergibt sich aus den typischen Bedrohungen eines Unternehmens und wie diese auf die zu schützenden Werte (Assets) einwirken können (s. Abbildung 2.4). Wie in weiteren Kapiteln dieses Buches gezeigt ist, erfolgen die Einschätzungen der Schäden und deren Eintrittswahrscheinlichkeiten am konkreten Risiko-Objekt mit sog. „Assessment“-Verfahren, die den jeweiligen Problemstellungen gerecht werden (s. Abschnitte 3.3 und 10.1.2).

Reduktion Wahrscheinlichkeit oder Schaden

Für die einem Risiko-Assessment*-Prozess folgenden Massnahmen-Entscheide ist es oft sinnvoll, sowohl das bewertete Risiko als auch die einzelnen Werte für die Schadenshöhe und die Wahrscheinlichkeit (Häufigkeit) darzustellen, da entweder die Reduktion des Schadens (Beispiel: Notfallmanagement) oder der Eintrittswahrscheinlichkeit (Beispiel: Vieraugenprinzip) sinnvoll sein kann.

Für die Massnahmen-Entscheide können aber auch die Messergebnisse von Risiko-Indikatoren, die einen kausalen Bezug zu den Risikovariablen haben, herangezogen werden (s. Abschnitt 2.8.2).

2.6.3

Risiko-Landkarte, Akzeptanz-Kriterien und Risiko-Portfolio

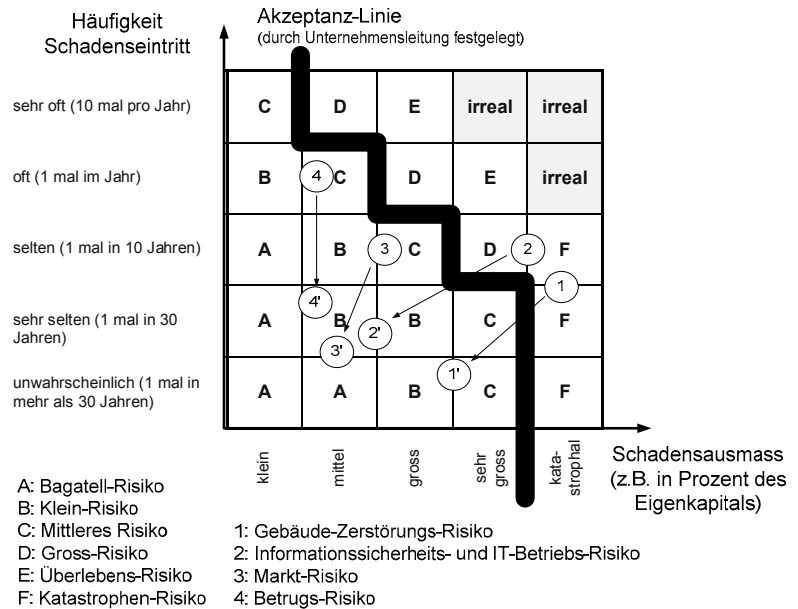
Risiko Portfolio / Risk Map

Eine übersichtliche Darstellung mehrerer Risiken kann als so genanntes Risiko-Portfolio in einer zweidimensionalen graphischen Risiko-Landkarte (Risk Map) vorgenommen werden.

Diese Darstellung eignet sich vorzüglich, um die Risiken nach strategischen Gesichtspunkten einzuordnen. Sowohl die Bewältigungsstrategien als auch die Risiko-Akzeptanz-Linie können im Risk Map dargestellt werden.

Die Risk Map in Abbildung 2.6 zeigt beispielhaft das Portfolio einiger Unternehmens-Risiken (Gebäude-Zerstörungs-Risiko, IT-Betriebs-Risiko, Markt-Risiko, Betrugs-Risiko) wie sie vor und nach der Risiko-Bewältigung positioniert sind.

* „Risiko-Assessment“ enthält die Aufgaben der Identifikation, der Analyse und der Bewertung der Risiken.



Abbildungung 2.6: Risiko-Portfolio in Risk-Map mit Akzeptanzlinie

Risiko-Akzeptanzlinie

Die Risiko-Akzeptanzlinie in der Risk-Map dient als grobes Kriterium dafür, welche Risiken in einem Unternehmen, allenfalls ohne weiteren Massnahmen, akzeptiert werden können. Die Geschäftsleitung eines Unternehmens wird zwar neben der Risiko-Akzeptanzlinie noch weitere Kriterien festlegen, die bei der Akzeptanz von Risiken oder deren Bewältigung beachtet werden müssen (z.B. Dringlichkeit und Kosten der Massnahmen). Für unterschiedliche Geschäftszweige sind die Portfolios und Akzeptanzlinien oft unterschiedlich definiert, da die Risiko-Toleranz vom Geschäft abhängt und im Verhältnis zu den Chancen und den verfügbaren Ressourcen definiert werden muss.

2.6.4

Risiko-Katalog

Die „Buchführung“ über die Risiken erfolgt mit so genannten Risiko-Katalogen (Risiko-Register). Die Risiko-Kataloge enthalten in geeigneter Weise die bisher vorgestellten Risiko-Parameter und Ordnungsbegriffe. Der Risiko-Katalog wird bereits bei der Risiko-Identifikation aufgebaut und muss für neue Risiko-Arten, Risiko-Objekte, Bedrohungen und System-Ziele flexibel erweiterbar sein (s. Beispiel in Abbildung 2.7).

Risiko-Art: Risiko-Art 1

Risiko-Bereich: IT-Abteilung

Risiko-Owner: Hans Holbein, Leiter IT-Abteilung

Objekte	Bedrohung (Gefahr)				Schadenshöhe Einstufung			Eintritt 1 mal in				Bemerkungen zu den potentiellen Schäden (Schadenstypen etc.)	Bestehende Massnahmen Beschreibungen / Bemerkungen	Vorgeschlagene Massnahmen Beschreibungen / Bemerkungen	
	Bedrohung 1	Bedrohung 2	Bedrohung 3	... Bedrohung n	System-Ziel 1	System-Ziel 2	System-Ziel 3	0.1 Jahr	1 Jahr	10 Jahren	30 Jahren				> 30 Jahre
Objekt 1	x				gross	klein	mittel			x			...		
		x			...										
			x												
				x											
					x										
Objekt 2															
	x														
		x													
			x												
				x											

Abbildung 2.7: Beispiel für den Aufbau eines Risiko-Katalogs

Der Aufbau der Kataloge ist stark von der jeweiligen Zweckbestimmung abhängig (z.B. Berichterstattung an die Geschäftsleitung oder Überwachung der Risiken und Massnahmen einzelner Unternehmensbereiche). In den Abschnitten 10.1.3 bis 10.1.6 ist ein Katalog gezeigt (auch Risikoregister genannt), der für das Risikomanagement der einzelnen „Assets“ sukzessive aufgebaut und gemäss dem Prozess-Fortschritt ergänzt werden kann.

Die von den einzelnen Organisationseinheiten des Unternehmens (z.B. Abteilungen) detailliert ausgefüllten Kataloge werden oft in einem für das gesamte Unternehmen gemeinsamen Risiko-Katalog konsolidiert. Dabei sind die Auslegungen der Kataloge und die Art der Konsolidierungen (ggf. der Risiko-Aggregation) von der Zweckbestimmung und der aufsichtsrechtlichen Anforderungen an das Unternehmen geprägt. Mit der auch häufig verwendeten Bezeichnung „Risiko-Inventar“ wird deutlich, dass der Katalog möglichst realitätsgetreu die Risikosituation wiedergeben sollte. Deshalb ist für eine möglichst flexible Erfassung, Auswertung und Kommunikation eines umfangreichen Risiko-Katalogs auch eine entsprechende Datenbank zu empfehlen. Eine solche Datenbank könnte auch mit einer für die Risiko-Identifikation und -Analyse hilfreichen „Schadensdatenbank“, welche die Fakten erfolgter Ereignisse enthält, kombiniert werden.

2.7

Risiko-Aggregation und Abhängigkeiten*Korrelationen*

Risiken interessieren nicht nur als Einzelwerte sondern auch in geeigneten Zusammenfassungen. Liegen die Risiken in numerischen Werten vor, entsteht unwillkürlich der Wunsch, die Risiken zu addieren. Da einzelne Risiken nach Wahrscheinlichkeiten eintreten und allenfalls bestimmte Abhängigkeiten untereinander haben können, weil sie beispielsweise auf denselben oder ähnlichen Ursachen beruhen oder sich aufgrund ihrer Auswirkungen gegenseitig beeinflussen, dürfen sie nicht ohne weiteres addiert werden. Derartige Abhängigkeiten von jeweils zwei Zufallsvariablen werden als „Korrelation“ bezeichnet. Bei der Korrelation interessiert in erster Linie die Stärke und das Vorzeichen der Abhängigkeit. So spricht man von einer positiven Korrelation, wenn sich bei der Vergrößerung eines Risikos auch die Vergrößerung bei einem anderen Risiko einstellt. Hingegen von negativer Korrelation, wenn bei der Vergrößerung eines Risikos bei einem zweiten Risiko eine Verringerung zu verzeichnen ist. Sind die beiden Risiken voneinander „stochastisch unabhängig“ dann besteht keine Korrelation. Wird die gegenseitige Abhängigkeit mit einem „Korrelationskoeffizienten“ ausgedrückt, dann beträgt der Wert des Korrelationskoeffizienten Null, wenn keine Korrelation vorliegt. Bei maximaler positiver Korrelation beträgt sein Wert + 1 und bei maximaler negativer Korrelation -1. Mit Werten zwischen + 1 und -1 können mehr oder minder starke Abhängigkeiten hinsichtlich Verstärkung oder Abschwächung ausgedrückt werden.

Zurückkommend auf das oben aufgestellte Postulat, dass Risiken nicht einfach addiert werden dürfen, kann festgehalten werden, dass eine Addition der Einzelrisiken nur bei maximaler positiver Korrelation zulässig ist und sich andernfalls ein zu hoher Wert für das Gesamtrisiko ergibt.

Sind hingegen die Risiken stochastisch voneinander unabhängig, dann kommt als Gesamtrisiko* näherungsweise die Quadratwurzel aus der Summe der Einzelrisiken zum Tragen. In der Praxis besteht zwischen den einzelnen operationellen Risiken meist eine gewisse, wenn auch nicht totale Korrelation.

* Approximatives Gesamtrisiko bei unkorrelierten Einzelrisiken:

$$R_{\text{ges}} = \sqrt{\sum_{i=1}^n R_i^2}$$

In der praktischen Anwendung muss zudem berücksichtigt werden, dass ein Korrelationskoeffizient* einen idealisierten Wert darstellt und lediglich ein Indiz für die Abhängigkeiten der Risiken untereinander liefern kann.

Die Aggregation kommt zum Tragen, wenn aus statistisch verteilten Werten eines „Einzelrisikos“ ein zusammengefasstes Risikomass bestimmt werden soll, oder wenn mehrere „Einzelrisiken“ innerhalb einer „Risikoart“ oder eines ganzen „Risikoportfolios“ zu einem Gesamtrisiko kumuliert werden sollen. So ist für die Darstellung einer Gesamtverlust-Risikoposition auf Unternehmensebene, zur Unterlegung mit Eigenkapital, eine Aggregation der Einzel-Risikopositionen in den verschiedenen Risikokategorien notwendig. Eine häufig angewendete Möglichkeit, die Risiken zu aggregieren, besteht in der Bildung des „Value at Risk“ aus den jeweiligen Einzelschäden (resp. Einzelverlusten) und ihren Eintrittswahrscheinlichkeiten† (s. Abschnitt 2.8.1). Aufbauend auf dem „Value at Risk“ können noch weitere Risikomasse, wie der „Expected Shortfall“, ermittelt werden, mit denen die seltenen Risiken mit extrem hohem Schadensausmass quantifiziert werden können.

*Rechnerische
Methoden der
Risiko-
Aggregation*

Wir werden in diesem Buch an verschiedenen Stellen auf die rechnerischen Methoden der Risiko-Aggregation eingehen (s. Abschnitt 2.8.1), diese aber nicht in der Tiefe behandeln, wie dies allenfalls für die Bestimmung des erforderlichen Eigenkapitals aus den operationellen Risikopositionen notwendig wäre. Die Gründe dafür sind die Komplexität und Aufwändigkeit bei der praktischen Anwendung, insbesondere beim Vorliegen von Korrelationen.

*Simulation mit
Monte Carlo-
Methode*

Die Aggregation zu einer Gesamtverlustverteilung kann vor allem mittels der „Monte-Carlo-Methode“ simuliert werden (s. Anhang A.5.3). Eine solche Simulation setzt entsprechende Annahmen über die Wahrscheinlichkeitsverteilungen voraus und ist aufwändig in der Durchführung.

* Der Korrelationskoeffizient basiert auf einem linearen Zusammenhang der miteinander in Beziehung stehenden Zufallsvariablen. Zudem müssen für seine Berechnung als Quotient der Kovarianz und der Standardabweichungen der beiden Zufallsvariablen die Voraussetzungen für „Normalverteilungen“ erfüllt sein, dies ist jedoch bei den operationellen Risiken nicht der Fall (s. Abschnitt 2.8.1).

† Vorsicht: Aufgrund der mangelnden Subadditivität dürfen die Value-at-Risik-Werte der Einzelrisiken nicht einfach addiert werden.

*Aufzeigen der
Abhängigkeiten
im Risikokatalog*

Trotz der Schwierigkeiten bei der Aggregation korrelierter Risiken können wir die Risiken auf Unternehmensebene zumindest „konsolidieren“, indem die ordinal eingestufteten Risiken in einem Risikokatalog nach ihrer Höhe absteigend und ihren Abhängigkeiten untereinander eingeordnet werden. Die Korrelationen zwischen den Risiken werden dabei mit heuristischen Methoden festgestellt und im Risiko-Katalog entsprechend vermerkt. Oft sind auch sog. „Risk Driver“ für die Beeinflussung mehrerer Risiken in ggf. unterschiedlicher Stärke massgebend (z.B. Outsourcing eines IT-Systems oder Restrukturierung von Organisations-/Organisationseinheiten). Auch solche „Risk Driver“ können mit ihrem voraussichtlichen Effekt auf die Risiken in geeigneter Weise im Risiko-Katalog vermerkt werden.

Ein derartiger Katalog eignet sich zur Registrierung und Umsetzungs-Überwachung von Gegenmassnahmen, die ja bei operationellen Risiken im Vordergrund stehen. Zudem gibt ein solcher Katalog in aussagekräftiger Weise die Risikosituation im Unternehmen wieder.

Hinsichtlich der Darstellung des Risikos, ob es bezüglich seines finanziellen Impacts oder anderen Impact-Arten dargestellt werden soll, hängt vom Zweck der Analyse ab. So wurde das in Abschnitt 2.3 beispielhaft aufgeführte Risiko von Serverausfällen auf der Aggregationsstufe der Folgekosten aus den Serverausfällen dargestellt, da in diesem Falle die Kosten interessierten. Für manche Zwecke, z.B. für die Berücksichtigung der Malus-Kosten im Jahres-Budget mag diese Berechnung sinnvoll sein. Hingegen für die Bestimmung passender Massnahmen zur Risiko-Reduktion ist dieses „aggregierte“ Risiko-Resultat auf der Kostenebene nicht immer besonders aussagekräftig. Für die Bestimmung der Massnahmen zur Risiko-Reduktion ist meist eine feinere Analyse des Risikos auf der Ebene der einzelnen Komponenten und Prozesse und allenfalls sogar auf der noch fundamentalen Ebene der für den Betrieb massgeblichen Fähigkeiten des Personals notwendig. Die Risiken aus den verschiedenen vorgelagerten Ebenen manifestieren sich jedoch schlussendlich auf der Ebene der Finanzen des Unternehmens.

2.8

Beschreibung der Risiken mit Risikomasszahlen

Bereits in Abschnitt 2.2 wurden einfache Darstellungen des Risikos in seinen Komponenten Wahrscheinlichkeit (resp. Häufigkeit) und Schadensausmass gezeigt und auf die Einschränkungen und Probleme bei der Anwendung einfacher Risikomasse aufmerksam gemacht. Da die Art der Analyse und Darstellung des

Arten der Risiko-Analyse

Risikos stark vom Anwendungszweck abhängig ist, soll nachstehend noch näher auf einzelne in der Praxis öfters vorkommende Risikomasse eingegangen werden.

Aufgrund ihres Anwendungszwecks können die Analysearten und daraus resultierenden Masszahlen für das Risiko wie folgt grob unterteilt werden:

1. **Schätzung der mittleren Werte** für die Wahrscheinlichkeiten (Häufigkeiten) und Schäden der Schadensereignisse an den Risiko-Objekten.
2. **Schätzung der maximal möglichen Werte** für Schäden an den einzelnen Risiko-Objekten und der Wahrscheinlichkeiten, dass diese Schäden eintreten. Diese maximal möglichen Werte resultieren aus einem „Worst Case Szenario“ (z.B. kompletter Datenverlust).
3. **Bestimmung von Risiko-Werten mittels stochastischer Methoden.** Entsprechend der Aufgabenstellung und der gewählten Methode wird das Risiko mit entsprechenden statistischen Parametern wie „Erwartungswert“, „Standardabweichung“, „Value at Risk“, „Conditional Value at Risk“ auf der Basis erhobener und/oder geschätzter Daten berechnet oder mittels stochastischer Simulationen unter wirklichkeitsnahen Annahmen bestimmt.
4. **Bestimmung von Risiko-Kennwerten mittels Risiko-Indikatoren,** welche wichtige hervorzuhebende Aspekte des Risikos ausdrücken, und einen kausalen Zusammenhang mit dem tatsächlichen Risiko aufweisen.
5. **Bestimmung von Risiko-Werten mittels Spieltheorie,** bei der die Ereignisse nicht nur aufgrund zufälliger Ursachen, sondern auch infolge des Verhaltens der beteiligten Personen (Opponenten und Betroffene) analysiert werden, z.B. Datenspionage.

Bei der Behandlung der Assessment-Verfahren in den Abschnitten 3.3 bis 3.7 werden noch einige prozedurale Verfahren gezeigt, mit denen solche Masszahlen ermittelt werden können.

2.8.1

Stochastische Methoden zur Bestimmung des Risikos

Arten der Risiko- Einschätzung

Wie wir in den bisherigen Betrachtungen sehen konnten, ergibt die einfache Multiplikation der Mittelwerte von Eintrittshäufigkeit und Schadenshöhe bei Risiken, die selten, aber mit grösseren Schäden vorkommen, ein zu geringes Ergebnis für das Risiko. Die ebenfalls einfache „Worst-Case-Betrachtung“ gibt zwar einen Anhaltspunkt für den maximalen Schaden, trifft aber keine Aussage über die weniger seltenen und weniger hohen Schäden. Sollen also Risiken gemäss ihrer statistischen Eigenschaften genauer gemessen werden, dann sind dafür entsprechend stochastische Risikomasse notwendig, von denen der „Value at Risk“ (VaR) ein wichtiger Vertreter ist.

Das Mass Value at Risk, VaR ($V; \alpha; T$), ist wie folgt definiert:

Der „**Value at Risk**“ ist der maximal erwartete Verlust (Schaden) V , der unter üblichen Bedingungen innerhalb einer bestimmten Zeit-Periode T mit einer bestimmten Wahrscheinlichkeit α , dem sog. Konfidenz-Niveau, nicht überschritten wird.

Konfidenz-Niveau und Restwahr- scheinlichkeit

Es sind zwar auch grössere Verluste als die maximal erwarteten Verluste möglich, aber eben nur mit einer Restwahrscheinlichkeit. Liegt das Konfidenz-Niveau beispielsweise bei 95 %, dann wird mit einer Restwahrscheinlichkeit von 5 % der Maximal-Schaden überschritten. Unterliegen die Verluste (Schäden) annäherungsweise einer theoretischen Wahrscheinlichkeits-Verteilung, dann lässt sich der „Value at Risk“ anhand dieser Verteilung analytisch ermitteln. Liegen empirisch ermittelte Daten vor, dann erfolgt die Kumulation anhand der diskret verteilten Zufallswerte (s. Beispiel im Anhang A.5).

Das oben angegebene Prinzip eines „Value at Risk“ zur Bestimmung einer Risiko-Masszahl wird vorteilhaft für Risiken angewandt, die näherungsweise einer Normalverteilung unterliegen (z.B. Marktrisiken). Das Konzept lässt sich aber auch in der Form eines „Operational Value at Risk“ auf unsere in die Kategorie der operationellen Risiken gehörenden Informationssicherheits- und IT-Risiken einsetzen ([Wolk07], S. 198-209), ([Jori07], S. 497-510). In der Abbildung 2.8 wird die Bildung des „Operational Value at Risk“ veranschaulicht.

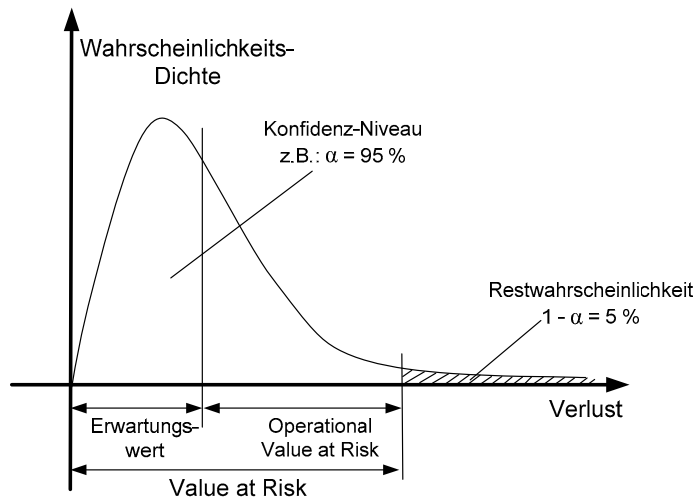


Abbildung 2.8: „Value at Risk“ mit Konfidenz-Niveau 95 %

Wahrscheinlichkeitsverteilung operationeller Risiken
Log-Normal-Verteilung

Dabei gilt es zu bemerken, dass die operationellen Risiken nicht einer symmetrischen Normalverteilung, sondern einer einseitigen asymmetrischen „rechtsschiefen“ Verteilungsdichtefunktion folgen.

Eine passende Wahrscheinlichkeits-Verteilung für operationelle Risiken kann manchmal nach heuristischen Überlegungen und bestimmten Anpassungstests aufgrund des vorhandenen Datenmaterials ausgewählt werden. So eignet sich für die Verteilung der „Verlusthöhen“ bei operationellen Risiken beispielsweise häufig die Log-Normal-Verteilung [Piaz02, 112]. Weitere gebräuchliche Wahrscheinlichkeits-Verteilungen für die Verteilung der Verlusthöhen operationeller Risiken sind die Weibull- und die Exponential-Verteilung. Bei diesen Verteilungen führen die „meisten“ Verlustereignisse zu einem „kleinen bis mittleren“ Schaden. Hingegen kommen die Ereignisse mit „schweren“ Schadensfolgen vergleichsweise selten (d.h. mit geringer Wahrscheinlichkeit) vor (s. Abbildung 2.8).

Die zur Berechnung der Masszahlen „Erwartungswert“ und „Value at Risk“ massgebliche Gesamt-Verlustverteilung ergibt sich aus der Kombination* der „Verlusthöhenverteilung“ und der „Ver-

* Sind die „Verlusthöhen“ und „Verlusthäufigkeiten“ voneinander stochastisch unabhängig, dann können ihre Verteilungen zu einer Gesamtverlustverteilung „gefaltet“ werden.

lusthäufigkeitsverteilung“ zu einer „Gesamtverlustverteilung“ (s. Beispiele im Anhang 5). Die Risikofestlegung mittels eines „Value at Risk“ führt auch zu einer von Abbildung 2.6 abweichenden Darstellung eines Risiko-Portfolios, wie dies in Abbildung 2.9 beispielhaft gezeigt ist (vgl. [Glei08]).

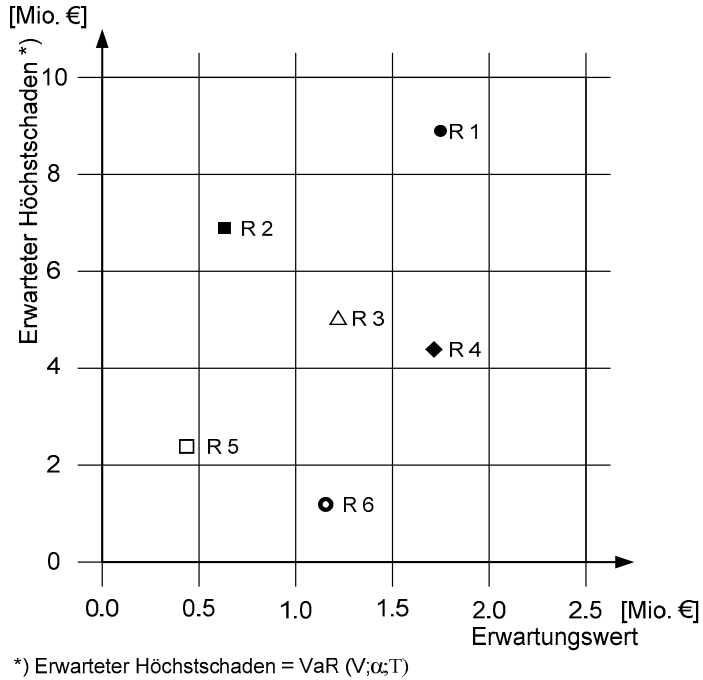


Abbildung 2.9: Beispiel alternative Risikoportfolio-Darstellung

Der für operationelle Risiken typische langgezogene rechte „Schwanz“ der Verlust-Verteilungsdichtefunktion (s. Abbildung 2.8) lässt jedoch die Berechnung eines „Value at Risk“ fürs Erste als fragwürdig erscheinen, da er ja lediglich eine Kumulation innerhalb des Konfidenzniveaus α darstellt, wobei die mit sehr grossen Schäden eintretenden seltenen Ereignisse jenseits des Konfidenzniveaus nicht berücksichtigt werden. Solche Ereignisse, die für ein Unternehmen sehr schmerzlich sein können, sollten jedoch für eine realistische Risikobeurteilung auch berücksichtigt werden. Zur Berücksichtigung auch dieser Schäden jenseits des Konfidenzniveaus des VaR stehen eine Reihe von Methoden zur Verfügung, wie beispielsweise die Berechnung des sog. „Expected Shortfall“, der den Erwartungswert (Mittelwert) der „Value at Risk“-Überschreitungen misst. Doch ist für eine solche Berech-

nung meist wenig statistisches Datenmaterial vorhanden, weshalb grosse Ungenauigkeiten zu erwarten sind. Mit der Anwendung der sog. „Extremwert-Theorie“ kann den Schätzungsproblemen im „Verteilungsschwanz“ noch besser Rechnung getragen werden, indem die über definierte Schwellenwerte „ausreissenden“ Verluste“ basierend auf teils beobachteten und teils prognostizierten Werten berechnet werden können. Für die relativ aufwändige mathematische Anwendung dieser Theorie zur Berechnung der „katastrophalen Verluste“ sei auf die entsprechende Literatur verwiesen ([Dölk06], S. 109-155, [Prok08], S. 58-63).

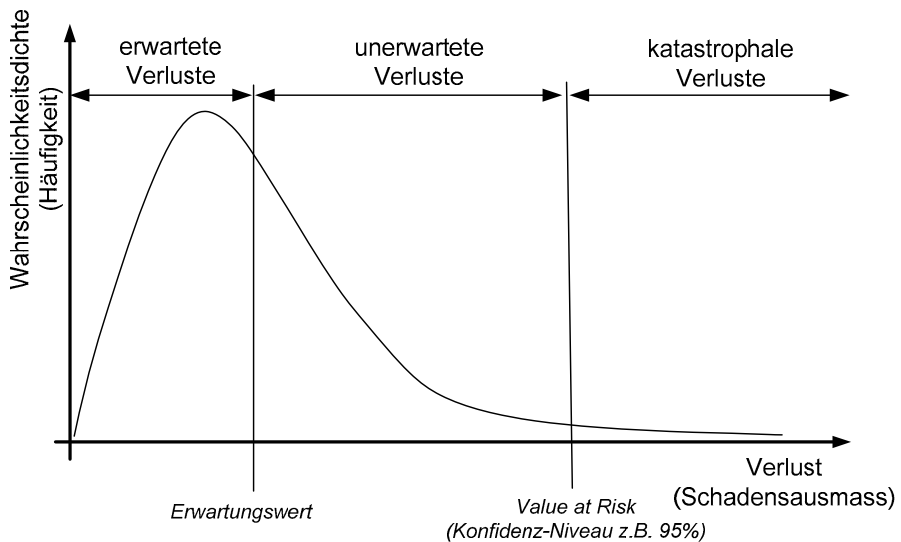


Abbildung 2.10: Einteilung der Verluste aufgrund verschiedener Risiko-Masszahlen

Wie die Abbildung 2.10 zeigt, ist es üblich, eine Einteilung in „erwartete Verluste“, „unerwartete Verluste“ und „katastrophale Verluste“ vorzunehmen*. Bei Banken und Versicherungen unterliegen die als Restrisiken verbleibenden „unerwarteten“ und „ka-

* Vgl. ([Alex03], S. 143), ([Oenb05], S. 15) und ([Glei05], S. 133):

Erwartete Verluste: Werden als laufende Kosten in den Preis eingekalkuliert

Unerwartete Verluste: Werden durch ökonomisches (Eigen-) Kapital unterlegt

Katastrophale Verluste: Werden durch Risikotransfer und Risikofinanzierung gedeckt.

tastrophalen“ Verluste regulatorischen Auflagen betreffend der Eigenkapitalunterlegung (s. Kapitel 3).

2.8.2

Risiko-Analyse und -Überwachung mit Indikatoren

In den vorangegangenen Ausführungen wurden Hilfsmittel zur Risikomessung und -darstellung basierend auf den beiden grundlegenden Dimensionen Wahrscheinlichkeit (Häufigkeit) und Auswirkung (Schaden) behandelt. Im praktischen Umgang mit der Risikomessung stehen diese beiden Dimensionen nicht immer im Vordergrund. Vor allem wenn diese Variablen schlecht oder nur auf Umwegen explizit ermittelt werden können, oder wenn die das Risiko beeinflussenden Faktoren, wie die Schwachstellen oder die Früherkennung der Risiken, für die Risikohöhe und die Risikobewältigung einen starken Einfluss haben.

Für eine solche an den konkreten Risikoverhältnissen orientierte Messung von Risikoaspekten werden entsprechend spezifische Indikatoren (resp. Kennzahlen) eingesetzt. Diese Indikatoren zeigen meist einen „Messwert“ über die Zielerreichung bei den für die Risikoaspekte massgeblichen Vorkommnissen an.

Voraussetzung ist, dass diese sog. Risiko-Indikatoren einen nachweislich kausalen Zusammenhang mit dem Risiko aufweisen. Wie im Abschnitt 5.4.4 noch näher gezeigt wird, ist gerade bei der Integration des Risikomanagements in das Unternehmens-Managementsystem das Arbeiten mit Indikatoren, welche die Zielerreichung der verschiedenen Managementprozesse messen, von grosser Bedeutung.

Im Gegensatz zu den sog. „Key-Performance-Indikatoren“ (KPI), welche das positive Erreichen von Prozess-Zielen der Managementprozesse messen, geben die sog. „Key-Risk-Indikatoren“ (KRI) Auskunft über das Nichterreichen von Prozesszielen oder über das Ergebnis von solchen Prozessen, die ausschliesslich der Risiko-Erkennung und -Bewältigung dienen.

Praxistipp:

Key-Risk-Indikatoren werden vorteilhaft zur Risikosteuerung eingesetzt, d.h. zum zeitgerechten Einsatz von angemessenen und wirksamen Massnahmen.

Aufgrund ihres Verwendungszweckes können die Key-Risk-Indikatoren auch in „Nachlaufende Indikatoren“ und „Vorlaufen-

de Indikatoren“ unterteilt werden. Wobei die nachlaufenden Indikatoren der Risikoerkennung ex-post, d.h. zur Auswertung erfolgter Ereignisse mit und ohne Schadensauswirkung dienen.

Hingegen erlauben die vorlaufenden Indikatoren ex-ante vorausschauend die Zustände zu analysieren und Prognosen zur Prävention und angemessenen Vorkehrungen zu treffen. Die Ergebnisse von Indikatoren können in geeigneter Weise, z.B. durch Kaskadierung, aggregiert werden.

Bei den quantitativen Indikatoren ist noch zu unterscheiden, ob sie einen Absolutwert abgeben, der mit anderen Absolutwerten verglichen werden kann oder ob sie einen auf eine Bezugsgrösse normierten relativen Wert angeben.

2.9

Risiko-Organisation, Kategorien und Arten von Risiken

Das Risikomanagement in einem Unternehmen bedarf einer hohen Systematik, gilt es doch, die wesentlichen Risiken zu erkennen und die Gegenmassnahmen effektiv einzusetzen. Bei der Risiko-Behandlung müssen zudem auch Chancen sowie die mit den Gegenmassnahmen allenfalls einhergehenden Chancen-Behinderungen (z.B. durch Verlangsamung der Betriebsprozesse) berücksichtigt werden.

Prinzip der Wesentlichkeit

Dabei ist das Risikomanagement weniger dem Prinzip der Vollständigkeit als dem Prinzip der Wesentlichkeit verpflichtet [Brüh03, 110]. Geht es doch in erster Linie darum, die Risiken nach Prioritäten, vorab die existenzbedrohenden, mit geeigneten Massnahmen zu bewältigen.

Dringlichkeit und Wichtigkeit von Massnahmen

Für die Planung der Massnahmen-Umsetzung ist die Einordnung der Risiken nach „Dringlichkeit“ und „Wichtigkeit“ nützlich, wobei die häufig auftretenden wichtigen Schadensereignisse oder die Ereignisse, deren Schäden sich bei jedem erneuten Auftritt vergrössern (z.B. Reputationsschäden*), allenfalls dringlicher zu bewältigen sind als grosse Risiken, die sich selten ereignen.

Angemessenheit der Massnahmen

Dem Aspekt der Angemessenheit der Massnahmen, mitunter auch aus Kostensicht, wird am besten Rechnung getragen, wenn die Risiken in den jeweiligen Verantwortungsbereichen selbst identifiziert und, wenn möglich, auch bewältigt werden. Der Wesentlichkeit gehorchend, wird sich die oberste Geschäftslei-

* Reputationsschäden bei Kunden und Geschäftspartnern entstehen meist infolge berechtigter oder unberechtigter Kommunikation negativer Informationen.

tung um die grössten (10 bis 20) Risiken direkt kümmern. Die untergeordneten Geschäftsbereiche und Organisations-Einheiten werden sich vor allem den Risiken in ihren Verantwortungs-bereichen und an den Schnittstellen zu anderen Verantwortungs-bereichen annehmen. Ein solcher Ansatz ist sinnvoll, weil er der Kongruenz von Risiken und Kosten mit dem jeweiligen Verant-wortungsbereich Rechnung trägt.

Verantwortungs-bereich für Risi-ken und Kosten

Top-Down-Vorgehen

Zudem wird das Berichten von einer Flut von zum Teil fachspe-zifischen Risiken an höhere Unternehmens-Ebenen eingedämmt, da die Bewältigung in „stufengerechter“ Verantwortlichkeit de-zentral durchgeführt wird. Jeder Bereich hat somit seine eigene „Risiko-Ownership“ und sein eigenes Risiko-Portfolio, und nur die grössten Risiken erscheinen im Portfolio des jeweiligen Ge-schäftsfeldes oder des Gesamtunternehmens. Einer solchen „Ri-siko-Organisation“ liegen auch, wie im Teil D des Buches gezeigt wird, von oben nach unten ineinandergreifende Risiko-management-Prozesse zu Grunde.

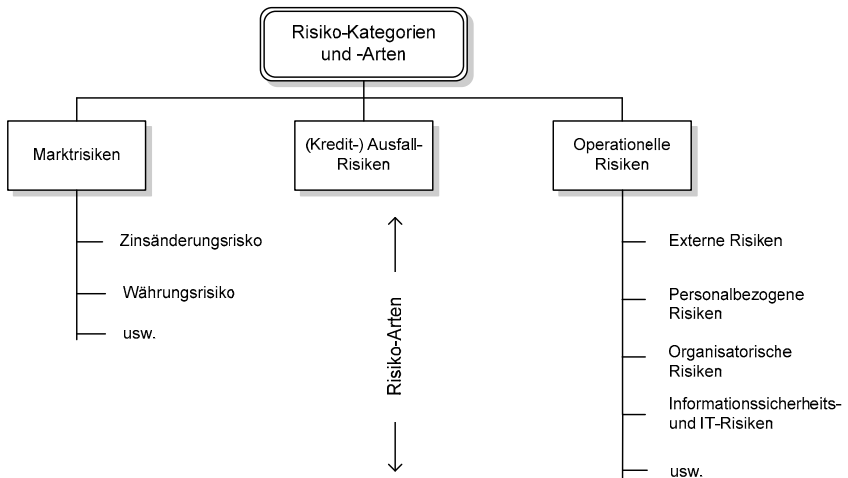


Abbildung 2.11: Beispiel von Risiko-Kategorien und -Arten einer Bank

Risiko-Kategorien und Risiko-Arten

Ähnlich der Kosten-Arten bei der Buchführung, bedarf es beim Risikomanagement einer Unterteilung in Risiko-Kategorien und Risiko-Arten, um die spätere Übersichtlichkeit bei der Erfassung und Bewältigung gewährleisten zu können. In der Abbildung 2.13 sind verschiedene Risiko-Arten ([Witt99], 474)] wie „Finanz- risiken“ oder „Projektrisiken“ aufgeführt. Eine solche Zusammen- stellung könnte für ein Unternehmen in der Nahrungsmittel- Branche sinnvoll sein. Für eine Bank fällt eine Zusammenstel-

lung der Risiko-Arten erheblich anders aus (s. Abbildung 2.11). Die Bildung von Risiko-Kategorien und Risiko-Arten hängt stark von der Branche, den Geschäften, Märkten und anderen Parametern eines Unternehmens ab. Die auf der Ebene des Gesamt-Unternehmens grob definierten Risiko-Kategorien und Risiko-Arten werden auf der Ebene der untergeordneten Organisationseinheiten (z.B. einer Abteilung oder eines Geschäftsprozesses) meist noch verfeinert. Abbildung 2.12 zeigt Beispiele von Faktoren, die auf die Bildung von Risiko-Arten in einem Unternehmen Einfluss nehmen.

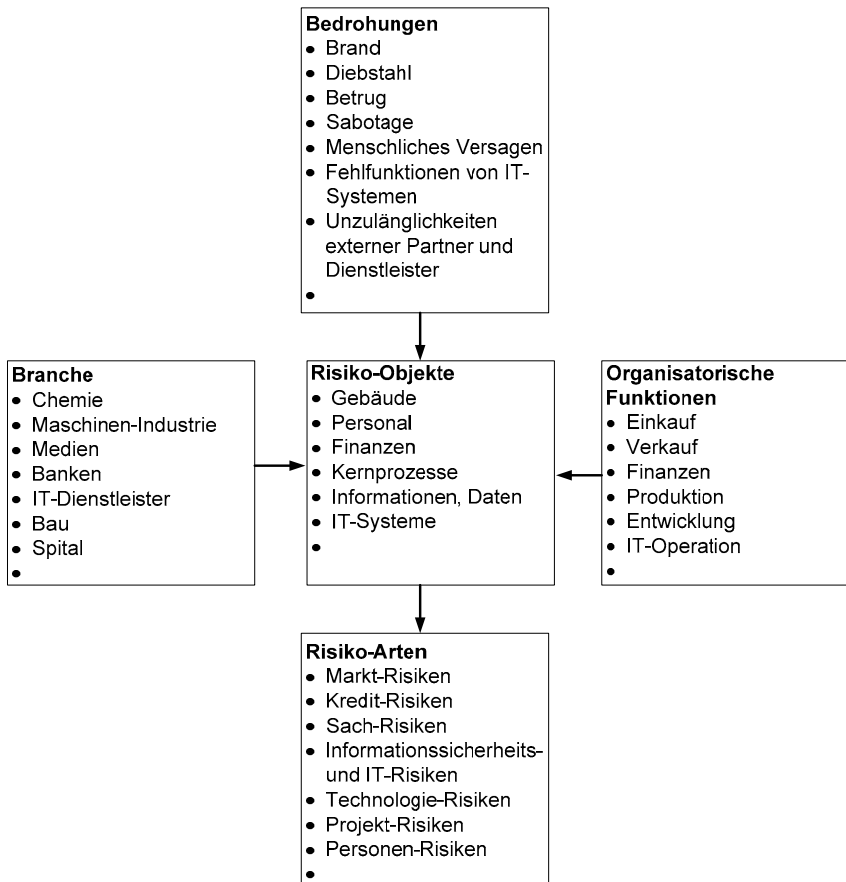


Abbildung 2.12: Faktoren zur Definition von Risiko-Arten (vgl. [Romi03, 167])

2.9.1

Bedrohungslisten

Wie aus der Abbildung 2.12 ersichtlich ist, spielen bei der Definition von Risiko-Arten auch die für ein Unternehmen relevanten Bedrohungen eine grosse Rolle. Um die Risiko-Analysen möglichst rationell durchführen zu können, ist es nützlich, die typischen Bedrohungen pro Risiko-Art in einer Liste zusammenzustellen; dabei sind sowohl innere als auch äussere Konstellationen und Einflüsse zu berücksichtigen.

Anpassung der Bedrohungslisten

Wickelt beispielsweise ein Unternehmen Geschäfte und Dienstleistungen über das Internet ab, dann muss die so genannte „Denial of Service Attacke“ auf die Bedrohungsliste für die IT-Risiken aufgenommen werden. Oder ist ein Unternehmen stark von Export abhängig, dann sind die Wechselkurseinflüsse auf die Bedrohungsliste für die Risiko-Art „Finanzrisiken“ aufzunehmen. Die Bedrohungslisten müssen ständig an die Veränderungen in einem Unternehmen angepasst werden.

Da die Bildung von Risiko-Arten stark von der Branche und auch vom einzelnen Unternehmen abhängig ist, sollen die im nächsten Abschnitt gezeigten Risiko-Arten lediglich als Beispiele verstanden werden.

2.9.2

Beispiele von Risiko-Arten

Abweichungen von System-Zielen

Entsprechend der in Abschnitt 2.2 vorgenommenen Risikodefinition werden in Abbildung 2.13 anhand von Beispielen der jeweiligen Risikoart die für die Risiken verantwortlichen „Abweichungen von System-Zielen“ sowie eine Liste mit den „ursächlichen Bedrohungen“ zugeordnet.

Bedrohungs-motivation und Angriffsmittel

Für Risiken aufgrund von „beabsichtigten“ Bedrohungen, wie sie beispielsweise durch Angriffe im „Cyber Space“ vorkommen, empfiehlt sich eine Aufschlüsselung nach der auf die Impacts abzielenden „Bedrohungsabsicht“ (z.B. Imageschädigende Kampagnen, Betrug, Sabotage) einerseits und die für die Gegenmassnahmen relevanten „Angriffsmittel“ (z.B. Soziale Netzwerke, Phishing, Malware*) andererseits (s. Anhang A.2).

Eine Zusammenstellung von Risiko-Arten, wie sie beispielsweise in Unternehmen der industriellen Fertigung, der Chemie- oder

* Malware = Schadprogramme wie Trojaner, Spyware, Computer-Viren und -würmer.

Nahrungsmittelbranche vorkommen können, ist im Anhang A.1 dieses Buches aufgeführt.

Finanzrisiken	Abweichungen von System-Zielen	Bedrohungslisten
	• Gewinneinbussen/Verluste • Schwacher Cash-Flow • Geringer Deckungsbeitrag • Schwierigkeiten bei der Finanzmittelaufnahme •	• Zinsänderung • Bonitätsverschlechterung einer Gegenpartei • Eigene Bonitätseinbüsse • Kursrisiken •
Sachrisiken	Abweichungen von System-Zielen	Bedrohungslisten
	• Betriebsbehinderungen • Produktionsausfälle • Sachbeschädigungen • Ressourcenschwund •	• Brand • Terror • Betrug • Unterschlagung • Sabotage • Vandalismus • Technische Fehler • Wassereinbruch • Versorgungsengpässe (Wasser, Strom, Energie) •
Informationssicherheits-Risiken	Abweichungen von System-Zielen	Bedrohungslisten
	• Verlust Integrität • Verlust Verfügbarkeit • Verlust Vertraulichkeit	• Maskerade einer Benutzer- oder System-Identität • Manipulieren/Infiltrieren von Informationen • Abhören von Informationen • Denial of Service Attacke • Einschleusen schädlicher / störender Software • Missbrauch / Lahmlegen von Systemressourcen • Diebstahl von Daten oder System-Ressourcen • Absichtliche Beschädigung • Benutzerfehler • Betriebsfehler • HW & SW – Fehler • Fehlfunktionen • Naturkatastrophen •

Abbildung 2.13 Beispiele von Risiko-Arten

2.10**Zusammenfassung**

Risikomanagement setzt sich hauptsächlich aus „Identifikation“, „Analyse“, „Bewertung“, „Bewältigung“ und „Überwachung“ von Risiken in einem vorbestimmten Kontext zusammen; es dient der Erarbeitung und Umsetzung von Massnahmen für ein akzeptables Restrisiko sowie der Risikokontrolle.

Die im Zusammenhang mit Unternehmens-Risiken sinnvolle betriebswirtschaftliche Definition lautet: „Ein Risiko ist eine nach Häufigkeit und Auswirkung beurteilte Bedrohung eines zielorientierten Systems.“ Die Zielabweichungen sind dabei die unerwünschten Abweichungen von Ziel-Vorgaben bezüglich Kosten, Qualität, Termin, Integrität usw., wobei die Folgen dieser Ziel-Abweichungen den Schaden darstellen.

Zur Durchführung der Risiko-Bewertung im Rahmen einer Risiko-Analyse verwenden wir eine Reihe vorbereiteter Instrumente wie eine Risiko-Matrix und eine Schadens-Einstufungstabelle. Zur Analyse der ursächlichen Bedrohungen der Objekte benützen wir für jede Risiko-Art eine vorgefertigte Bedrohungsliste.

Mittels eines Katalogs führen wir Buch über die einzelnen vorhandenen Risiken und fassen diese zusammen. Die Zusammenfassung erfolgt nicht durch Addition, sondern durch Aggregation, wobei die Abhängigkeiten (Korrelationen) zwischen den einzelnen Risiken zu berücksichtigen sind. Zur Berechnung einer Gesamtverlustposition im Unternehmen ist die Aggregation der Risiken notwendig.

Trotz der Schwierigkeiten bei der Risiko-Aggregation können wir die Risiken auf Unternehmensebene zur Massnahmenbestimmung und -überwachung zumindest „konsolidieren“, indem die ordinal eingestuften Risiken in einem Risikokatalog nach ihrer Höhe absteigend und ihren Abhängigkeiten untereinander eingeordnet werden. Die Korrelationen zwischen den Risiken werden dabei mit heuristischen Methoden festgestellt und im Risiko-Katalog entsprechend vermerkt. Ein solcher Katalog eignet sich zur Bestimmung und Umsetzungs-Überwachung der bei operationellen Risiken im Vordergrund stehenden Gegenmassnahmen und gibt die diesbezügliche Risikosituation im Unternehmen wieder.

Für die Planung der Massnahmen-Umsetzung ist die Einordnung der Risiken nach „Dringlichkeit“ und „Wichtigkeit“ nützlich. Die „Risiko-Landschaft“ und die Strategien der „Risiko-Bewältigung“ veranschaulichen und kommunizieren wir mittels der „Risiko-

Portfolio“-Darstellung. Für die typischen Risiken in einem Unternehmen definieren wir Risiko-Arten, diese sind bei einer Bank beispielsweise in die Kategorien „Marktrisiken“, „Kreditrisiken“ und „Operationelle Risiken“ eingeteilt.

2.11

Kontrollfragen und Aufgaben

1. Wie lautet die Risikoformel für ein einzelnes Risiko?
2. Wie lautet die verbale Risikodefinition für betriebswirtschaftliche Fragestellungen?
3. Wie ist die Risikoformel für den Erwartungswert definiert?
4. Was sind die möglichen Probleme mit den einfachen Risikoformeln?
5. Aufgrund welcher Kriterien erfolgen die Schadenseinstufungen?
6. Welche Nachteile können kardinale Risiko-Bewertungen haben?
7. Ermitteln Sie das Risiko mit Hilfe der Risiko-Matrix in Abbildung 2.4 bei einem katastrophalen Schaden mit einer Häufigkeit „selten“. Ermitteln Sie das Risiko bei einem katastrophalen Schaden auch für die Häufigkeiten „oft“ und „sehr selten“. Was stellen Sie fest? Begründen Sie.
8. Welche Elemente enthält ein Risiko-Katalog?
9. Zu welchen Zwecken wird ein Risiko-Portfolio erstellt?
10. Welche Bewandnis hat die „Akzeptanzlinie“?
11. Welche beiden Dimensionen enthält das gebräuchliche „Risk Map“ zur Darstellung eines Risiko-Portfolios?
12. Nennen Sie die Koordinaten eines alternativen Risiko-Portfolios, das auch den „unerwarteten Verlusten“ Rechnung trägt.
13. Benennen und erklären Sie geeignete „Stochastische Risikomasse“ für „unerwartete Verluste“ und für „katastrophale Verluste“.
14. Zu welcher Risikokategorie gehören die Informationssicherheits- und IT-Risiken?

Nachdem in den vorangegangenen Kapiteln wesentliche Elemente, Definitionen und Hilfsmittel für das Risikomanagement erarbeitet wurden, wenden wir uns nun dem allgemeinen Prozess des Risikomanagements zu. Ein der Komplexität und Dynamik heutiger Risikosituationen angepasster Risiko-Management-Prozess ist als inhärent rekursiv, d.h. mit bedarfsgesteuerten Rückkopplungen, und nicht als rigide Abfolge einzelner Aktivitäten zu verstehen.

In dieser Eigenschaft soll der Prozess ein aktuelles, umfassendes und situationsgerechtes Verständnis der Risiken für die Anspruchsgruppen (Eigentümer, Mitarbeiter, Kunden etc.) und Entscheidungsträger liefern sowie gewährleisten, dass sich die Risiken innerhalb von akzeptierten Grenzen bewegen.

Die Grundstruktur dieses im Folgenden behandelten Prozesses wird an den derzeit verfügbaren Standards über Risikomanagement wie dem ISO Guide 73 [IsoV09], sowie den Standards ISO 31000 [IsoR09] und ISO/IEC 27005 [IsoI11] ausgerichtet.

RM-Prozess hat Modellcharakter

Ein solcher RM-Prozess (s. Abbildung 3.1) ist generisch und hat für sämtliche betrieblichen Risikomanagement-Probleme Modell-Charakter. Er wird sowohl auf der Ebene des Gesamt-Unternehmens eingerichtet (s. Kapitel 12) als auch für andere untergeordneten Risikomanagement-Prozesse eingesetzt. Beispiele dafür sind das in Abschnitt 10.1 behandelte IT-Sicherheitskonzept oder das im Abschnitt 13.2 beschriebene Geschäftskontinuitäts-Management.

Teil-Prozesse

Die Aufgaben, Verantwortlichkeiten und Verfahren innerhalb der einzelnen Schritte sowie die Objekte und Hilfsmittel sind selbstverständlich bei den verschiedenen Prozess-Anwendungen unterschiedlich. Die oben bereits angesprochenen Aufgaben, wie „Kontext-Festlegung“ und „Risiko-Identifikation“ werden als Teil-Prozesse mit Eingang und Ausgang zu einem Gesamtprozess verknüpft.

*Rückkopplungen
Iterationen und
zyklische Wiederholungen*

Durch Rückkopplungen und Iterationen einzelner Prozess-Schritte werden die Ergebnisse der einzelnen RM-Aufgaben verbessert und optimiert. Da sich die Risiko-Situationen in dem zu behandelnden Bereich (z.B. Unternehmen, Geschäft oder System) immer wieder verändern, werden Teile des Prozesses oder auch der gesamte Prozess (z.B. im Rahmen des periodischen Strategiefindungs-Prozesses) zyklisch wiederholt durchlaufen.

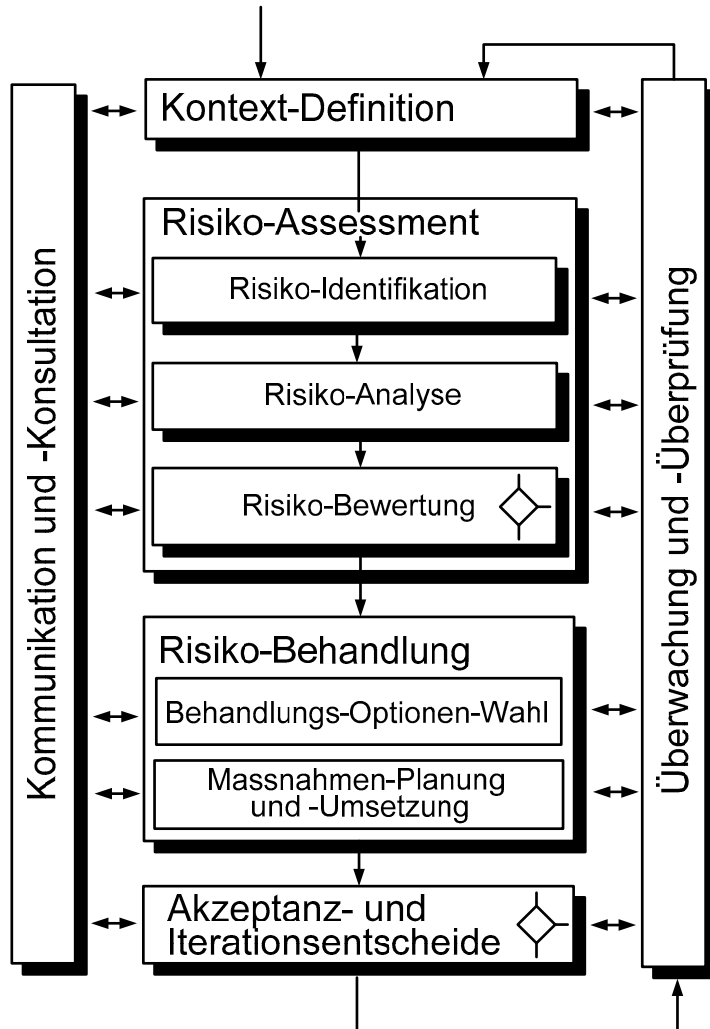
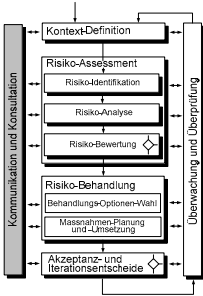


Abbildung 3.1: Allgemeiner Risikomanagement-Prozess

3.1

Kommunikation und Konsultation



Sowohl die direkt Beteiligten in einem Risikomanagement-Prozess als auch die Betroffenen (z.B. Anspruchsgruppen) sind in jedem Teil-Prozess auf einen entsprechenden Informations-Austausch angewiesen. Diese **Kommunikation** dient der Mitteilung, dem Austausch, dem Einbezug sowie der Erläuterung und Erklärung der Aktivitäten und Ergebnisse im gesamten Ablauf des Risikomanagement-Prozesses. Auch ist es unumgänglich, für bestimmte Untersuchungen, Einschätzungen und Entscheide essenzielle Informationen durch **Konsultationen** bei den dafür kompetenten Stellen einzuholen. Oft ist auch die Verifikation oder Ergänzung von Ansichten und Informationen durch eine „second opinion“ angezeigt.

Angemessene und verständliche Kommunikation

Die am Risikomanagement-Prozess direkt beteiligten Personen sind oft verschiedenartige Fachpersonen und Experten, welche ihre Informationen untereinander und mit den Entscheidungsträgern in angemessener und verständlicher Form kommunizieren müssen. Es empfiehlt sich deshalb, an den einzelnen Prozess-Punkten, wo wichtige Informationen (z.B. über die Risiken und ihre Ursachen, ihr Auftreten und ihre Konsequenzen) anfallen oder unmissverständlich weitergegeben werden müssen, entsprechend vorbereitete stark strukturierte Kommunikationsformen einzusetzen, z.B. Formulare oder formulargesteuerte Kommunikations-Systeme.

Kommunikationskonzept

Ein auf die Anwendung zugeschnittenes Kommunikations-Konzept, welches auf alle wesentlichen Schritte im Prozessablauf abgestimmt ist und die Risiko-Wahrnehmung im Unternehmen sowie die unterstützenden Kommunikations-Medien einbezieht, trägt massgeblich zur Qualität der Ergebnisse eines Risikomanagement-Prozesses bei. Auch verhilft eine gute und ausgewogene Risiko-Kommunikation sicherlich zur Verbesserung der Risikokultur, dem Risikobewusstsein und letztlich zur Verbesserung der Risikosituation im Unternehmen.

Unterscheidung interne und Externe Kommunikation

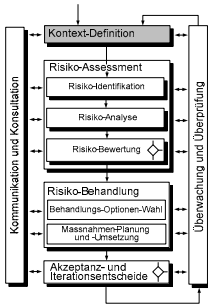
Das Kommunikationskonzept enthält sicherlich einen Teil über die anforderungsgerechte (allenfalls stufengerechte) interne Information und einen anderen Teil über die externe Kommunikation mit externen Medien und Anspruchsgruppen.

Kommunikation im normalen Betriebsablauf und im Notfall

Unterschieden und allenfalls in separaten Konzepten definiert wird das Kommunikationsvorgehen für das Risikomanagement während des normalen Betriebsablaufs und in Notfallsituationen.

3.2

Festlegung Risikomanagement-Kontext



*Gegenstand,
Zweck, Absichten
und Ziele*

*Externe und
interne Unter-
nehmensaspekte*

*Führungs-Aspekte
und organisatori-
sche Festlegungen*

*Risiko-Arten und
System-Ziele*

Zum Beginn des RM-Prozesses legen wir den Behandlungs-Gegenstand*, d.h. den Bereich und die darin befindlichen Systeme und Objekte fest, über die wir das Risikomanagement durchführen werden. Zur Festlegung des Gegenstandes gehört seine Abgrenzung, unter anderem auch die Nennung von Gegenständen, die nicht betrachtet werden. Auch wichtige Einschränkungen und Randbedingungen sind hier aufzuführen.

Der Zweck des Behandlungs-Gegenstandes sowie die Absichten und Ziele des Risikomanagements für diesen Gegenstand sind ebenfalls zu erklären. Dabei wird festgelegt, wessen Risiken zur Behandlung anstehen und für wen und für was das Risikomanagement durchgeführt werden soll.

Wichtig ist auch die Beschreibung wesentlicher Aspekte der externen und internen Umgebung des betrachtenden Gegenstandes. Ist der zu betrachtende Gegenstand ein Unternehmen, dann gehören zur externen Umgebung beispielsweise Aspekte wie Gesellschaft, Natur, Technologie und Wirtschaft und vor allem die resultierenden gesetzlichen, regulatorischen und vertraglichen Bedingungen. Zu den internen Aspekten gehören Normen, Werte, Ressourcen sowie die internen Anliegen und Interessen.

Zum Kontext gehören auch Führungs-Aspekte und organisatorische Festlegungen, wie organisatorische Strukturen und zugeordnete Verantwortlichkeiten, Budgetbeschränkungen, Dokumentationsvorgaben, Berichterstattungs- und Eskalationswege und wichtige Termine. Und nicht zuletzt sind die für den Behandlungsgegenstand relevanten wichtigen Ziele der Geschäfts- und Support-Prozesse (z.B. IT-Prozesse), einschliesslich der im Risikomanagement zu verfolgenden generellen Ziele.

Im Rahmen des definierten Kontextes werden nun die relevanten Risiko-Arten festgelegt. Solche Risiko-Arten sind beispielsweise Finanzrisiken, Sachrisiken und die in diesem Buch speziell the-

* Der Begriff „Gegenstand“ wird in diesem Buch synonym zu „Objekt“ sowohl für greifbare als auch für abstrakte Güter, Objekte und Strukturen verwendet und schliesst den in der englischsprachigen Standardisierung oft verwendeten Begriff „Asset“ ein. Solche Gegenstände können beispielsweise die für das Unternehmen lebenswichtigen Geschäftsprozesse sein.

Festlegung Bewertungskriterien und -massstäbe

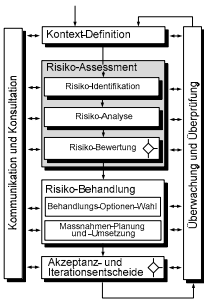
„Risiko- und Sicherheits-Politik“ für wichtigste Kontext-Elemente

matisierten Informationssicherheits- und IT-Risiken. Für die einzelnen Risiko-Arten können nun die im Rahmen des Kontextes massgeblichen System-Ziele zur Risiko-Analyse bestimmt werden. Ein solches System-Ziel ist beispielsweise die Wahrung der Vertraulichkeit von Informationen in den Geschäftsprozessen. (Im Anhang A.1 sind Beispiele von Risiko-Arten und System-Zielen zusammengestellt). Sodann werden die Bewertungskriterien und -massstäbe für die im Prozess später folgende Risiko-Bewertung festgelegt (s. Abschnitt 2.6). Da die Bewertungskriterien (z.B. Akzeptanzkriterien) meist auf bestimmten Methoden zur Risiko-Beurteilung (Risiko-Assessment-Methode) basieren, sind die anzuwendenden Methoden, zumindest im groben Ansatz, bereits bei Kontext-Behandlung festzulegen und zu kommunizieren.

Die wichtigsten generellen Kontext-Elemente auf Unternehmens-Ebene werden mittels einer „Risiko-Politik“ festgehalten und kommuniziert. Für wichtige Behandlungsgegenstände im Unternehmen werden auch entsprechend untergeordnete spezifische „Risikomanagement-Prozesse“ mit ihrem eigenen Kontext definiert, z.B. für einzelne Geschäftsfelder, für die Geschäftskontinuität oder für die Informationssicherheit. Es empfiehlt sich, auch für die untergeordneten Risikomanagement-Prozesse die wichtigsten Kontext-Elemente mit entsprechenden „Policies“ vorzugeben.

3.3

Durchführung Risiko-Assessment



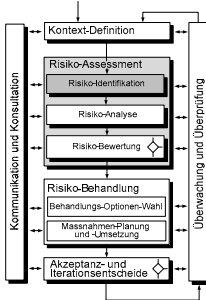
Risiko-Assessment

Unter dem Begriff „Risiko-Assessment“ (Risiko-Beurteilung) werden in der heute gültigen ISO-Standardisierung [IsoV09] alle Aufgaben der drei Teilprozesse „Risiko-Identifikation“, „Risiko-Analyse“ und „Risiko-Bewertung“ zusammengefasst. Wie wir im Rahmen dieses Buches immer wieder feststellen können, werden die Aktivitäten des Risiko-Assessment und auch dessen Teilprozesse stark rekursiv durchlaufen, d.h. dass aufgrund der in den Einzelschritten gewonnenen Erkenntnisse die Teilprozesse oder Prozessschritte wiederholt durchlaufen werden. Aber auch Rückkopplungen zur Korrektur oder Erweiterung des Kontextes, z.B. Erweiterung der Risikoarten oder Erweiterung oder Anpassung der zu verwendenden Assessment-Methoden sind oft angezeigt.

Die Methoden, mit denen die Risiken ermittelt und aus Unternehmenssicht bewertet und beurteilt werden können, sind vielfältig und es gilt, für die konkrete Risikosituation die geeigneten Methoden anzuwenden. Im Standard ISO/IEC 31010 ist eine Übersicht über mögliche Assessment-Methoden zu finden

[Isoa09]. Wie die einzelnen Methoden zeigen, ist eine strikte Trennung der Aufgaben für Identifikation, Analyse oder Bewertung nicht immer möglich. So können einzelne Assessment-Methoden sowohl für die Identifikation als auch für die Analyse oder gar für die Bewertung eingesetzt werden. Als Ergebnis soll der Assessment-Prozess die Informationen darüber liefern, wo sich Risiken befinden, wie sie zu verstehen sind und wie damit, unter anderem auch hinsichtlich einer Akzeptanz, umgegangen werden soll. Für den als Problemlösungsprozess verstandenen RM-Prozess bedeutet dies aber auch, dass aufgrund von Assessment-Ergebnissen die rekursive Modifikation von Kontext-Bedingungen jederzeit möglich sein muss.

3.4



Risiko-Identifikation

Am Anfang des Assessment-Prozesses steht die „**Risiko-Identifikation**“, mit der wir möglichst systematisch alle relevanten Risiken eines Unternehmens oder eines Teilbereichs (z.B. Abteilung, Geschäftsprozess oder System) identifizieren. Dabei ist es empfehlenswert, neben den Risiken innerhalb der getroffenen Assessment-Abgrenzung auch Risiken oder deren Quellen ausserhalb zu identifizieren, die allenfalls Einfluss haben könnten. Die Erfassung der Risiken soll zwar dem Prinzip der Vollständigkeit, aber auch dem Prinzip der Wesentlichkeit gehorchen, deshalb werden Verfahren, die nach Risiken vom „Groben“ ins „Feine“ fahnden, bevorzugt. Dabei umfasst der Prozess der Identifikation die möglichst vollständige Erfassung der signifikanten Gefahrenquellen und möglichen Konsequenzen auf die Risiko-Objekte* im betrachteten Gebiet. Ist das betrachtete Gebiet ein ganzes Unternehmen, dann wird das Gebiet in einzelne Risiko-Kategorien und Risiko-Arten unterteilt (s. Abschnitt 2.9). Die Risiko-Objekte werden vorzugsweise in der folgenden Weise definiert, granularisiert[†] und logisch geordnet:

- wie sich die Bedrohungen auf sie auswirken und zu entsprechenden Schadensereignissen führen können und
- wie den Risiken sinnvolle Massnahmen entgegengesetzt werden können.

* Risiko-Objekte (Assets) können Prozesse, Systeme, Systemkomponenten, Informationen, Lokalitäten, Personen oder Projekte sein.

[†] Durch die Granularisierung wird eine für die Analyse und Massnahmendefinition sinnvolle Objektgrösse definiert.

Zu a):

Ausgehend von den Bedrohungen und den Schwachstellen an den betrachteten Risiko-Objekten soll die Identifikation alle relevanten Ursachen-Wirkungsketten für die verschiedenen Impact-Arten erfassen.

Das Identifizieren von Bedrohungen kann mit Hilfe vorgefertigter Bedrohungslisten erleichtert werden. Die Identifikation von Schwächen (Schwachstellen) kann u.a. anhand von Sicherheitsstandards, Vorschriften, Regulationen oder Gesetzen erfolgen.

Die Relevanz von Bedrohungen und Schwachstellen hängt mitunter von den für das zu ermittelnde Risiko massgeblichen System-Zielen ab.

Zu b):

Die Risiken können in unterschiedlichen Konsequenzarten (z.B. technisch oder finanziell) und Zusammenfassungen (Aggregations-Niveaus) ausgewiesen werden. Die anzustrebenden Massnahmen sollen auf die zusammengefassten Risiken wirken können.

In den Abschnitten 10.2, 10.4 und 10.5 wird an konkreten IT-Beispielen gezeigt wie mit geeigneten Strukturen (z.B. CRAMM* Asset-Modell, Fehlerbäume oder Ereignisbäume), die Risiko-Objekte für eine Risiko-Analyse zweckmässig geordnet werden können.

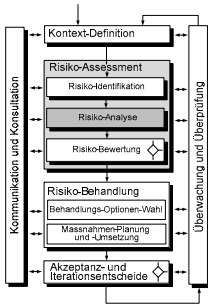
*Aufsuchen bereits
existierender
Massnahmen*

Zur Identifikation gehört auch das Feststellen von bereits existierenden Massnahmen und der an den einzelnen Risiko-Objekten vorhandenen Stärken und Schwächen.

* CRAMM (= Centre for Information Systems Risk Analysis und Management Method)

3.5

Risiko-Analyse



Sind die relevanten Risiken identifiziert, dann dient die „**Risiko-Analyse**“ dem tieferen Verständnis der Risiken und liefert die Ergebnisse über deren Ausprägung und Höhe in Grössen für die Wahrscheinlichkeit (Häufigkeit) sowie dem Schadensausmass (Schadensfolgen) für jede Zielabweichung eines Schadensereignisses. Dabei gehen die „Bedrohungen“, „Schwachstellen“ und der „Wert der Risiko-Objekte“ als Faktoren in die Bestimmung (ex-ante) der beiden Risiko-Variablen „Wahrscheinlichkeit (Häufigkeit)“ und „Schadensausmass“ ein. Die Schwachstellen können aufgrund der bereits vorhandenen Massnahmen und deren Effektivität in Bezug auf das Risiko-Objekt abgeschätzt werden. Zusätzlich oder alternativ können die beiden Risiko-Variablen „Wahrscheinlichkeit (Häufigkeit)“ und „Schadensausmass“ auch aus historischen Aufzeichnungen gewonnen werden (ex-post). Sind die beiden Variablen mit ihren Werten resp. ihren Wahrscheinlichkeitsverteilungen gefunden, dann werden sie in geeigneter Weise zu einem Risiko-Wert resp. Risikomass „kombiniert“, wie dies im Abschnitt 2.8 anhand einiger Varianten gezeigt wurde. Neben diesen klassischen Möglichkeiten, das Risiko auszudrücken, kann es auch mit Indikatoren gemäss Abschnitt 2.8.2 oder mit den Ergebnissen aus Teilanalysen gemäss Abschnitt 3.5.1 ausgedrückt werden.

Quantitative oder qualitative Risiko-Analyse

Entsprechend der gestellten Anforderungen kann die Risiko-Analyse „quantitativ“ oder „qualitativ“ durchgeführt werden. Die „quantitative“ Analyse liefert numerische Werte einer Kardinal-Skala. Die qualitative Analyse unterscheidet sich von der quantitativen Analyse dadurch, dass der Schaden und die Häufigkeit nicht mit absoluten numerischen Grössen, sondern mit verbalen Aussagen beschrieben werden. Um letztendlich rationale Risiko-Bewertungen durchführen zu können, müssen jedoch auch die verbalen Risiko-Beschreibungen einem geeigneten Skalensystem unterworfen werden. Ein dafür gebräuchliches Skalensystem ist die Ordinalskala (sehr gross, gross, mittel usw.).

Semi-quantitative Analyse

Werden einer solchen Ordinalskala zusätzlich noch numerische Werte zugeordnet, dann wird die mit einer derartigen Skala durchgeführte Analyse als „semi-quantitativ“ bezeichnet (vgl. [Asnz04], S. 18). Berechnungen aufgrund „semi-quantitativer“ Analysen sind mit Vorsicht zu behandeln, da ihre numerischen Aussagen unter Umständen nicht vorhandene Genauigkeiten vortäuschen können.

Zusätzlich zu diesen primären, die Risikohöhe beschreibenden Ergebnissen werden, entsprechend dem Zweck der Analyse, eine Vielzahl sekundärer Ergebnisse und „Risiko-Attribute“, wie „Dringlichkeit“ oder Ursachen- und Szenarienbeschreibung, erwartet.

3.5.1

Teil-Analysen

Die Art des Ergebnisses einer Risiko-Analyse richtet sich vor allem nach ihrem Zweck und den vorliegenden Gegebenheiten. Ist es beispielsweise nicht möglich oder nicht erforderlich, sowohl die Häufigkeit als auch die Schadensfolgen eines Ereignisses zu analysieren, dann können auch Teil-Analysen durchaus sinnvolle Ergebnisse liefern.

Teil-Analysen

Solche Teil-Analysen sind:

1. Bedrohungs-Analyse (Analyse der relevanten Bedrohungen)
2. Schwächen-Analyse (Analyse der relevanten Schwachstellen)
3. Impact-Analyse (Analyse der potentiellen Schäden)
4. Beliebige Kombination der Analysen 1 bis 3

Die Kombination der Teil-Analysen 1 bis 3 liefert das Ergebnis einer vollen Risiko-Analyse.

3.5.2

Bedrohungs-Analyse

Bedrohungs-Analyse

Die Bedrohungs-Analyse zeigt die für ein Objekt (Asset) relevanten Bedrohungen auf. Bedrohungs-Analysen werden vor allem dann durchgeführt, wenn entsprechende Entscheide, meist strategischer Art anstehen, z.B. Standortwahl für ein neues Rechenzentrum oder Eröffnung einer neuen Produktlinie. Bei der Bedrohungsanalyse werden lediglich die Bedrohungen, welche die Assets beeinträchtigen könnten, identifiziert und allenfalls nach einem gewählten Wertemassstab analysiert und bewertet. Findet ein numerischer Wertemassstab Verwendung, dann wird damit nicht ein absolutes Analyse-Ergebnis, sondern meist ein Vergleich zwischen alternativen Varianten angestrebt.

Bei strategischen Entscheiden werden meist nicht nur die Bedrohungen, sondern mit ähnlichen Wertemassstäben auch die mit der betrachteten Variante möglichen Chancen sowie die für das Eingehen der Variante zu betrachtenden operationellen Stärken und Schwächen analysiert. Dieses als „SWOT-Analyse“ bekannte

und für die Strategiefindung nützliche Verfahren deckt jedoch keinesfalls die Anforderungen an eine Risiko-Analyse ab, da die Werte der durch die Bedrohungen beeinträchtigten Objekte (Assets) nicht in das Verfahren eingehen.

3.5.3

Schwächen-Analyse

Zeitaufwändige Risiko-Analyse

Wie die bisherigen Ausführungen zeigten, ist die Durchführung einer vollen Risiko-Analyse in der Regel umfangreich und zeitaufwändig. Dazu kommt, dass die Risiko-Analyse eines grösseren Bereichs, z.B. eines ganzen Unternehmens oder eines grösseren Geschäfts- oder Unterstützungs-Prozesses, nicht durch externe Experten alleine durchgeführt werden kann, sondern der intensiven Mitarbeit der betriebsinternen Verantwortlichen und Wissensträger bedarf. Dabei ist es insbesondere für die Analyse der bedrohten Assets und des Schadensausmasses notwendig, die internen Wissensträger des Geschäftsfeldes und der Geschäfts-Prozesse einzubeziehen. Weiter werden für die Analyse der Bedrohungen, Schwachstellen sowie für das Aufstellen entsprechender Szenarien die Fachleute der Unterstützungs-Prozesse (z.B. der IT) benötigt. Bei einer Auslagerung (Outsourcing) der Unterstützungsprozesse muss gar mit zusätzlichem Aufwand auf beiden Partnerseiten gerechnet werden.

Schwächen- Analyse

Ein weniger aufwändiges und deshalb häufig verwendetes Verfahren ist die Schwächen-Analyse. Mit der Schwächen-Analyse (auch Schwachstellen-Analyse) werden die Schadensauswirkungen und die Eintritts-Wahrscheinlichkeiten nicht analysiert, da dazu die konkreten Kausalketten der Bedrohungsauswirkungen auf die Objekte und die Objektbewertungen fehlen.

Schwachstellen- Bewertungs- prozess

Wird ein Objekt einer Schwächen-Analyse unterzogen, dann werden zwar, wie bei der Risiko-Analyse, anhand von vorgefertigten Bedrohungslisten die bedrohten Objekte identifiziert. Doch werden beim nachfolgenden Schwachstellen-Bewertungsprozess die zu analysierenden Objekte lediglich auf das Vorhandensein von inhärenten Schwächen gegenüber den Bedrohungen sowie das Fehlen der gegen diese Bedrohungen üblichen Massnahmen untersucht.

Einschätzung der Schwachstelle

Mit der Schwächen-Analyse (oder Schwachstellen-Analyse) werden die Schwachstellen an den zu untersuchenden Gegenständen ermittelt. Sie setzt das Vorhandensein von typischen Bedrohungen in einem bestimmten Analysegebiet voraus (z.B. Analysegebiet „Internet-Zugriff“). Die Einschätzung der Schwach-

stelle wird meist aufgrund von allgemein bekannten möglichen Konsequenzen vorgenommen.

Schwachstellen-Kataloge

Die Schwachstellen-Kataloge werden in ähnlicher Weise wie die Risiko-Kataloge angefertigt. Dabei können die Schwachstellen, wie bei der Risiko-Analyse, bezogen auf die Objekte (Assets) aufgeführt werden. Sinnvoll ist auch, die für eine Schwachstelle relevanten Bedrohungen aufzuführen. Anstelle der Risiko-Einschätzung kann beispielsweise auch eine ordinale oder gar numerische Einschätzung der Schwäche anhand eines entsprechenden Wertemassstabes ermittelt und ausgewiesen werden. Wie bei der Bedrohungs-Analyse dürfen die Ergebnisse nicht als absolute Werte interpretiert werden.

Vorgelagerte Schwachstellen-Analyse

Die Schwachstellen-Analyse wird oft, zusammen mit einer Bedrohungs-Analyse, einer „vollen Risiko-Analyse“ vorgelagert durchgeführt. Mit einem solchen zweistufigen Analyse-Verfahren, wird vor allem die Komplexität der „vollen Risiko-Analyse“ verringert, indem die für die Risiko-Analyse notwendige Einschätzung der Bedrohungsauswirkungen auf die Objekte aus der vorgängig durchgeführten Schwachstellen-Analyse hergeleitet werden kann.

Schwächen-Analyse

Wenn auch die Schwächen nur unter der Voraussetzung konkreter Bedrohungen und Schadenspotentiale zu einem wirklichen Risiko führen, kann eine Schwächen-Analyse ohne vollständige Risikoeinschätzung dennoch sinnvoll sein; nämlich dann, wenn bei einem bestimmten Bedrohungsumfeld und bei Annahmen von möglichen Schadenspotentialen die Schwachstellen (Verletzlichkeiten) herauszufinden sind, an denen „normalerweise“ Schäden entstehen könnten. Die Schwachstellen-Analyse greift dabei stark auf die Erfahrungen mit bereits bestehenden Massnahmen zurück (Best Practices oder Standards). Die Schwachstellen-Analyse zeigt somit auch, wo Massnahmen fehlen und wo allenfalls Massnahmen anzusetzen sind.

Dringlichkeits-Kategorien bei Schwachstellen

Beim Umgang mit Bedrohungen im Bereich des Internets ist es üblich, die Schwachstellen in die folgenden zwei Dringlichkeits-Stufen einzuteilen:

- 1.) **„Vulnerability“** (Verletzlichkeit) lässt gemäss analytischer Überlegungen ein Schadensereignis zu (z.B. ein bekannter Programmfehler könnte unter bestimmten Bedingungen das Einbringen eines Trojanischen Pferdes ermöglichen);
- 2.) **„Exploit“** hat sich durch einen entsprechenden Angriffs-Code als ausnützbare Schwachstelle erwiesen (z.B. Schwach-

stelle in einem Softwareprodukt wird nachweislich durch einen Angriffscod zum Einbringen eines Trojanischen Pferdes ausgenutzt). Meist wird bereits die reine Beschreibung des Angriffscodes als „Exploit“ bezeichnet. Gibt es einen Angriffscod noch am selben Tag, an dem die Schwachstelle bekannt wird, wird dieser als „Zero-Day-Exploit“ bezeichnet.

3.5.4

Impact-Analyse

Wertverluste

Sind die Risiken identifiziert, und die Objekte festgelegt, auf denen die Risiken anfallen, dann können aufgrund der Bedrohungen und Schwachstellen die möglichen Wertverluste ermittelt werden. Die Einschätzung der möglichen Wertverluste wird als „Impact-Analyse“ bezeichnet, wobei die Impact-Analyse lediglich die Schadenshöhe eines Risikos unter Weglassung der Bedrohungs- und Schwachstelleneinflüsse liefert.

Impact-Analyse

Die Impact-Analyse wird oft dann durchgeführt, wenn es beispielsweise darum geht, festzustellen, ob für ein betrachtetes System überhaupt signifikante Risiken vorliegen und ob aufgrund der Höhe der potentiellen Schäden eine vertiefte Risiko-Analyse erforderlich ist. Impact-Analysen sind auch dann notwendig, wenn sich die Schadensfolgen im zeitlichen Verlauf eines Ereignisses stark verändern. Diesem Aspekt muss beispielsweise bei der Geschäftskontinuitäts-Analyse Rechnung getragen werden.

Katastrophale Schadensereignisse

Dann macht eine Impact-Analyse vor allem bei der Absicherung gegen seltene, aber katastrophale Schadensereignisse Sinn, da für das Aufstellen von Geschäftskontinuitäts- oder Notfall-Plänen die Eintritts-Wahrscheinlichkeiten (-Häufigkeiten) wenige Entscheidungsgrundlagen liefern. Hingegen ist das mögliche Schadensausmass in Abhängigkeit von der Ausfall-Zeit wichtig, da ja das mit der Zeit meist ansteigende Schadensausmass mit vorsorglichen Massnahmen reduziert werden soll.

Die Einschätzung des Impacts kann auf eine der folgenden Arten vorgenommen werden:

Maximal

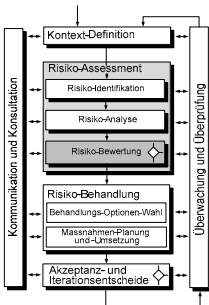
1. Es werden die maximal möglichen Schäden aufgrund von Zielverfehlungen an den einzelnen Risiko-Objekten eingeschätzt. Insbesondere bei der Geschäftskontinuitäts-Planung interessiert die zeitliche Entwicklung eines maximal möglichen Schadens, welcher im Rahmen eines „Worst Case“-Szenarios Rechnung getragen werden soll.

statistisch

2. Es werden durchschnittliche Schäden aufgrund von Zielverfehlungen an den einzelnen Risiko-Objekten erhoben oder eingeschätzt.
3. Die Schäden werden aufgrund von Zielverfehlungen an den einzelnen Risiko-Objekten gemäss ihrer statistischen Verteilung erhoben oder eingeschätzt.

3.6

Risiko-Bewertung



Die in der Risiko-Analyse gefundenen Risiken mit ihren Werten für Wahrscheinlichkeit, Schadensausmass und Risiko sowie Risiko-Proxies bedürfen einer Interpretation und Bewertung im Kontext des Untersuchungs- und Behandlungs-Gegenstands. Die Kriterien dafür waren zuvor bereits im Kontext festzulegen. Aus den Erkenntnissen der durchgeführten Risiko-Analyse können auch zusätzliche Kriterien relevant werden (z.B. Qualitätsanforderungen oder Zeitprioritäten), die für die anstehenden Entscheide hinsichtlich einer optimalen Risiko-Behandlung zu beachten sind.

Reduktion Häufigkeit oder Schadensausmass

Risiken / Chancen

Optimum

Attribute zur Risikobehandlung

Wichtigkeit - Dringlichkeit

So muss beispielsweise geklärt werden, ob die Häufigkeit oder das Schadens-Ausmass oder beides zu reduzieren sind. Für geringe, aber häufige Dienstleistungs-Ausfall-Risiken könnte beispielsweise angezeigt sein, „nur“ die als „Qualitätsmangel“ wahrnehmbare Häufigkeit der Ausfälle zu reduzieren. Eine solche Anforderung könnte an die nachfolgenden Bewältigungs-Massnahmen gestellt werden. Ein blindes Reduzieren oder gar Vermeiden der Risiken würde unter Umständen das Ergreifen von Chancen verhindern. Es stellt sich deshalb die Frage, inwieweit das Reduzieren der Risiken die Chancen beeinträchtigt oder gar zunichtemacht.

So wird es Risiken geben, die nur auf eine bestimmte Art und Weise oder solche, die gar nicht bewältigt werden sollen, wenn ein Optimum im Verhältnis zu den Chancen anzustreben ist.

Für die nachfolgende Definition und Ausarbeitung der Massnahmen sind eine Reihe zusätzlicher Anforderungen zu berücksichtigen. Solche Anforderungen sind beispielsweise ethische Aspekte, Standards, Leistungsanforderungen, Gesetze, Zeit- und Kostenbeschränkungen. Die Risiken können daher mit „Attributen“ für die nachfolgende Risiko-Behandlung und die Bewältigungs-Massnahmen versehen werden.

Ein solches Attribut ist beispielsweise die Dringlichkeit der Risiko-Bewältigung. So gibt es Risiken, die aufgrund gesetzlicher

oder regulatorischer Vorschriften bis zu einem bestimmten Termin unbedingt bewältigt sein müssen. Andere grosse und wichtige Risiken haben hingegen unter Umständen weniger hohe Dringlichkeit, da sie selten vorkommen. Bei der Reflektion der Risiken im Kontext der definierten Rahmenbedingungen, kann sich sogar herausstellen, dass einige Risiken für die Behandlung weder „wichtig“ noch „dringlich“ sind. In einem solchen Falle kann eine Reduktions-Massnahme unterbleiben. Doch könnte ein solches Risiko das Attribut erhalten, dass das Risiko weiterhin beobachtet werden muss.

*Risiko-
Wahrnehmung
der Umgebung
und des Ma-
nagements*

An dieser Stelle des Risikomanagement-Prozesses spielt die Risiko-Wahrnehmung der Umgebung und des Managements eine wichtige Rolle. Dazu bedarf es der Kommunikation mit den zuständigen Entscheidungsträgern (ggf. auch mit bestimmten Anspruchsgruppen) mit entsprechenden Reports und Darstellungen (z.B. mit einem fortgeschriebenen Risiko-Katalog und einem Risiko-Portfolio). Auch ist es meist nützlich und gegebenenfalls sogar obligatorisch, an dieser Stelle des Risikomanagement-Prozesses die Zustimmung des zuständigen Managements zur Risiko-Lage und zu Fragen der Akzeptanz und der Dringlichkeit der Massnahmen und deren Umsetzung einzuholen.

*Entscheid über
Nachbesserung
Analyse-
Ergebnisse*

Beim Teilprozess der Risiko-Bewertung wird auch zu überprüfen und zu entscheiden sein, ob die Analyse-Ergebnisse, was ihre Vollständigkeit, Genauigkeit und Aussagekraft betrifft, den Anforderungen, beispielsweise des Managements, genügen. Andernfalls muss der Prozess oder Teile davon wiederholt oder nachgebessert werden.

*Verständliche,
bindende und
nachvollziehbare
Dokumentation*

Die Ergebnisse der Risiko-Bewertung stellen den Abschluss des Risiko-Assessment (Risikobeurteilung) dar. Anhand dieser Ergebnisse werden die folgenden Prozesse der Massnahmen-Planung und -Umsetzung gesteuert sowie die Risiko-Lage vor und nach der Bewältigung beurteilt. Deshalb ist es besonders wichtig, die Ergebnisse der Risiko-Bewertung mit den angestellten Betrachtungen und Entscheiden in verständlicher, bindender* und nachvollziehbarer Weise zu dokumentieren.

* Verschiedene gesetzliche oder regulative Vorgaben verlangen eine mit Unterschrift des zuständigen Managements bestätigte Risikobeurteilung.

3.7

Risiko-Assessment Methoden

In den Abschnitten 3.3 bis 3.6 wurden die verschiedenen Vorgehensweisen bei den Teilprozessen Identifikation, Analyse und Bewertung behandelt sowie in den Abschnitten 2.6 bis 2.8 die statistischen Zusammenhänge zur Messung und Darstellung des Risikos. Im folgenden Abschnitt wird nun auf die Methoden eingegangen, die sich für die „systematische“ Behandlung von einzelnen Aufgaben bis hin zu mehreren Teilprozessen des Risiko-Assessment etabliert haben. Zum „systematischen“ Assessment eines Bereichs legen wir modellhaft jeweils ein „System“ mit seinen Subsystemen, Abgrenzungen und Schnittstellen zu Grunde, welches es auf seine Risiken hin zu untersuchen gilt. Ein solches System kann ein ganzes Unternehmen, ein Projekt, ein Geschäftsprozess oder ein IT-System sein.

Um in einem solchen System zu den erforderlichen Analyse-Ergebnissen zu kommen, unterscheiden wir prinzipiell die „Bottom-up-Methoden“ und die „Top-down-Methoden“*. Ebenfalls unterscheiden wir, ob die Methode „qualitative“ oder „quantitative“ Ergebnisse liefern soll.

Bottom-up-Analyse

Bei den **Bottom-up-Methoden** werden aufgrund von Ursachen, mögliche Schadensereignisse und deren Konsequenzen hergeleitet und die Risiken eingeschätzt. Dazu ist eine eingehende Analyse der Sub-Systeme oder Sub-Prozesse mit ihren Abhängigkeiten und Korrelationen im Rahmen des Gesamtsystems notwendig. Ein solches aufwändiges Verfahren liefert aber gleichzeitig die Anhaltspunkte zum Ansetzen der Sicherheitsmassnahmen. Hingegen ist besondere Sorgfalt bei der Aggregation der Einzel-Risiken zu Unternehmens-Risiken hinsichtlich

* Die Begriffe „Bottom-up“ und „Top-down“ werden in der Risikomanagement-Praxis unterschiedlich angewandt, z.B. für die Schwachstellen-Suche bei der Risikoidentifikation oder für das Vorgehen bei der Durchführung der Risiko-Analyse. Für „Bottom-up“ ist dabei grundsätzlich ein „induktives“, von den Ursachen ausgehendes Vorgehen und mit Top-down ein „deduktives“, von den Folgen ausgehendes Vorgehen zu verstehen. Die Begriffe werden meist bei der Analyse des Gesamtrisikos aus Unternehmenssicht angewandt, wobei beim Top-Down-Verfahren verschiedene Ergebniszahlen im Hinblick auf ihre Volatilität zur Ermittlung eines Gesamtrisikos untersucht werden; hingegen werden beim Bottom-up Verfahren die Risikokategorien, Geschäftsbereiche und Prozesse ursächlich erfasst, analysiert und die entsprechenden Einzelrisiken zu einem Gesamtrisiko aggregiert.

Überschneidungen und Doppelbewertungen einzelner Risiken nötig.

Top-down-Analyse

Bei den **Top-down-Methoden** gehen wir primär von den Folgen grosser Schadensereignisse aus, die als hauptsächliche Risiken angesehen werden. Die Wahrscheinlichkeiten werden meist aus historischen Informationen geschätzt. Solche Verfahren lassen sich leicht durchführen und geben Anhaltspunkte über Art und Höhe der Risiken, liefern aber wenige Erkenntnisse über die Zusammenhänge und Ursachen. Damit liefert ein solches Verfahren auch wenige Anhaltspunkte darüber, wo die Massnahmen angesetzt werden können.

Analyse-Methoden

In der Praxis kommt für ein umfassendes, aussagekräftiges Risiko-Assessment meist die Anwendung verschiedener Methoden in Frage. Einige solcher zum Einsatz gelangenden Methoden sind in der Abbildung 3.2 zusammengestellt.

Methode	Quantitativ	Qualitativ
Bottom-up	☐ Ereignisbaum-Analyse ☐ Fehler-Effekt- und Ausfall-Analyse (FMEA) ☐ Sensitivitäts-Analyse ☐ Simulations-Ansätze	☐ Szenario-Analyse ☐ Prozessrisiko-Analyse ☐ Expertenbefragung
Top-down	☐ Fehlerbaum-Analyse ☐ Risiko-Datenbank ☐ Zufallsverteilungen ☐ Extremwert-Theorie ☐ Value at Risk (VaR)	☐ Key Performance Indicator (KPI) ☐ Key Control Indicator (KCI) ☐ Key Risk Indicator (KRI) ☐ Nutzwert-Analyse

Abbildung 3.2: Risiko-Analyse-Methoden (vgl. [Piaz02], S. 107)

An verschiedenen Stellen des Buches werden einige dieser Methoden im Zusammenhang mit konkreten Fragestellungen eingehender behandelt. Eine Übersicht über 31 solcher Assessment-Techniken mit kurzen Erläuterungen ist im Standard ISO/IEC 31010 zu finden.

In den folgenden Abschnitten werden einige grundlegenden Aspekte bei der Risikosuche und Risikobestimmung behandelt.

3.7.1

Such-Methoden

Suchmethoden werden in komplexen Systemen und Anordnungen angewendet, um Schwachstellen und Risiken und insbesondere die Ursachen oder die Auswirkungen einzelner Ereignisse herauszufinden. Dabei dienen sie vorab der Risiko-Identifikation; oft liefern sie auch gerade die Ergebnisse einer Risiko-Analyse. Für das Assessment von mehreren, bezüglich Störungsbeeinflussung verschachtelten Subsystemen, ist es oft wichtig, wie sich die Störereignisse innerhalb der Subsysteme und in Bezug auf das Gesamtsystem auswirken* ([Leve95], S. 309).

Bottom-up-Suche Eine derartige Untersuchung erfolgt mit der Bottom-up-Suche (s. Abbildung 3.3).

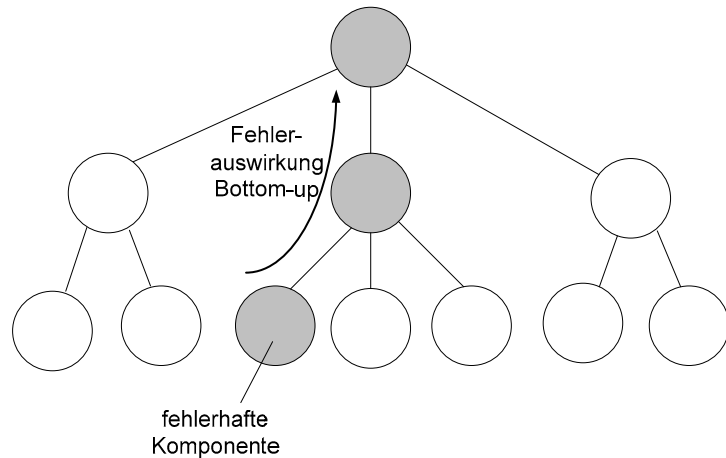


Abbildung 3.3: Prinzip der Bottom-up-Suche

Beispiel:

Welche Auswirkung auf das Gesamtsystem hat ein Programmfehler in einer bestimmten Software-Routine?

In der Form eines „Ereignisbaums“ kann eine Bottom-up-Suche zu einer quantifizierenden Analysen-Methode ergänzt werden, indem beispielsweise die Wahrscheinlichkeit für den Ausfall eines Gesamtsystems, aus den Ausfallwahrscheinlichkeiten einzelner Subsysteme, ermittelt wird (s. Abschnitt 10.5).

* Im allgemeinen Fall können die Systeme und Subsysteme auch immaterieller Natur sein (z.B. Prozesse) und müssen nicht notwendigerweise eine hierarchische Struktur aufweisen.

Top-down-Suche Bei der Top-down-Suche werden vom Gesamtsystem die verschiedenen Pfade zu den Subsystemen durchsucht, um festzustellen, wie sich eine Störung des Gesamtsystems durch Stör-Ereignisse in den einzelnen Subsystemen ergeben kann.

Beispiel:

Welche Ereignisse (z.B. Komponenten-Ausfälle) führen zu einem Stromversorgungs-Ausfall des Gesamt-Systems?

In der Form eines „Fehlerbaums“ kann die Top-down-Suche zu einer quantifizierenden Analysen-Methode ergänzt werden, indem die Wahrscheinlichkeit eines „Top-Ereignisses“ aus den Wahrscheinlichkeiten der verschiedenen möglichen Ursachen errechnet wird (s. Abschnitt 10.4).

3.7.2

Szenarien-Analyse

Zur Beschreibung des Übergangs von einer Bedrohung zu einem Risiko dient das „Szenario“.

Drehbuch für ungünstige Entwicklungen

Das Szenario ist sozusagen das Drehbuch für ungünstige Entwicklungen, die wir als Schadensereignisse wahrnehmen. Mit der Szenarien-Analyse wird ein in die Zukunft prognostiziertes Ereignis mit einem entsprechenden Ablauf untermalt. Es dient der Simulation von kausalen Zusammenhängen.

Wenn-dann-Fragen

Diese können durch „Wenn-dann“-Fragen herausgearbeitet werden. Die Szenario-Analyse wird vor allem dann angewendet, wenn wenig oder keine konkreten Daten über Verlustereignisse aus der Vergangenheit vorliegen.

Befragung Experten

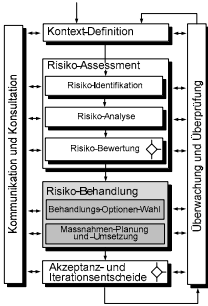
Die Szenarien werden durch Befragung von Experten in Workshops oder mittels spezieller Befragungsmethoden definiert.

Ex-ante-Schätzungen

Bei den „Ex-ante-Schätzungen“ werden sowohl die Schadenshöhen als auch die Eintrittswahrscheinlichkeiten der Szenarien eingeschätzt. Durch entsprechende Fragestellungen können auch Erwartungswerte und der „Value at Risk“ für entsprechende Konfidenz-Niveaus eingeschätzt werden. In der oben gegebenen Terminologie handelt es sich bei der Szenarien-Analyse um eine Bottom-up-Methode.

3.8

Risiko-Behandlung



Die Risiko-Behandlung im Rahmen eines Risikomanagement-Prozesses dient der Auswahl von Behandlungs-Optionen und der Definition, Konzeption, Planung und Umsetzung von Massnahmen aufgrund der bei der Risiko-Bewertung definierten Anforderungen. Der Prozess der Risiko-Behandlung wird auch als Risiko-Steuerung bezeichnet, da es darum geht, die Risikolage des Unternehmens, wenn nötig, positiv zu verändern. Wie bereits in der vorangegangenen Phase der Risiko-Bewertung sind auch hier die Chancen mit den Risiken in ein ausgewogenes Verhältnis zu bringen. Dabei ist bei operationellen Risiken nicht das Ausbalancieren von Risiken mit Erträgen, sondern das Erreichen der Geschäftsziele durch eine angemessene und nachhaltige Risikobehandlung gemeint.

Abwägen Risiken mit Massnahmenkosten

Eine nicht einfache Aufgabe dabei ist das Abwägen der Risiken mit den Massnahmenkosten (s. Kapitel 11).

Machbarkeit der Massnahmen

Zu den vorbereitenden Aktivitäten der Risiko-Behandlung gehört die Untersuchung der Machbarkeit der Massnahmen sowohl aus der Sicht der gestellten Anforderungen als auch aus der Sicht der Finanzierbarkeit, des Aufwandes und der Termine.

Bewältigungs-Optionen

Bezüglich der Massnahmengestaltung stehen prinzipiell die folgenden **Behandlungs-Optionen** zur Auswahl:

- **Risiken vermeiden;** z.B. durch Aufgabe risikoreicher Aktivitäten oder Verlagerung von Aktivitäten an Orte, wo das Risiko nicht auftritt.
- **Risiken reduzieren;** durch Reduktion entweder der Eintritts-Wahrscheinlichkeit oder des Schadensausmasses mittels entsprechender Massnahmen (z.B. durch Firewall oder Katastrophenorganisation). Reduziert werden die Risiken auch durch Diversifikation (z.B. durch örtlich getrennte Produktionsstätten oder Backup der Risiko-Objekte und Ressourcen). Die gänzliche Unterdrückung des Risikos durch die Entfernung der Risiko-Quelle kann auch eine gültige Sub-Option sein.
- **Risiken transferieren;** z.B. Überwälzung finanzieller Schäden auf Versicherungen.
- **Risiken bewusst eingehen und tragen;** z.B. Tragen des Restrisikos, welches im Rahmen der betrieblichen Reserven und eines allfälligen Goodwill-Verlusts verkraftbar ist.

Letztere Option ist auch der Grund, warum der internationale Standard ISO 31000 bei den Optionen nicht generell von „Risiko-Bewältigung“, sondern von einer „Risiko-Behandlung“ spricht. In diesem Sinne stellt auch das Vergrössern eines Risikos in der Absicht, eine Chance wahrzunehmen, gemäss dem Standard ebenfalls eine gültige Behandlungs-Option dar.

Auswahl von Optionen

Die Auswahl einer oder mehrerer Behandlungs-Optionen und deren allfälligen Massnahmen wird jeweils anhand der gestellten Anforderungen und der Machbarkeit verifiziert sowie auf deren Wirksamkeit in Bezug auf das ursprüngliche Risiko überprüft. Zu diesem Zweck werden gegebenenfalls die Risiko-Analyse und die Risiko-Bewertung mit unterschiedlichen Massnahmen erneut mehrere Male durchgespielt, um das Optimum zwischen zielgerechter Risiko-Behandlung und Massnahmenkosten zu finden. Eine zielgerechte Risiko-Behandlung setzt voraus, dass die Kriterien für die Risiko-Akzeptanz bei den verbleibenden Restrisiken erfüllt sind.

Kosten-/Nutzen-Untersuchungen

Bei solchen Kosten-/Nutzen-Untersuchungen müssen die direkten, indirekten und auch langfristigen Kosten betrachtet werden (s. Kapitel 11). Das Optimum von Risiko und Massnahmenkosten kann gegebenenfalls auch dadurch erreicht werden, dass verschiedene Massnahmen in Kombinationen eingesetzt werden (z.B. technische Massnahmen und entsprechend vertragliche Absicherungen). Ausser den Kosten sind die Vorstellungen, Erwartungen und Werte der Anspruchsgruppen in die Massnahmenentscheide mit einzubeziehen. Massnahmen, die beispielsweise keine Akzeptanz bei Kunden finden sind womöglich zu vermeiden. Auch können Massnahmen sekundäre Risiken herbeiführen, die bei der Bewältigung und bei der Akzeptanz der Restrisiken berücksichtigt werden müssen.

Umsetzungsplan

Für die festgelegten Massnahmen muss nun ein Umsetzungsplan festgelegt werden. Im Umsetzungsplan sind die Gründe und Rechtfertigungen für die Wahl der Massnahmen sowie deren Dringlichkeiten und die wesentlichen projektmässigen Planungsinformationen, einschliesslich der dafür zur Verfügung stehenden Umsetzungs-Ressourcen, zu berücksichtigen.

Viele Massnahmen, z.B. solche organisatorischer Natur, werden oft nicht einmalig umgesetzt, sondern erfordern eine ständige, meist periodische Betreuung und Überwachung. Die Planung auch solcher periodischer Aktivitäten muss aus dem Umsetzungsplan hervorgehen.

Zusammengefasst müssen vor allem die folgenden Informationen im Plan enthalten sein (vgl. [Isor09, S. 20]):

- Gründe für die Wahl bestimmter Behandlungs-Optionen und ausgesuchter Massnahmen;
- Angaben über Effektivität der Massnahmen im Verhältnis zu den Aufwendungen resp. Kosten;
- Bezeichnung der für die Genehmigung sowie für die Umsetzung der Massnahmen verantwortlichen Personen und Organisationseinheiten;
- Notwendige Ressourcen für Massnahmen-Umsetzung und -Betrieb;
- Allfällige Leistungseinbussen und durch Massnahmen entstandene sekundäre Risiken sowie Nützlichkeiten der Massnahmen gegenüber Anspruchsgruppen (z.B. Kunden);
- Überwachungs- und Berichterstattungs-Aktivitäten bei Massnahmen-Umsetzung und -Betrieb, integriert in die Management-Prozesse des Unternehmens;
- Aktionsplan einschliesslich Terminen zur Umsetzung der Massnahmen.

*Erneute Risiko-
Einschätzung
und -Bewertung*

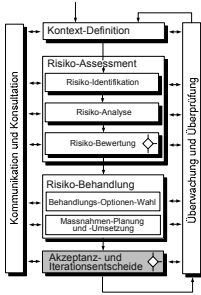
Bei der Festlegung des Umsetzungs-Plans können wiederum unvorhergesehene Kosten sowie Ressourcen- und Umsetzungs-Probleme auftauchen, sodass die Risiko-Behandlung mit anderen Massnahmen überprüft werden muss. Auch in einem solchen Falle ist allenfalls die Risiko-Analyse und Risiko-Bewertung unter den neuen Voraussetzungen zu wiederholen, um die Einhaltung der Akzeptanzkriterien und Zusatzforderungen bei der Risiko-Bewertung zu verifizieren.

Für ein tragbares Restrisiko ist jedoch nicht alleine die Planung, sondern in erheblichem Masse auch die Umsetzung der geplanten Massnahmen wichtig. Die im Abschnitt 3.9 näher behandelte Überwachung des Prozesses zur Risiko-Behandlung muss diesem Umstand in besonderer Weise Rechnung tragen, um allfälligen Planabweichungen wirksam entgegentreten zu können.

Als Ergebnisse für die im nächsten Prozessschritt formalen Akzeptanz-Entscheidungen sind also die Planungsinformationen wie auch die Informationen über den Ist-Zustand der Realisierungen sowie das Restrisiko mit seinen Abhängigkeiten zu liefern. Dazu muss das Restrisiko in der Weise dokumentiert sein,

dass es nachvollzogen, weiterhin überwacht, überprüft und wenn notwendig, erneut behandelt werden kann.

3.9



*Akzeptanz
Restrisiko*

*Kriterien für
Prozesswieder-
holungen*

Akzeptanz- und Iterationsentscheide

Bei diesem wichtigen Teilprozess des Risikomanagements werden sich vor allem die verantwortlichen Führungspersonen (ggf. das Top-Management) versichern, dass sich das aktuelle und auch zukünftige Restrisiko in einem tolerablen Bereich befindet. Dazu wird sich das Management zu angemessenen Zeitpunkten mit der Massnahmenplanung, dem geplanten Restrisiko sowie dem Stand der Massnahmenumsetzung befassen.

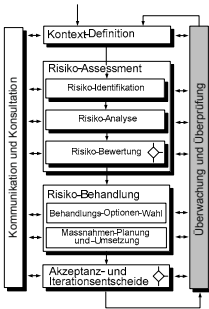
Ebenfalls wird das Management zu entscheiden haben, ob die Kontext-Definitionen und Assessment-Ergebnisse der momentanen und bevorstehenden Risikolage genügen.

Basierend auf den Informationen über das Restrisiko, das in seinen Abhängigkeiten dokumentiert sein muss, sowie den Überwachungs- und Überprüfungsergebnissen (s. Abschnitt 3.10) wird das zuständige Management das Restrisiko formal zur Kenntnis nehmen und akzeptieren, oder die Durchführung weiterer Aktivitäten des Risikomanagementprozesses entscheiden und veranlassen. Neben den situativ bedingten Entscheidungen über das erneute Durchführen des Prozesses oder einzelner Prozessschritte ist nach dem vollständigen Durchlaufen des Prozesses auch eine periodische Wiederholung des gesamten Prozesses (z.B. synchron zum rollierenden Strategieprozess) üblich.

Entsprechend der modernen Management-Systeme ist der Risikomanagement-Prozess ein inhärent zyklischer Prozess, welcher der Dynamik von internen und externen Veränderungen gerecht werden muss. So sollen zur Verbesserung der Zwischenergebnisse hinsichtlich der gesetzten Ziele nicht nur einzelne Zwischenschritte, sondern der gesamte Prozess wiederholt werden. Die Kriterien dafür können beispielsweise ändernde Umgebungsbedingungen, inakzeptable Restrisiken, resultierend aus ungenügend realisierten Massnahmen, oder regulative Anforderungen sein. Für bestimmte Situationen wird der Prozess zum Zeitpunkt der aktuell anstehenden Veränderung gestartet (z.B. Entwicklung einer neuen Produktions-Plattform). Hingegen wird der Risikomanagement-Prozess für das ganze Unternehmen meist mit anderen periodischen Management-Prozessen (z.B. Strategieprozess) in geeigneter Weise synchronisiert und wiederholt (s. Kapitel 12).

3.10

Überwachung und Überprüfung



Die Aktivitäten und Massnahmen zur „Überwachung“ und „Überprüfung“ sollten in den Risikomanagement-Prozesses eingeplant sein und klar definierten Verantwortlichkeiten unterliegen; die diesbezüglichen Aktivitäten können fortlaufend, anlassgesteuert oder periodisch erfolgen.

Sowohl während allen Teilprozessen des Risikomanagement-Prozesses als auch nach dem Durchlauf des gesamten Prozesses ist es wichtig, den Prozess bezüglich Effektivität, Effizienz sowie der Risiko-Situation und allfälliger Veränderungen zu überwachen. Anzeichen für Veränderungen können beispielsweise aus der Überwachung der Änderungs-Prozesse, der Entwicklungsprozesse und der Betriebsprozesse gewonnen werden.

Es empfiehlt sich, die Leistungsfähigkeit des Risikomanagement-Prozesses und seiner Teilprozesse sowie die Effektivität und Effizienz der Massnahmen anhand von Key-Performance-Indikatoren (KPIs) zu messen.

Auch können mit Key-Risk-Indikatoren (KRI) sowohl externe als auch interne Risiko-Situationen ständig überwacht werden, indem diese Indikatoren bei entsprechenden Situationen Alarme auslösen. Solche Alarmsituationen sind denkbar bei Veränderungen des Risiko-Kontextes, der Bedrohungslage oder aufgrund anderer ein Risiko anzeigenden Faktoren (z.B. ungewöhnliche Volumenveränderungen).

Eine solche Überwachung kann zu einem Frühwarnsystem mit entsprechendem Reporting ausgebaut werden, z.B. mit visueller Darstellung auf einem „Dashboard“. Durch ein solchermassen konzipiertes Reporting können vor allem die zuständigen Führungspersonen in angemessener Weise über die aktuelle Risikosituation informiert werden.

Die Risiken, die Massnahmen, wie auch der gesamte Prozess des Risikomanagements bedürfen der Überprüfung durch Personen und Instanzen, die den Tatsachen unbefangen und neutral gegenüber stehen. Dazu eignen sich beispielsweise externe unabhängige Auditoren, die unter anderem auch den Aufbau und Ablauf des Prozesses mit seinen Verantwortlichkeiten, einschliesslich der im Kontext vorgegebenen Kriterien und Methoden überprüfen. Eine solche externe Überprüfung des Risikomanagements ist ab einer bestimmten Unternehmensgrösse Bestandteil der Geschäftsprüfung respektive der Jahresabschlussprüfung. In grösseren Unternehmen wird zudem im Rahmen des

*Überwachung
Risiko-Indikatoren
und Frühwarn-
system*

*Überprüfung
durch unabhän-
gige Auditoren*

Verifikation anhand von Reifegradmodell

IKS (Internes Kontroll-System) die Prüfung des Risikomanagements durch interne Revisoren vorgenommen.

Um die Güte des Prozesses in seiner Wirksamkeit und Effizienz zu überprüfen, wird auch die Verifikation anhand eines entsprechenden Reifegradmodells empfohlen (z.B. [Horw04], S. 402-403). Da die gewünschte Qualität des Prozesses meist erst nach einiger Zeit, eventuell nach Jahren erreicht wird, empfiehlt es sich, den Reifegrad periodisch untersuchen zu lassen.

Risiko-Berichte

Analysen und Risikoberichte enthalten beispielsweise Informationen über:

- Statusmeldungen über die aktuelle und voraussichtliche Risikosituation;
- eingetretene oder fast eingetretene Risikoereignisse und daraus gezogenen Lehren;
- Stand, Wirksamkeit und Effizienz der Massnahmen-Umsetzungen und allfällige Verbesserungsvorschläge;
- geplante Ereignisse und Aktivitäten zur Verbesserung des Risikomanagements sowie die Resultate aus solchen Ereignissen und Aktivitäten (z.B. Resultate und Lehren aus Übungen oder Awareness-Aktionen);
- Voraussichtliche Veränderungen und resultierende Konsequenzen für das Risikomanagement und dessen Resultate.

Die Risiko-Berichte gehören, in entsprechend zusammengefasster Form, ähnlich den Budgetberichten, zu den regelmässigen Berichterstattungen an die Unternehmensleitung. Auch bei diesem regelmässigen Reporting ist auf die Unabhängigkeit der Berichterstattung durch weitgehend unabhängige Personen und neutrale Aufzeichnungssysteme zu achten.

3.11

Universeller Risikomanagement-Prozess

RM-Prozess universell einsetzbar

Das grobe Muster eines Risikomanagement-Prozesses kann in allen Situationen angewendet werden, wo es um die Erkennung, Analyse, Bewertung und Bewältigung von Risiken geht. So ist der Prozess auch als Frühwarnsystem mit schwachen Risiko-Signalen (z.B. Konjunkturindikatoren, Trends hinsichtlich Marktrisiken) einsetzbar. Ebenso ist er anwendbar für die Problembehandlung in Notfällen mit plötzlichen und völlig „unangemeldeten“ Schadensereignissen oder plötzlichen akuten Bedrohungen und „Exploits“, die zu Schäden eskalieren können (z.B. Computer-Würmer).

Die Teilprozesse sind dabei unterschiedlich strukturiert. Bei plötzlich auftretenden Ereignissen können beispielsweise die Risiko-Analysen meist nur grob mit qualitativen Einschätzungen durchgeführt werden. Die genaueren Untersuchungen (z.B. die Impact-Analysen) für solche plötzlichen Ereignisse werden womöglich im Voraus, im „vorsorglichen Plan“, vorgenommen.

Teilprozesse induktiv oder deduktiv

Die Teilprozesse im RM-Prozess können, je nach Anwendung, induktiv (von den Ursachen und Fakten zum Resultat) oder deduktiv (vom Resultat rückwärts zu den Ursachen und Fakten) durchgeführt werden. Oft kommt ein optimales Ergebnis aus der Mischung beider Vorgehensweisen zustande.

Somit halten wir fest:

Problemlösungs-Prozess

Der Risikomanagement-Prozess ist der „Problemlösungs-Prozess“ zur folgerichtigen und „systemischen“ Behandlung von Risiken.

Beispiele RM-Prozess

Nachfolgend sind einige Beispiele aufgeführt, bei denen es sinnvoll ist, einen dem Grundprinzip folgenden Risikomanagement-Prozess aufzubauen:

- ☐ Unternehmens-Risikomanagement-Prozess
- ☐ Frühwarnsystem für wichtige Unternehmens-Risiken
- ☐ Sub-Risikomanagement-Prozess für IT-Betriebsrisiken
- ☐ Sub-Risikomanagement-Prozess bei der Erstellung von Sicherheits-Konzepten
- ☐ Sub-Risikomanagement-Prozess für Projektrisiken
- ☐ Geschäftskontinuitäts-Plan
- ☐ IT-Notfall-Plan

Die Teilprozesse, Systemunterstützungen und Prozessbeteiligten sind für jeden Anwendungsfall den Anforderungen entsprechend anzupassen.

Einige dieser Risikomanagement-Prozesse werden wir in den Teilen C und D des Buches noch näher behandeln.

3.12

Zusammenfassung

Der Risikomanagement-Prozess ist generischer Natur und kann in praktisch allen Risiko-Situationen mit entsprechend ausgelegten Teilprozessen verwendet werden.

Die Hauptaufgaben „Kontext-Definition“, „Risiko-Assessment“ mit den Teilaufgaben „Risiko-Identifikation“, „Risiko-Analyse“, „Risiko-Bewertung“ sowie der „Risiko-Behandlung“ sind zu einem Prozess verknüpft. Dazu kommen der wichtige Entscheidungsschritt der Risikoakzeptanz sowie die wichtigen begleitenden Aufgaben der „Kommunikation und Konsultation“ und der „Überwachung und Überprüfung“. Durch Rückkopplungen und Iterationen im Prozess werden die Ergebnisse der einzelnen Aufgaben verbessert.

Eine effektive und effiziente Durchführung der Risiko-Analyse bedarf ausgefeilter Methoden für die Identifikation und die Analyse der Risiken. Aufgrund der gestellten Anforderungen sind manchmal nicht nur qualitative sondern auch entsprechend quantitative Methoden einzusetzen.

Eine komplette Risiko-Analyse enthält eine Impact-Analyse, eine Bedrohungs-Analyse und eine Schwächen-Analyse. Für Risiken, bei denen für eine komplette Risiko-Analyse die Angaben über die Schadensauswirkungen und/oder Eintrittswahrscheinlichkeiten fehlen, weichen wir auf die Erstellung einer Schwächen-Analyse oder einer Impact-Analyse aus. Die Schwächen-Analyse zeigt, wo aufgrund inhärenter Schwächen oder ungenügender Massnahmen Risiken zu erwarten sind. Die Impact-Analyse zeigt die Höhe des Schadens bei den einzelnen Risiko-Objekten. Für die Geschäftskontinuität ist die Höhe des Schadens in Abhängigkeit der Ausfallzeit von Interesse. Das Risiko-Assessment geht entweder Top-down von den im Vordergrund stehenden Folgen und dem nachlaufenden Aufsuchen der Ursachen aus oder es erfolgt Bottom-up, ausgehend von den Ursachen hin zu den möglichen Konsequenzen. Ähnliche Verfahren sind bei der Analyse für Ursachen und Wirkungen von fehlerhaften Systemkomponenten gebräuchlich.

Die „Risiko-Bewertung“ ist eine separate Aufgabe, bei der die zuvor analysierten Risiken bewertet werden. Für die Bewertung ist vor allem der Kontext der Risikomanagement-Aufgabe massgebend. Dabei spielen die Abwägungen der Risiken gegenüber den Chancen, die Anforderungen bezüglich der zu ergreifenden Sicherheits-Massnahmen und die Prioritäten für die Risiko-Bewältigung eine Rolle. Bei der Risiko-Bewertung wird auch zu überprüfen und zu entscheiden sein, ob die Ergebnisse der Identifikation und Analyse den Anforderungen genügen oder ob der Prozess, oder Teile davon, wiederholt und nachgebessert werden müssen.

Die Massnahmen zur „Risiko-Behandlung“ sind im Rahmen der Behandlungs-Optionen „Vermeiden“, „Reduzieren“, „Transferieren“ oder „Bewusst tragen“ zu wählen. Der Umsetzungsplan enthält vor allem die Aktivitäten, Termine und Verantwortlichkeiten zur Umsetzung der Massnahmen. Aufgrund bestimmter Kriterien können die Restrisiken akzeptiert werden oder der Risikomanagement-Prozess oder Teile davon erfahren eine Wiederholung.

3.13

Kontrollfragen und Aufgaben

1. Erklären Sie die Unterschiede zwischen einer Risiko-, einer Impact- und einer Schwächen-Analyse?
2. Was verstehen Sie unter einer Szenario-Analyse?
3. Nennen Sie die Hauptaufgaben und begleitenden Aufgaben eines Risikomanagement-Prozesses.
4. Erklären Sie kurz die beiden der Risikomanagement-Praxis verwendete Begriffe Top-down-Methode und Bottom-up-Methode.
5. Welche Aufgaben enthält das Risiko-Assessment?
6. Nennen und erklären Sie die vier prinzipiellen Behandlungs-Optionen.
7. Nennen Sie Beispiele und Verfeinerungen der prinzipiellen Behandlungs-Optionen.
8. Worauf ist bei der „Überwachung und Überprüfung“ zu achten?
9. Worauf ist bei der „Kommunikation und Konsultation“ zu achten?
10. Der Risikomanagement-Prozess ist ein zyklischer Prozess; er wird aufgrund bestimmter Ereignisse gestartet und in einzelnen Teilabschnitten, aber vor allem nach vollständigem Durchlauf, wiederholt.

Nennen Sie Kriterien aufgrund derer

- a) der Risikomanagement-Prozess gestartet wird
oder
- b) der Prozess wiederholt wird.

Teil B

Anforderungen aus Unternehmenssicht berücksichtigen

4

Risikomanagement, ein Pflichtfach der Unternehmensführung

Kontext des Unternehmens

Das Risikomanagement in einem Unternehmen und das in diesem Buch im Detail behandelte Informationssicherheits- und IT-Risikomanagement können nicht zufriedenstellend behandelt werden, wenn nicht der Kontext des Unternehmens mit seinem Management-System und seiner Umwelt beleuchtet und einbezogen wird. Die Risiken stammen doch aus einer einzigartigen Positionierung des Unternehmens zu seiner Umwelt und seinen dem Unternehmenszweck dienenden Leistungsprozessen. In diesem Buch verfolgen wir deshalb einen ganzheitlichen, integrierten Management-Ansatz. Dieser wird dadurch charakterisiert, dass verschiedene Management-Prozesse im Unternehmen mit ihren unterschiedlichen Zweckbestimmungen in ein übergeordnetes „Management-System“ oder „Führungssystem“ integriert sind. Der Risikomanagement-Prozess ist einer dieser Management-Prozesse. Die Notwendigkeit der Integration des Risikomanagement-Prozesses in das Management-System des Unternehmens ergibt sich aus der Tatsache, dass zum einen die Unternehmensziele durch die Risiken negativ beeinflusst werden können und zum anderen die Forderungen an das „Risikomanagement“ wichtige Bestandteile der „Corporate Governance“-Regeln sind.

In den weiteren Ausführungen im Teil B dieses Buches werden somit die wichtigsten Anforderungen, wie sie im Rahmen eines integrierten Risikomanagements auch für die Informationssicherheits- und IT-Risiken zutreffen, aus der Sicht der Unternehmensführung behandelt.

4.1

Risikomanagement integriert in das Führungssystem

Die Positionierung der Managementprozesse im Unternehmen vergegenwärtigen wir uns mit dem St. Galler Management Modell [Rüeg02].

Modell eines Unternehmens

Anhand dieses Modells (s. Abbildung 4.1) ist leicht zu verstehen, dass sich Risiken nicht alleine aus innerbetrieblichen Prozessen ergeben, sondern gleichermassen wie die Chancen bei den

Interaktionen der Unternehmensprozesse mit der Umwelt des Unternehmens (Gesellschaft, Natur, Technologie und Wirtschaft) entstehen.

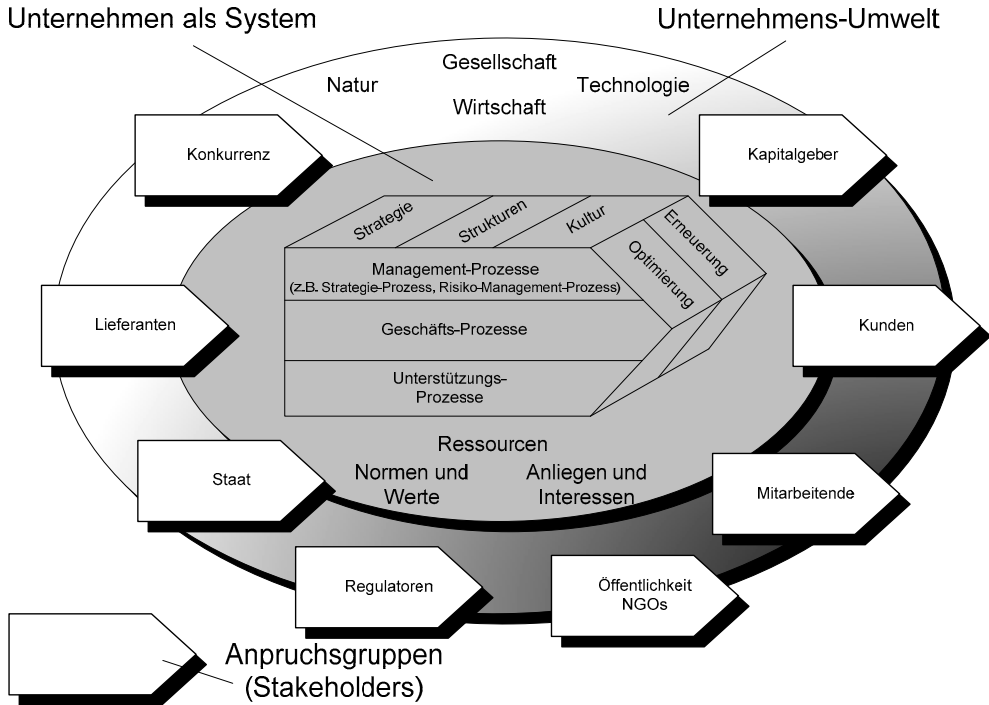


Abbildung 4.1: Unternehmens-Management-Modell (vgl. [Rüeg02], S. 22)

Das St. Galler Management-Modell unterscheidet die drei Prozesskategorien:

- Managementprozesse
- Geschäftsprozesse und
- Unterstützungsprozesse

Die auf der obersten Ebene angesiedelten Managementprozesse sind für die effektive und effiziente Führung eines komplexen Unternehmens unerlässlich. Solche Managementprozesse sind beispielsweise der Strategieprozess, der Risikomanagement-Prozess, die Prozesse für das Qualitätsmanagement oder das Sicherheitsmanagement, die Planungs- und Budgetierungspro-

	zesse sowie die Kontrollprozesse, wie sie beispielsweise durch CobIT* (s. Abschnitt 9.4) vorgegeben werden.
<i>Managementprozesse</i>	Die durch die „Managementprozesse“ gelenkten wertschöpfenden Geschäftsprozesse werden durch darunterliegende „Unterstützungsprozesse“ bedient.
<i>Typische Unterstützungsprozesse</i>	Typische Unterstützungsprozesse sind die „IT-Prozesse“, aber auch die Prozesse zur Bereitstellung von Ressourcen, wie Personal oder Infrastruktur. Im Zusammenhang mit dem Risikomanagement sind auch Unterstützungsprozesse zur Bewältigung der Risiken zu erwähnen. Die starke Verflechtung dieser drei Prozesskategorien ist offensichtlich. Allen diesen Unternehmensprozessen gemeinsam sind: • die Fokussierung auf eine Unternehmensstrategie, • die Festlegungen von Aufbau- und Ablaufstrukturen sowie • die Orientierungen auf eine Unternehmens-Kultur. Entsprechend dem Wandel der Wirtschaft und der Märkte sind die Geschäfts- und Unterstützungsprozesse ständigen Veränderungen, von innen und von aussen, gewollt oder ungewollt, unterworfen.
<i>Kontroll- und Rückkopplungsschleifen</i>	Diesen Veränderungen muss durch die Managementprozesse mittels entsprechender Kontroll- und Rückkopplungsschleifen im Sinne von „Optimierung“ und „Erneuerung“ Rechnung getragen werden können. Wie jüngste Fälle† zeigen, sind an einem guten Risikomanagement nicht nur die Anteilseigner‡ eines Unternehmens interessiert, sondern eine breite Zahl von anderen Interessenvertretern, deren Anforderungen bei den Unternehmenszielen und folglich bei den Unternehmensrisiken eine Rolle spielen.
<i>Anforderungen aller Anspruchsgruppen</i>	Die Anforderungen aller Anspruchsgruppen§ bezüglich der Risiken sind deshalb im Rahmen des Unternehmens-Risiko-

* Control Objectives for Information and Related Technology

† z.B. Bankrott der Bank Lehmann & Brothers; Abhörskandal bei der Deutschen Telekom; 2,3 Milliarden Verlust bei UBS durch nichtautorisierte Geschäfte eines Investmentbankers.

‡ Bei Aktiengesellschaften sind dies die Aktionäre (engl. Shareholders).

§ Anspruchsgruppen (engl. Stakeholders) sind Mitarbeitende, Kunden, Lieferanten, Staat, Kommunen, Verbände, Regulatoren usw.

managements zu interpretieren und im langfristig angelegten Interesse des Unternehmens anforderungsgerecht umzusetzen.

4.2

Corporate Governance

*Anforderungen
bezüglich
Führung und
Kontrolle*

Wenn es um die an das Unternehmen gestellten Anforderungen bezüglich Führung und Kontrolle geht, taucht immer wieder der Begriff „Corporate Governance“ auf. Dieser Begriff existiert seit einigen Jahrzehnten und steht für die grundlegenden Anforderungen der Anspruchsgruppen an die Führung und Kontrolle eines Unternehmens*.

*Verantwortlichkeit
und Transparenz*

Spätestens nach den Zusammenbrüchen von Unternehmen wie Enron, Worldcom, Swissair oder die KirchGuppe ist „Corporate Governance“ zum „Buzzword“ für Verantwortlichkeit und Transparenz im Unternehmen auf oberster Kontroll- und Führungsebene geworden. In der seit 2007 herrschenden globalen Finanz- und Wirtschaftskrise mit einer Vielzahl kollabierender Firmen sowie staatlicher Stützmassnahmen wird die Abhängigkeit breiter Anspruchsgruppen von funktionstüchtig geführten Firmen vermehrt zum öffentlichen Interesse.

*Grundlegendes
Anliegen der
Corporate
Governance*

Das grundlegende Anliegen der Corporate Governance besteht nun darin, die Bedingungen dafür herzustellen, dass die Unternehmensführung im Interesse des Unternehmens, der Anteilseigner[†], des Kapitalmarktes, der Mitarbeiter und anderer Anspruchsgruppen handelt. Dabei geht es um die „Führungsfunktion“ der Geschäftsleitung, die Oberleitung und Überwachungsfunktion des „Verwaltungsrates“ und der Prüfungsfunktion der Revisoren, *„aber auch und vor allem, um die zweckmässige Zusammensetzung und Strukturierung des Verwaltungsrates als Gremium“* ([Böck04], S. 1759).

*Begriffsverständnis
der OECD*

Entsprechend der Bedeutung für das Risikomanagement wählen wir aus der immer noch bestehenden Vielfalt von Begriffsdefini-

* Als Synonym für „Corporate Governance“ wird oft der Begriff „Unternehmens-Verfassung“ verwendet.

† Im angloamerikanischen Raum steht die Regelung des Verhältnisses hältisses zwischen den Anteilseignern, namentlich den grossen Investoren, und der obersten Unternehmensleitung im Vordergrund und ist durch den „Shareholder-Value“-Ansatz, d.h. die Maximierung des Börsenwerts, geprägt. In der im Sommer 2007 offenbar gewordenen Finanzkrise hat sich jedoch der „Shareholder-Value“-Ansatz als schädliche, nicht nachhaltige Unternehmens-Maxime erwiesen.

tionen für Corporate Governance das Begriffsverständnis, wie es in der Präambel der durch die OECD im Jahr 2004 veröffentlichten „Grundsätze der Corporate Governance“ * ([Oecd04], S. 11) definiert wurde:

„Corporate Governance“ ist eine der Schlüssel-Voraussetzungen für die Verbesserung von wirtschaftlicher Effizienz und Wachstum wie auch für die Stärkung des Anlegervertrauens. Corporate Governance betrifft die Beziehungen zwischen dem Management (*Geschäftsleitung*) eines Unternehmens, seinem Verwaltungsrat[†] (Board), seinen Anteilseignern (*Shareholder*) und anderen Anspruchsgruppen (*Stakeholder*). Die Corporate Governance liefert auch den strukturellen Rahmen für die Festlegung der Unternehmensziele, die Identifizierung der Mittel und Wege zu deren Umsetzung und der Überwachung des erreichten Erfolgs. Eine gute Corporate Governance soll dem Verwaltungsrat (*Board*) und der Geschäftsleitung[‡] (*Management*) die angemessenen Anreize zur Verfolgung der im Interesse des Unternehmens und seiner Aktionäre liegenden Ziele geben und eine wirkungsvolle Überwachung erleichtern.

In den nun folgenden Abschnitten 4.3 werden vor allem die gesetzlichen und regulativen Anforderungen und im Abschnitt 4.4 die Anforderungen der Kunden und der Öffentlichkeit an das Risikomanagement in einem Unternehmen behandelt.

* Im Jahr 1999 wurden erstmalig durch die OECD Grundsätze zur Corporate Governance veröffentlicht, welche im April 2004 durch sechs überarbeitete und erweiterte Grundsätze ersetzt wurden.

† Das in der englischen Fassung der OECD-Definition genannte „Board“ ist in der Schweiz der „Verwaltungsrat“, in Deutschland der „Aufsichtsrat“ und in den meisten anglo-amerikanischen Ländern das „Board of Directors“ (vgl. [Böck04], S. 1759). Die gesetzlichen Regelungen über dieses oberste Gremium weichen in den verschiedenen Ländern voneinander ab, so dürfen beispielsweise in Deutschland Mitglieder des Vorstandes nicht gleichzeitig Mitglieder des Verwaltungsrates sein. Hingegen sind in Grossbritannien solche Mitgliedschaften erlaubt.

‡ Mit „Management“ in der englischen Fassung ist in der Schweiz vor allem die „Geschäftsleitung“, in Deutschland der „Vorstand“ und in den meisten anglo-amerikanischen Ländern das „Executive Management“ gemeint.

4.3

Anforderungen von Gesetzgebern und Regulatoren

*Umgang mit
Unternehmens-
Risiken*

Die wirtschaftlichen und menschlichen Katastrophen der letzten Jahre infolge von Missbräuchen und falschem Risikoverhalten in den Unternehmensführungen haben die Regulierungsbehörden und Gesetzgeber in einigen Ländern dazu bewogen, die „Corporate Governance“ und den Umgang mit Unternehmens-Risiken straff zu regeln. So sind in den USA, in Ländern der EU und der Schweiz zwingende Rechtsvorschriften entstanden.

*Codes of best
practice*

Daneben gibt es eine Reihe von „Codes of best practice“, wie den „COSO-Report (1992)“ in den USA, den „Cadbury Report (1992)“ und „The combined Code Principles of Good Governance and Best Practices (2000)“ in Grossbritannien, den „Swiss Code of best practices for Corporate Governance (2002)“ in der Schweiz, den deutschen „Corporate Governance Kodex (2002/2003)“ und den „Kodex Corporate Governance (2002)“ in Österreich.

Auch haben mit „Basel II“ umfassende Risikomanagement-Auflagen der Bankenaufsichtsbehörden der G-10-Länder im Banken-Sektor Einzug gehalten. Analog zu diesem Regelwerk in der Bankenbranche ist mit Solvency II auf europäischer Ebene ein Regelwerk zur Eindämmung von Missbräuchen und Risiken in der Versicherungsbranche entstanden, welches am 31.10.2012 in nationales Recht umgesetzt wird. Ausserdem werden über die EU-Gremien verstärkte Regelungen und Harmonisierungen in den Bereichen Corporate Governance, Risikomanagement, Interner Kontrolle und Abschlussprüfung vorangetrieben. Mit der bis Mitte 2008 in lokales Recht umgesetzten „Abschlussprüfer-Richtlinie“, auch EuroSOX genannt, wurde durch die EU ein wichtiger Schritt in dieser Richtung vollzogen.

Alle diese die Corporate Governance berührenden Vorschriften nehmen sich auch dem Thema Risikomanagement in der einen oder anderen Form an, da der verantwortungsvolle Umgang mit Risiken zur ordnungsgemässen Führung eines Unternehmens gehört.

4.3.1

Gesetz KonTraG in Deutschland

*Kontrolle und
Transparenz im
Unternehmensbe-
reich*

In Deutschland wurde 1998 unter dem Kürzel „KonTraG“, ein Gesetz zur „Kontrolle und Transparenz im Unternehmensbereich“ erlassen. Mit diesem Gesetz wird der Vorstand einer Aktiengesellschaft zur Einrichtung eines „Frühwarnsystems“ verpflichtet:

<i>Überwachungssystem</i>	So hat der Vorstand einer Aktiengesellschaft „geeignete Massnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“ (§ 91 Abs. 2 AktG), ([Homm00], S. 8).
<i>Berichterstattung im Lagebericht</i>	Im Weiteren erweitert der deutsche Gesetzgeber die Pflicht der „Berichterstattung im Lagebericht“, indem die Unternehmensführung bei der Darstellung des Geschäftsverlaufs und der Lage der Gesellschaft „auch auf die Risiken der künftigen Entwicklungen einzugehen hat“ (§289 Abs. 2 HS 2 HGB).
<i>Prüfungen des Abschlussprüfers</i>	Beide Forderungen des Gesetzgebers sind durch den Abschlussprüfer gutachterlich zu prüfen: „Bei einer Aktiengesellschaft, die Aktien mit amtlicher Notierung herausgegeben hat, ist ausserdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die im nach § 91 Abs. 2 des AktG obliegenden Massnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgabe erfüllen kann.“ (§317 HGB). Über diese Prüfung hat der Abschlussprüfer gegenüber dem Aufsichtsrat Stellung zu nehmen und seine Prüfungsergebnisse im Testat gegenüber der Allgemeinheit offen zu legen (§321 HGB und §322 HGB) [Homm00]. Zu den Risiken, die mit dem Frühwarnsystem (§ 91 Abs. 2 AktG) frühzeitig erkannt und überwacht werden müssen, gehören auch mögliche Schadensereignisse und Fehlentwicklungen der IT und der Informationssicherheit (z.B. Datenverluste und Datenmissbrauch infolge Cloud-Computing, Malware, Angriffe auf IT-Ressourcen, Datenkorrumpierungen).

4.3.2 Obligationenrecht in der Schweiz

<i>Erweiterungen des Aktienrechts</i>	In der Schweiz sind 1992 Erweiterungen des Aktienrechts im „Schweizerischen Obligationenrecht“ in Kraft gesetzt worden, welche die Verantwortlichkeiten regeln.
<i>Unübertragbare und unentziehbare Aufgaben</i>	Gemäss Art 716a, Ziffer 1, OR gehören beispielsweise zu den „unübertragbaren und unentziehbaren Aufgaben“ des Verwaltungsrats: 1. die Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen; 2. die Festlegung der Organisation; (...)

5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen; (...).

Art. 716a, Ziffer 2, OR legt weiter fest: „Der Verwaltungsrat kann die Vorbereitung und die Ausführung seiner Beschlüsse oder die Überwachung von Geschäften Ausschüssen oder einzelnen Mitgliedern zuweisen. Er hat für eine angemessene Berichterstattung an seine Mitglieder zu sorgen.“

Organhaftung

Zum Thema Organhaftung hält B. Lehmann fest ([Lehm02], S. 28):

„Die Mitglieder von Verwaltungsrat und Geschäftsleitung können aufgrund ihrer Garantenstellung persönlich haftbar werden, wenn Schäden aus einem Datenunfall auf eine Vernachlässigung ihrer Pflichten im Zusammenhang mit Aufbau, Organisation, Aufsicht und Kontrolle eines Systems zur Informationssicherung zurückzuführen sind.“

Aufgrund der Finanzskandale im In- und Ausland sowie im Zuge der internationalen Harmonisierungen wurde per 1.1.2008 das „Schweizerische Obligationenrecht“ dahingehend erweitert, dass „Risikomanagement“ und „Internes Kontrollsystem“ zur Pflicht geworden sind.

Pflicht für Risikomanagement: Art. 663b, Ziffer 12 OR

So werden mit Artikel 663b, Ziffer 12 OR im Anhang des Geschäftsberichts (Jahresrechnung) in der Verantwortlichkeit des Verwaltungsrats Angaben zur Risikobeurteilung gefordert: *„Der Anhang enthält: (...) 12. Angaben über die Durchführung einer Risikobeurteilung. (...)“*. Die Gesetzesänderung gilt insbesondere für Aktiengesellschaften, GmbHs, Genossenschaften und Stiftungen und verpflichtet alle betroffenen Rechtsformen unabhängig von ihrer Grösse.

Pflicht für Internes Kontrollsystem: Art. 728 a/b OR

Die Pflicht für ein Internes Kontrollsystem (IKS) aufgrund des Artikels 728a/b OR richtet sich an Unternehmen, die der „ordentlichen Revision“ unterliegen.

Der ordentlichen Revision unterliegen Gesellschaften dann, wenn sie in zwei aufeinanderfolgenden Geschäftsjahren zwei der drei folgenden Kriterien überschreiten (Artikel 727 OR)*:

- a. Bilanzsumme CHF 20 Mio.

* Inkrafttreten dieser geänderten Fassung am 1. Januar 2012

b. Jahresumsatz CHF 40 Mio.

c. Mehr als 250 Vollzeitstellen im Jahresdurchschnitt

Die bezüglich IKS am 1.1.2008 in Kraft getretenen Neuerungen lauten:

Artikel 728a OR:

„Die Revisionsstelle prüft, ob: 1. (...); 2. (...); 3. ein internes Kontrollsystem existiert. (...)“

Artikel 728b OR:

„Die Revisionsstelle erstattet dem Verwaltungsrat einen umfassenden Bericht mit Feststellungen über die Rechnungslegung, das IKS sowie die Durchführung und das Ergebnis der Revision.“ (...).

Was zumindest in der Schweiz unter IKS verstanden wird, kann dem „Schweizer Handbuch für Wirtschaftsprüfung“* wie folgt entnommen werden:

Unter „Interner Kontrolle“ (Synonym: Internes Kontrollsystem) werden alle von Verwaltungsrat, Geschäftsleitung und übrigen Führungsverantwortlichen angeordneten Vorgänge, Methoden und Massnahmen verstanden, die dazu dienen, einen ordnungsgemässen Ablauf des betrieblichen Geschehens sicherzustellen. Die organisatorischen Massnahmen der Internen Kontrolle sind in die betrieblichen Abläufe integriert.

* Treuhand Kammer, Schweizer Handbuch der Wirtschaftsprüfung 1998, Band 2, S. 171.

4.3.3

Swiss Code of best Practice for Corporate Governance

In der Schweiz wurde am 25. März 2002 ein „Code of best Practice“ zur „Corporate Governance“ durch den Vorstand der *économiesuisse**, auf einstimmige Empfehlung einer Expertengruppe „Corporate Governance“ hin genehmigt†

Swiss Code

Der „Swiss Code“ wird durch Organisationen und Unternehmensverbände der Schweiz, wie Schweizerische Bankiervereinigung, Schweizerische Gesellschaft für Chemische Industrie, Schweizerischer Gewerbeverband, Vereinigung der privaten Aktiengesellschaften, mitgetragen.

Der „Swiss Code“ wendet sich im Sinne von Empfehlungen an die schweizerischen Publikumsgesellschaften. Auch nicht kotierte volkswirtschaftlich bedeutende Gesellschaften oder Organisationen (im Übrigen auch in anderer Rechtsform als derjenigen einer Aktiengesellschaft) können dem „Swiss Code“ zweckmässige Leitideen entnehmen ([Scod02], S. 4).

Verantwortlichkeit zum Umgang mit Risiken

Zum Umgang mit Risiken weist der „Swiss Code“ dem Verwaltungsrat unter der Ziffer 19 folgende Verantwortlichkeiten zu ([Scod02], S. 13):

„Der Verwaltungsrat sorgt für ein dem Unternehmen angepasstes internes Kontrollsystem und Risikomanagement.“

- *Das interne Kontrollsystem ist der Grösse, der Komplexität und dem Risikoprofil der Gesellschaft anzupassen.*
- *Das interne Kontrollsystem deckt, je nach den Besonderheiten der Gesellschaft, auch das Risikomanagement ab; dieses bezieht sich sowohl auf finanzielle wie auf operationelle Risiken.*
- *Die Gesellschaft richtet eine interne Revision ein. Diese erstattet dem Prüfungsausschuss („Audit Committee“) oder gegebenenfalls dem Präsidenten des Verwaltungsrats Bericht.“*

* Wirtschafts-Dachverband der Schweizer Unternehmer.

† 2007 wurde ein Anhang 1 „Empfehlungen zu den Entschädigungen von Verwaltungsrat und Geschäftsleitung“ zugefügt.

4.3.4

Rahmenwerke Basel II und Basel III

*Neue Kapital-
vereinbarungen:
Basel II*

*Risiken mit Eigen-
kapital unterlegen*

*Aufschläge auf
Kreditzinssatz*

Speziell für Finanzinstitute sind die Rahmenvereinbarungen des Baseler Ausschusses für Bankenaufsicht unter dem Begriff „**Basel II**“ zu nennen. Das am 26.6.2004 verabschiedete Rahmenwerk* umfasst im Wesentlichen die adäquate Unterlegung von Kredit-, Markt- und operationellen Risiken der Banken mit Eigenkapital. Auch sind die Banken verpflichtet, die Kreditrisiken in Abhängigkeit vom Risiko des Kreditnehmers mit Eigenkapital zu unterlegen. Die massgeblichen Bonitätseinstufungen erfolgen dabei durch interne oder externe Ratings.

Der Kreditzinssatz von Banken an die kreditnehmenden Unternehmen wird demzufolge umso höher, je höher die Risiken des Unternehmens sind. Damit erhält der Kreditzinssatz aufgrund der Risiken zusätzliche Aufschläge (s. Abbildung 4.2).

Basispunkte		Betriebskosten	Unternehmensspezifischer Bonitäts-Spread
		Kosten für operationelle Risiken	
		Ausfallwagnis in Abhängigkeit von der Ausfall-Wahrscheinlichkeit	
		Eigenkapitalverzinsung der Bank	
		Kosten für Geldeinkauf	

Abbildung 4.2: Zusammensetzung Kreditzinssatz infolge Basel II [Bein03], S. 30)

* Titel: International Convergence of Capital Measurement and Capital Standards – A Revised Framework [Bisf04].

	Im Sinne stabiler Finanzmärkte werden zudem Vorschriften über „aufsichtliche Prüfverfahren“ sowie „Marktdisziplin durch Offenlegung“ erlassen.
<i>Drei Säulen</i>	Somit wird die Vereinbarung auf den drei Säulen: „Mindestkapitalanforderungen“, „aufsichtlicher Überprüfungsprozess“ und „Marktdisziplin“ getragen.
<i>Bessere Risikomanagement-Praktiken</i>	Die Rahmenvereinbarung sollte vor allem die Anwendung besserer „Risikomanagement-Praktiken“ durch den Bankensektor fördern und eine weitere Stärkung der Solidität und Stabilität des internationalen Bankensystems unter Beibehaltung hinreichender Konsistenz sicherstellen. Der Vereinbarung haben die Zentralbank-Gouverneure und Leiter der Bankenaufsichtsbehörden der G-10-Länder zugestimmt und war für international tätige Banken der Mitgliedstaaten des Baseler Ausschusses bis Ende 2006 umzusetzen. Für Institute, welche sog. „fortgeschrittene“ Messansätze zur „Risiko-Messung“ verwenden, gelten die Bestimmungen ab Ende 2007. (Aufgrund von Verzögerungen in den USA hat der Baseler Ausschuss die Inkraftsetzung des fortgeschrittenen internen „rating-basierenden“ Ansatzes zur Eigenmittelbemessung auf den 1.1.2008 verschoben). Die Inkorporierung von Basel II in Europäisches Gemeinschaftsrecht wurde inzwischen durch den Rat am 14. Juni 2006 in Form der „Capital Requirement Directive“ erlassen*. Die nationale Umsetzung der EU-Richtlinie ist beispielsweise in Deutschland in einem entsprechenden Gesetz vom 17.11.2006 erfolgt und per 1.1.2007 in Kraft gesetzt worden. In der Schweiz erfolgte die Umsetzung in schweizerisches Recht anhand der Rundschreiben der Eidg. Bankenkommission† (EBK 06/1 bis EBK 06/5) per 1.1.2007. Bei den zu bewertenden Risiken spielen nicht nur die Markt- und Kreditrisiken, sondern auch die operationellen Risiken sowohl der Banken als auch der Kreditkunden eine massgebliche Rolle.

* Obwohl die EU-Richtlinie stark an die Baseler Vereinbarungen angelehnt ist, ergeben sich bei der Umsetzung einzelner Anforderungen Unterschiede (vgl. [Foll07], 35 u. 36).

† Seit 1.1.2009 liegt Zuständigkeit bei „FINMA“.

*Operationelles
Risiko nach
Basel II*

Das operationelle Risiko definiert der Baseler Ausschuss in Basel II wie folgt:

Operationelles Risiko ist die Gefahr von Verlusten, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder in Folge externer Ereignisse eintreten.

Diese Definition schliesst Rechtsrisiken ein, beinhaltet aber nicht strategische Risiken oder Reputationsrisiken.

*Messansätze Basel
II für OpRisk*

Von den mit Basel II vorgegebenen Ansätzen zur Bestimmung der Eigenkapital-Unterlegung interessieren im Rahmen dieses Buches die Ansätze für operationelle Risiken, die in der folgenden Abbildungen 4.3 und 4.4 kurz zusammengestellt sind:

Basisindikatoransatz (BIA):

- Banken mit geringen operationellen Risiken;
- 15% der durchschnittlichen Bruttoerträge der vergangenen 3 Jahre als Eigenkapitalunterlegung.

Standardansatz (STA):

- Einstiegsansatz für international tätige Banken sowie Banken mit signifikantem OpRisk;
- Bruttoerträge im Dreijahresdurchschnitt auf acht Geschäftsfelder differenziert, mit festgesetzten bankenaufsichtlichen „Beta-Faktoren“ multipliziert;
- Gesamtkapitalunterlegung für operationelle Risiken resultiert aus Summierung über die Geschäftsfelder;

Alternativer Standardansatz (ASA) für Nicht-G-10-Banken verwendet statt Bruttoerträge die durchschnittlichen Portfolio-Volumen.

Fortgeschrittene (ambitionierte) Messansätze (AMA):

- Billigung durch nationale Bankenaufsicht (in der Schweiz FINMA, in Deutschland BaFin und in Österreich FMA);
- Ermittelt die bankspezifischen, individuellen Risiken einer Bank, was zu einem optimierten Eigenmittelbedarf führt;
- Interne Ermittlung der Eigenmittelanrechnungsbeträge mittels Verlustdaten über mindestens 5 Jahre (übergangsweise 3 Jahre), Externe Verlustdaten, Szenarien-Analysen sowie qualitative Komponenten (Ratings, Key Risk Indikatoren, Selfassessments etc.);

Bis zu 20 % Minderung durch Anerkennung von Versicherungen.

Abbildung 4.3: Messansätze Basel II für operationelles Risiko

*Fortgeschrittene
Bemessungsan-
sätze für OpRisk*

Als **fortgeschrittene Bemessungsansätze** für das **operationelle Risiko** wurden in einem Arbeitspapier des Baseler Ausschusses einige Verfahren vorgeschlagen, die in Abbildung 4.4 im Überblick dargestellt werden ([Bisw01], S. 33-35):

Interner Bemessungs-Ansatz (IMA=Internal Measurement Approach):

$$UL = \sum_{i=1}^n \sum_{j=1}^m \gamma_{i,j} \times EI_{i,j} \times PE_{i,j} \times LGE_{i,j}$$

UL : Unerwarteter Gesamtverlust

mit

$\gamma_{i,j}$: Gamma-Faktor für Geschäftsfeld i und Schadensereignistyp j

$EI_{i,j} \times PE_{i,j} \times LGE_{i,j}$: Erwarteter Verlust (p.a.) im Geschäftsfeld i für den Schadensereignistyp j

mit

$EI_{i,j}$: Exposure Indikator für Geschäftsfeld i und Schadensereignistyp j

$PE_{i,j}$: Eintrittswahrscheinlichkeit von Schadensereignistyp j im Geschäftsfeld i

$LGE_{i,j}$: Mittlerer Verlust eines Schadensereignisses

Anhand des „γ-Faktors“ werden die analysierten erwarteten Verluste in unerwartete Verluste umgerechnet. Der γ-Faktor ist in Abhängigkeit der Häufigkeitswerte für ein bestimmtes „Konfidenzintervall“ (z.B. 99.9 % Quantil) in Form einer Tabelle vorgegeben. Zum Genauigkeitswert dieser relativ einfachen Berechnungsmöglichkeit für relativ „seltene“ Ereignisse gilt es zu berücksichtigen, dass die Hochrechnung der „unerwarteten Verluste“ mittels Gammafaktor nicht auf aktuellen Daten im „Verteilungsschwanz“ beruht und zudem die Summation der Einzelrisiken ein zu hohes Gesamtrisiko vorgibt.

Verlustverteilungs-Ansatz (LDA=Loss Distribution-Approach):

Die Interne Berechnung der Höhe des zu unterlegenden Eigenkapitals wird auf der Basis interner historischer Daten sowie des „Operational Value at Risk“ und allenfalls mit Hilfe der Monte-Carlo-Simulation durchgeführt.

Scorecard-Ansatz (SCA=Scorecard-Approach)

Anhand eines intern definierten Kennzahlensystems wird die Höhe des zu unterlegenden Eigenkapitals berechnet.

(Anm.: Die Variablen-Bezeichnungen sind im Rahmen von Basel II standardisiert.)

Abbildung 4.4: Vorgeschlagene Bemessungsansätze für operationelle Risiken

Inwieweit diese fortgeschrittenen Ansätze für seltene Schadensfälle mit hohem Ausmass aufgrund der in einer Bank vorhandenen Datenbasis zu akzeptablen Ergebnissen führen, unterliegt dem Urteil der nationalen Bankenaufsicht.

Als hoffnungsvoller Ansatz kann die auf einer Expertenbefragung beruhenden **Szenario-Analyse** erwähnt werden, da damit insbesondere für die Informationssicherheits- und IT-Risiken auch Prognosen für die Zukunft angemessen berücksichtigt werden können (s. Abschnitt 3.2.6.).

Mindestanforderungen bei Standardansatz

Wählt eine Bank beispielsweise den sogenannten Standardansatz für die Eigenkapitalunterlegung, dann müssen, wie der folgende Auszug zeigt, bestimmte Mindestanforderungen erfüllt werden:

- Die oberste Leitungsebene (oberstes Verwaltungsorgan und Geschäftsleitung) ist in angemessenem Umfang aktiv in die Überwachung des Management-Systems für operationelle Risiken involviert.
- Die Bank verfügt über ein konzeptionell solides Risikomanagement-System für operationelle Risiken, das vollständig umgesetzt und integriert wurde.
- Die Bank verfügt über ausreichende Ressourcen zur Umsetzung des Ansatzes, sowohl in den wichtigsten Geschäftsfeldern als auch in den Kontroll- und Revisionsbereichen.

Zusätzliche Anforderung für international tätige Bank

Zur Anwendung des vorerwähnten Standard-Ansatzes muss eine international tätige Bank noch zusätzlich die folgenden Anforderungen erfüllen:

- a) Die Bank muss für den Bereich der operationellen Risiken über ein Management-System verfügen, das einer für das Management der operationellen Risiken verantwortlichen Stelle klare Verantwortungen zuweist. Diese Einheit ist dafür verantwortlich, dass Strategien zur Identifikation, Bewertung, Überwachung und Steuerung/Minderung operationeller Risiken entwickelt werden; dass unternehmensweit geltende Grundsätze und Verfahren für Management und Kontrolle der operationellen Risiken niedergelegt werden; dass eine Methodik zur Bewertung der operationellen Risiken entwickelt und umgesetzt wird; und dass ein Berichtssystem für operationelle Risiken entwickelt und implementiert wird.

- b) Als Teil des bankinternen Systems zur Bewertung der operationellen Risiken muss die Bank systematisch die relevanten Daten zum operationellen Risiko einschliesslich erheblicher Verluste je Geschäftsfeld sammeln. Das System zur Bewertung der operationellen Risiken muss eng in die Risikomanagementprozesse der Bank integriert sein. Dessen Ergebnisse müssen fester Bestandteil der Risikoprofilüberwachungs- und Kontrollprozesse sein. Zum Beispiel müssen diese Informationen im Risiko-Bericht, im Management-Bericht und in der Risiko-Analyse eine wesentliche Rolle spielen. Die Bank muss Methoden zur Schaffung von Anreizen zur Verbesserung des Managements operationeller Risiken innerhalb der Gesamtbank verfügen.

*Zulieferer und
Geschäftspartner*

Die Bewertung nach Risiken erfolgt nicht nur für Finanzinstitute und deren Kreditkunden, sondern auch für Zulieferer und Geschäftspartner der Bankkunden.

*Risikomanage-
ment-System*

Es gehört deshalb zum ureigensten Interesse nicht nur der Finanzinstitute, sondern auch aller anderen in die Finanzmärkte eingebundenen Unternehmen, sich ein Risikomanagement-System aufzubauen, das zu den Geschäftsrisiken auch die operationellen Risiken nach prüfbaren Standards unter Kontrolle umfasst.

Die Ausgestaltung des Managements und der Überwachung von operationellen Risiken wird durch den Baseler Ausschuss für Bankenaufsicht mit zusätzlichen Papieren unterstützt. So werden in den „Sound Practices for the Management and Supervision of Operational Risk“ zehn Grundsätze zur Ausgestaltung angegeben [Biss03]. Auch werden die Typen von operationellen Risiko-Ereignissen spezifiziert und mit Beispielen untermauert (s. Abbildung 4.5):

Basel II Ereignis-Typen	Beispiele
Interne betrügerische Handlungen	• Nicht gemeldete Transaktionen (vorsätzlich) • Unzulässige Transaktionen (mit finanziellem Schaden) • Falschbezeichnung einer Position (vorsätzlich) • Betrug / Kreditbetrug / Einlagen ohne Wert • Diebstahl / Erpressung / Unterschlagung / Raub • Veruntreuung von Vermögenswerten • Böswillige Vernichtung von Vermögenswerten • Fälschung
Externe betrügerische Handlungen	• Diebstahl / Raub / Betrug • Fälschung • Schäden durch Hackeraktivitäten • Diebstahl von Informationen (mit finanziellem Schaden)
Beschäftigungspraxis und Arbeitsplatzsicherheit	• Probleme aufgrund Löhne, Gehälter, Sozialleistungen, Kündigung • Gewerkschaftsaktivitäten • Haftpflicht (Ausrutschen und Stürzen usw.) • Verstoss gegen Gesundheits- und Sicherheitsbestimmungen • Diskriminierung
Kunden, Produkte und Geschäftsgepflogenheiten	• Verstoss gegen treuhänderische Pflichten • Verletzung von Informationspflichten gegenüber Kunden • Verletzung von Datenschutzbestimmungen • Missbrauch vertraulicher Informationen • Insidergeschäfte (auf Rechnung des Arbeitgebers) • Unerlaubte Geschäftstätigkeit • Geldwäsche • Produktmängel • Versagen bei der Kundenprüfung gemäss Richtlinien
Physische Schäden	• Verluste durch Naturkatastrophen (Wasser, Erdbeben usw.) • Personenschäden aufgrund von externen Ereignissen
Geschäftsunterbrechungen und Systemausfälle	• Hardware, Software oder Telekommunikation • Ausfall/Störung der Versorgungseinrichtungen
Abwicklung, Lieferung und Prozessmanagement	• Verständigungsfehler • Fehler bei der Dateneingabe, -pflege oder -speicherung • Nichterfüllung von Vertragspunkten • Buchungsfehler / falsche Kontozuordnung • Fehlerhafte Lieferung • Fehlerhafte Verwaltung von Besicherungsinstrumenten • Nichteinhaltung zwingender Meldepflichten • Fehlende/unvollständige Rechtsdokumente • Unberechtigter Zugriff auf Konten • Fehlerhafte Kundenunterlagen (Schaden eingetreten) • Outsourcing • Auseinandersetzungen mit Lieferanten oder Geschäftspartnern

Abbildung 4.5: Operationelle Verlust-Ereignis-Typen (vgl. [Bisr06], S. 305-307)

IT-Risiken

Wie aus der Liste der operationellen Verlust-Ereignis-Typen ersichtlich ist, gehören die Informationssicherheits- und IT-Risiken

zu den operationellen Risiken. Die Kontrolle und Bewältigung dieser Risiken erfolgt weitgehend nach standardisierten Methoden, wie sie im dritten Teil dieses Buches behandelt werden (z.B. CobiT oder ISO 27002).

Basel III Rahmenwerk

Als Konsequenz aus der Finanzmarktkrise in den Jahren 2007 und 2008 wurde durch den Baseler Ausschuss am 16. Dezember 2010 das neue Basel III-Rahmenwerk* finalisiert. Das Rahmenwerk enthält vor allem verschärfte Anforderungen für die Anrechenbarkeit von Eigenmitteln und erhöhte Mindestkapitalquoten sowie die Einführung einer „Leverage Ratio“ (Verschuldungsgrenze) als weitere Risikokennzahl. Enthalten ist auch der Aufbau von gegenzyklischen Kapitalerhaltungspuffern sowie die verstärkte Abfederung des „Kontrahentenausfallrisikos“. Ebenfalls werden Vorschriften und Massnahmen zur Überwachung und Gewährleistung der Liquidität definiert. Die Umsetzung des Rahmenwerks mit der schrittweisen Erhöhung der Kapitalquoten erfolgt ab 1. Januar 2013 bis 1. Januar 2019.

4.3.5

Sarbanes-Oxley Act (SOX) der USA

Am 30. Juli 2002 wurde in den USA der Sarbanes-Oxley Act (SOX) in Kraft gesetzt. Das Gesetz ist nach den beiden Kongress-Abgeordneten und Initianten Paul S. Sarbanes und Michael G. Oxley benannt.

Massnahme der US-Regierung

Das Gesetz ist eine Massnahme der US-Regierung gegen Pleiten namhafter Firmen (z.B. Enron und Worldcom), die auf mangelhafte und manipulierte Buchführung sowie Unzulänglichkeiten bei der Wirtschaftsprüfung (z.B. Arthur Anderson) zurückzuführen waren. Die massiven Bilanzfälschungen der Worldcom in Höhe von 11 Mrd. US \$ hatten 2002 zum grössten Konkurs in der amerikanischen Geschichte geführt. Von einem einstigen Börsenwert des Unternehmens auf dem Höhepunkt von 180 Mrd. US \$ ist für die Aktionäre lediglich ein kleiner symbolischer Restbetrag als „Trostpflaster“ übrig geblieben.

Die bei solchen Firmenzusammenbrüchen entstandenen Schäden hatten ihren Niederschlag besonders in der Finanz- und Volkswirtschaft der USA, aber auch in anderen Ländern. Ziel des Gesetzes ist, den Kapital-Anlegern mehr Sicherheit zu bringen.

* “Basel III: A global regulatory framework for more resilient banks and banking systems”.

<i>Corporate Governance, Berichterstattung und Interne Kontrolle</i>	Das Gesetz enthält neue Bestimmungen der „Corporate Governance“, der „Berichterstattung“ und der „Internen Kontrolle“. Diese Bestimmungen müssen von bestimmten Firmen des öffentlichen Sektors und solchen, die an der amerikanischen Börse (US Securities and Exchange Commission) registriert sind, strikt eingehalten werden.
<i>Entzug Börsenkotierung und hohe Haftstrafen</i>	Verstösse gegen das Gesetz können den Entzug der Börsenkotierung und hohe Haftstrafen (10 bis 20 Jahre) für Mitglieder der Unternehmensleitung (Board Members und Executive Management) zur Folge haben.
<i>Section 404 SOX-Gesetz</i>	Die Section 404 des Sarbanes-Oxley Gesetzes behandelt die „Interne Kontrolle“ des „Financial Reportings“ (Überprüfung der Berichterstattung und Offenlegung der Geschäftstätigkeit des Unternehmens). Die Wirtschaftsprüfer müssen entsprechend diesem Gesetz nicht nur die Richtigkeit der im Finanzergebnis ausgewiesenen Zahlen überprüfen, sondern auch den unternehmensinternen Prozess und die Fehlerfreiheit der Systeme beurteilen, die zu diesen Zahlen geführt haben. Genau dieser Punkt hat in jüngster Zeit zu heftigen Kontroversen geführt und ist durch Wirtschaftsprüfer, nicht zuletzt als Selbstschutz, aussergewöhnlich breit interpretiert worden. Der SEC*-Vorsitzende Christopher Cox habe sich in einem Gespräch mit Journalisten dahingehend geäussert, <i>„die Vorschriften (...) neu zu interpretieren und die Dinge, die keinen Bezug auf die finanziellen Ergebnissen hätten, nicht länger als wesentlich anzusehen“</i> [†] .
<i>COSO-Standards zur internen Kontrolle</i>	Das Sarbanes-Oxley Gesetz fordert die Unternehmen auf, eine passende „Internal Control Structure“, zu wählen und einzusetzen. Diese „Internal Control Structure“ muss jährlich auf ihre Wirksamkeit hin überprüft und durch das Management berichtet werden. Die mit der Überwachung der SOX-Compliance beauftragte „US Securities and Exchange Commission“ (SEC) macht konkret zur Auflage, ein anerkanntes Framework für interne Kontrolle anzuwenden und referenziert dabei die COSO [‡] -Standards zur internen Kontrolle [Cosa02].

* SEC=Securities and Exchange Commission: US-amerikanische Wertpapier- und Börsenaufsicht.

† Revision von Sarbanes-Oxley angestrebt, Neue Zürcher Zeitung, 12. November 2006.

‡ COSO = Committee of Sponsoring Organizations of the Treadway Commission

Die Reporting-Zahlen werden meist aus den IT-Systemen der gesamten Wertekette des Unternehmens extrahiert und mit den Buchhaltungssystemen des Unternehmens aufbereitet, daher ist auch das Management der Informations-Risiken eine wesentliche Anforderung der Section 404 des Sarbanes-Oxley Act.

*Section 302
SOX-Gesetz*

Section 302 des Sarbanes-Oxley Acts fordert das Management auf, sowohl vierteljährlich als auch jährlich zu bescheinigen, dass die interne Kontrolle unter ihrer Aufsicht und Verantwortung die für die Finanz-Berichtserstattung wesentlichen Informationen ordnungsgemäss offenlegt. Die Offenlegungen müssen autorisiert, komplett und korrekt aufgezeichnet, sowie in der durch die SEC geforderten Regeln, Formularen und Fristen zusammengefasst und berichtet werden.

Unternehmen, die Dienstleistungen für andere Unternehmen erbringen, welche der SOX-Pflicht unterliegen, müssen ebenfalls SOX einhalten.

*IT-Kontroll-
Framework CobiT*

Das „IT Governance Institut“ der ISACA mit seinem umfassenden IT-Kontroll-Framework CobiT (Control Objectives for Information and related Technology) hat die Kontroll-Prozesse des COSO-Frameworks zur Erfüllung des SOX-Gesetzes im IT-Bereich auf IT-relevante Kontroll-Ziele des CobiT-Frameworks abgebildet.

*COSO/CobiT-
Mapping*

Nachfolgende Abbildung 4.6 zeigt anhand von Beispielen die Erfüllung der fünf „COSO-Komponenten“ durch CobiT-Kontrollziele. Ausführliche „Mapping“-Tabellen können dem Dokument „IT Control Objective for Sarbanes-Oxley, 2nd Edition“ des IT Governance Instituts entnommen werden [ITgs06].

COSO Kontroll- komponenten	CobiT-Kontrollziele (ausgewählte Beispiele)	Ebene	
		Umgebung	Aktivität
Kontroll- Umgebung	PO 4.2: „Organisatorische Einordnung der IT-Funktionen“	x	
	PO 6.1: „Positive Informations-Kontrollumgebung“	x	
	PO 6.2: „Verantwortung des Managements für Weisungen“	x	
	...		
Risiko- Assessment	PO 9.0: „Risikobeurteilung“	x	
	...		
Kontroll- Aktivitäten	AI 1.4: „Anforderungen Drittparteien-Dienstleistungen“		x
	AI 6.0-6.8: „Änderungswesen“		x
	DS 5.0-5.21: „Systemsicherheit“		x
	DS 10.0-10.5: „Problem- und Incidentmanagement“		x
	DS 11.0-11.30: „Verwaltung von Daten“		x
	...		
Information und Kommunikation	PO 6.0-6.11: „Kommunikation von Zielsetzungen und Richtung des Managements“	x	
	DS 10.0-10.5 „Problem- und Incidentmanagement“		x
	...		
Überwachung	ME 2.0-2.4: „Überwachung und Beurteilung der internen Kontrollen“	x	
	DS 10.0-10.5 „Problem- und Incidentmanagement“		x
	...		

Abbildung 4.6: Erfüllung von COSO-Komponenten durch CobiT-Kontrollziele*

* Weitergehende Erläuterungen zur Konzeption der CobiT-Prozesse und -Kontrollziele s. Abschnitt 9.4

4.3.6**EuroSOX***8. EU Richtlinie*

Wie in den USA haben Skandale weltweit tätiger europäischer Unternehmen wie Parmalat oder Ahold eine Verschärfung und Vereinheitlichung der gesetzlichen Anforderungen an die Prüfung und Berichterstattung von Unternehmen auf europäischer Ebene deutlich gemacht. Zur Wiederherstellung des Vertrauens der Investoren in die Märkte und Unternehmen hat, ähnlich dem amerikanischen SOX, das Europäische Parlament und der Rat im Juni 2006 die Neufassung der 8. EU Richtlinie („Abschlussprüfer-Richtlinie“) verabschiedet. Der Zweck der Richtlinie ist „eine Harmonisierung der Anforderungen an die Abschlussprüfung auf hohem Niveau, wenn auch eine vollständige Harmonisierung nicht angestrebt wird“.

Die Änderungen zweier bestehender Richtlinien (4. und 7. EU-Richtlinie), die in der neuen 8. Richtlinie angesprochen werden, sind ebenfalls seit dem Juli 2006 in Kraft. Darin wird beispielsweise eine Erklärung über die Unternehmensführung im Lagebericht, der die wichtigsten Merkmale des Internen Kontrollsystems (IKS) und des Risikomanagement-Systems beschreibt, verlangt.

Die Umsetzung der neuen 8. Richtlinie (auch EuroSOX genannt) in lokales Recht war durch die Mitgliedstaaten bis zum 29. Juni 2008 durchzuführen.

Qualität der Audits, Abschlussprüfer und Prüfungsgesellschaften

Zu den vielen neuen Regelungen hinsichtlich Qualität der Audits, der Abschlussprüfer und der Prüfungsgesellschaften wird die Einführung eines Prüfungsausschusses (wie „Audit Committee“ bei SOX) und ein wirksames internes Kontrollsystem verlangt, mit denen die finanziellen und betrieblichen Risiken sowie das Risiko von Vorschriftenverstößen auf ein Mindestmass begrenzt und die Qualität der Rechnungslegung verbessert werden.

Direkt betroffen von der neuen Richtlinie sind Unternehmen, die unter das Recht eines Mitgliedstaates fallen und deren übertragbaren Wertpapiere zum Handel auf einem geregelten Markt eines Mitgliedstaates zugelassen sind. Die Mitgliedstaaten können auch zusätzlich „Unternehmen des öffentlichen Interesses“ bestimmen, auf welche die Richtlinie anzuwenden ist, wenn ein solches Unternehmen aufgrund der Art, der Tätigkeit, dessen Grösse oder Zahl der Beschäftigten von erheblicher öffentlicher Bedeutung ist.

Für die IT eines von EuroSOX betroffenen Unternehmens gilt es vor allem, wie bei SOX, regelkonforme IT-Systeme bereitzustellen.

len und die geforderte „Compliance“ mit Hilfe von IT-Systemen durchzusetzen. Ein hauptsächliches Augenmerk gilt denjenigen Prozessen und IT-Systemen, mit denen Geldflüsse abgewickelt und überwacht werden. In Deutschland beispielsweise müssen ab Juli 2008 alle Kapitalgesellschaften ein IT-Sicherheitskonzept vorweisen.

Die wichtigsten Anforderungen an die IT, die von EuroSOX abgeleitet werden können, sind (vgl. [Comw08]):

- Steuerung der IT-Infrastruktur, Organisation Applikationsentwicklung und Pflege;
- Steuerung und Überwachung der logischen und physischen Zugriffs- und Zutrittssicherheit (Berechtigungswesen, umfeldbedingte Sicherheit);
- Steuerung und Überwachung der Kommunikationssicherheit (z.B. Firewalls) und Schutz gegen Software- und Datenkorruptionen (z.B. Virenschutz);
- Planungen für den Erhalt der Betriebs- und Geschäftskontinuität und der Erstellung von Notfallkonzepten;
- Überwachung der Systementwicklung und der IT-Projekte, des Systembetriebs sowie der Speicherung der relevanten Daten und Dokumente für Nachvollzug und Archivierung.

Selbstverständlich wird der in der Disziplin IKS (Internes Kontrollsystem) geschulte Abschlussprüfer auch prüfen, inwiefern die getroffenen Massnahmen die Risiken adäquat abdecken.

Für Lücken haftet der Geschäftsführer respektive der Vorstand (Geschäftsleitung) vollumfänglich. Bei Nichteinhaltung können Haftungsklagen, Marktzugangsbarrieren sowie Schwierigkeiten für die Kreditaufnahme entstehen, aber insbesondere die Verweigerung des Testats durch den Wirtschaftsprüfer resultieren.

4.3.7

Datenschutz: Eine wichtige Unternehmensanforderung

Der Datenschutz als gesetzliche Anforderung an die Unternehmen erhält eine immer höhere Wichtigkeit, wenn es um Compliance und Risiken im Zusammenhang mit Informationen geht. Eine wesentliche Herausforderung besteht in der zunehmenden Vielfalt von Beteiligten in den Dienstleistungsketten heutiger Informationsverarbeitungen.

Drittfirmen als Service-Provider

So kommen beispielsweise als „Service-Provider“ vermehrt Drittfirmen ins Spiel. Diese Vielfalt geht einher mit dem rasanten Anwachsen von technologischen Möglichkeiten.

Als Beispiele seien genannt: Die fast überall verfügbare drahtlose Vernetzung der Daten (z.B. über Internet, E-Mail), die sozialen Netzwerke, das Cloud-Computing, die mobilen Gerätetechnologien, die miniaturisierten Ton-, Bild- und Videoaufzeichnungen und die mobilen hochvolumigen Speichertechnologien.

Persönlichkeitsrechte an Informationen

Mit dem unbestrittenen Nutzen, den all diese Technologien erbringen können, gehen auch Risiken hinsichtlich der Persönlichkeitsrechte an den Informationen einher, für deren angemessenen Schutz auch die Betreiber solcher Technologien Verantwortung tragen.

Begrifflichkeit des Datenschutzes

Zur Begrifflichkeit des Datenschutzes gibt es weltweit bisher kein Übereinkommen. So versteht die Europäische Richtlinie* unter Datenschutz „insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten“.† In der Zweckbestimmung des deutschen Bundes-Datenschutzgesetzes (BDSG) heisst es hingegen: „(...) den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsbereich beeinträchtigt wird.“ Das Datenschutzgesetz in Österreich beschreibt Datenschutz (DSG 2000) als „(...) Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.“

juristische Personen in Schweiz und Lichtenstein

Die Schweiz und Lichtenstein definieren Datenschutz (DSG) als „Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.“, wobei hier die Anwendung ausdrücklich sowohl auf natürliche als auch auf juristische Per-

* Die Allgemeine Datenschutzrichtlinie der EU (95/46/EG) wurde durch eine bereichsspezifische Richtlinie „Datenschutzrichtlinie für elektrische Kommunikation“ (2002/58/EG) ergänzt. Inzwischen ist eine weitere EU-Richtlinie 2009/136/EG dazugekommen, die vor allem die Verwendung von „Cookies“ beim Internet-Browsen regelt, z.B. dass die Nutzer ausdrücklich in die Platzierung von Cookies einwilligen müssen.

† Die Richtlinie beschreibt Mindeststandards für den Datenschutz, die in allen Mitgliedstaaten der Europäischen Union durch nationale Gesetze sichergestellt werden müssen. Die Richtlinie soll im Rahmen der Datenschutzreform durch die Datenschutz-Grundverordnung abgelöst werden.

	sonen gilt. Die Datenschutz-Richtlinie der EU sowie die Datenschutzgesetze von Deutschland und Österreich klammern die Daten von juristischen Personen aus dem Geltungsbereich aus.
<i>Verbotsprinzip mit Erlaubnisvorbehalt</i>	Den Gesetzen gemeinsam ist das „Verbotsprinzip mit Erlaubnisvorbehalt“, welches besagt, dass die Bearbeitung oder Nutzung personenbezogener Daten nur dann erlaubt ist, wenn entweder eine klare Rechtsgrundlage gegeben ist oder wenn die betroffene Person ausdrücklich ihre Zustimmung zur Behandlung und Verwendung der Daten gegeben hat (vgl. [Witt10], S. 76).
<i>Vergleichbares Schutzniveau in Drittländern</i>	Sowohl die durch die Mitgliedstaaten der EU umzusetzende Richtlinie als auch das schweizerische Datenschutzgesetz verlangen, dass personenbezogene Daten nur dann in Drittländer transferiert werden dürfen, wenn diese ein angemessenes vergleichbares Schutzniveau aufweisen oder gemäss dem Schweizerischen Datenschutz, hinreichende Garantien bestehen, dass ein solches gewährleistet wird. Diese an sich selbstverständliche Forderung bedarf vor allem bei Outsourcing-Vorhaben und noch ausgeprägter bei Cloud-Computing einer sorgfältigen Abklärung und Behandlung.
<i>Datenschutz in der öffentlichen Verwaltung</i>	Der Datenschutz im Anwendungsbereich der öffentlichen Verwaltung ist meist mit gesonderten Gesetzen geregelt. In der Schweiz haben beispielsweise die kantonalen Organe entweder eigene Datenschutzvorschriften, „die einen angemessenen Schutz gewährleisten“* oder sie verwenden Teile des für „Bundesorgane“ bestimmten Datenschutzrechts.
<i>Privacy in den USA</i>	In den USA sind Gesetze [†] und Richtlinien unter dem Begriff „Privacy“, d.h. Schutz der „Privatsphäre“ in Kraft, dabei gilt es zu beachten, dass der Zugriff auf private Daten in vielen Fällen sogar gesellschaftlich akzeptiert wird, z.B. Bonitätsprüfung vor der Vereinbarung eines Arbeitsverhältnisses [‡] .
<i>Spezifische Gesetze zum Schutz der Privatsphäre</i>	Zu den Datenschutzgesetzen kommen für bestimmte Branchen noch spezifische Gesetze, die dem Schutz der „Privatsphäre von Personen“ dienen, so beispielsweise die ärztliche Schweige-

* s. Art. 37, Bundesgesetz über den Datenschutz (DSG)

† The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

‡ <http://de.wikipedia.org/wiki/Datenschutz>, Abschnitt 4.2.

	pflicht, das Bankgeheimnis, das Postgeheimnis oder das Fernmeldegeheimnis.
<i>Compliance-Risiken und Reputations-Risiken</i>	Für die Unternehmen resultieren aus Verstössen zu diesen Gesetzen vor allem „Compliance-Risiken“ (z.B. mit Strafauswirkungen) oder Reputations-Risiken (z.B. Verlust von Kundschaft). Für die Anwendung der konkreten Compliance-Anforderungen geben die aktuellen Gesetze, Verordnungen, Richtlinien und sonstigen Vorschriften Aufschluss.
<i>Datenschutz-beauftragter und Datenschutz-kommission</i>	Die Beurteilung konkreter Anwendungsfälle kann auch anhand der zahlreich vorhandenen Literatur und nicht zuletzt im Dialog mit den öffentlich bestellten Datenschutzbeauftragten (oder Datenschutzkommission in Österreich) vorgenommen werden. Gemeinsam für die oben genannten Datenschutz-Vorschriften ist die Einteilung der Daten gemäss ihrer Sensibilität und der entsprechenden Abstufung der Schutzmassnahmen.
<i>Technische und organisatorische Massnahmen</i>	Die technischen und organisatorischen Massnahmen sowie die Vorgaben für die Umsetzung des Gesetzes sind in der Schweiz beispielsweise in einer „Verordnung zum Bundesgesetz über den Datenschutz enthalten“. Das deutsche Datenschutzgesetz enthält einen (zu Paragraph 9, technische und organisatorische Massnahmen gehörenden) Anhang mit technischen und organisatorischen Massnahmen zur automatisierten Verarbeitung und Nutzung von personenbezogenen Daten. Eine praktische Umsetzungsanleitung für solche Massnahmen für einen „angemessenen“ Datenschutz ist im Anhang A.3 dieses Buches gezeigt.
<i>Unternehmens-interne Anweisungen zum Datenschutz</i>	Die im Anhang A.3 aufgezeigten technischen und organisatorischen Massnahmen sind an Mitarbeiter und beauftragte Dritte im Verantwortlichkeitsbereich des Unternehmens gerichtet. Solche als „Ausführungsbestimmungen“ benannte unternehmensinterne Anweisungen können nicht nur die Massnahmen für den gesetzlichen Datenschutz, sondern auch die Massnahmen für die zu schützenden Geheimnisse des Unternehmens selbst enthalten.
<i>Schutz der unternehmensinternen Informationen</i>	Der Schutz dieser Informationen gehört ebenfalls zum Risikomanagement des Unternehmens. Solche Geheimnisse können beispielsweise Informationen über Strategien oder hängige Patente des Unternehmens sein. Die Gesetze zum Schutz solcher unternehmenseigenen geheimhaltungsbedürftigen Informationen fallen in Deutschland und Österreich unter den Begriff „Betriebs-

und Geschäftsgeheimnis“ und in der Schweiz unter den Begriff „Fabrikations- und Geschäftsgeheimnis“*.

4.4

Risikomanagement: Anliegen der Kunden und Öffentlichkeit

*Ausbändigung
persönlicher In-
formationen und
Vermögenswerte*

Vermehrt übergeben Personen in Treu und Glauben irgendwelchen Unternehmen ihre persönlichen Informationen und Vermögenswerte zur Bearbeitung, Aufbewahrung und Übermittlung.

So werden beispielsweise Kreditkarten und Kreditkartennummern bei einer Vielzahl von tagtäglichen Vorgängen irgendwelchen Unternehmen ausgehändigt (z.B. Hotels, Restaurants, Läden). Aber auch die leibliche Sicherheit wird einigen Unternehmen anvertraut, so vertrauen die Passagiere von Verkehrsmitteln wie dem Flugzeug, der Bahn oder dem Bus ihre Gesundheit und ihr Leben der Transportfirma und ihren Mitarbeitern an. In der öffentlichen Diskussion steht auch immer wieder das Vertrauen zum Unternehmen „Spital“, dem wir oft „Leib und Leben“ für eine entsprechende Behandlung anvertrauen.

*Öffentliche Mei-
nung bezüglich
Risiko-Ereignisse*

Es ist deshalb nicht verwunderlich, dass sich die öffentliche Meinung in Form der Medien (Zeitung, Fernsehen, Radio usw.) besonders den Risiko-Ereignissen annimmt.

So konnten beispielsweise am 8. Februar 2005 in der Schweizer Presse zwei grosse Unternehmens-Risiken zur Kenntnis genommen werden:

Zürich: Ein Computer-Absturz im Hauptbahnhof Zürich sorgte gestern ab 8.45 für Chaos im Schienenverkehr. Erst gut vier Stunden später konnte die Panne behoben werden. Betroffen waren Tausende Pendler und hunderte Züge (...)

Zürich: Fast-Crash mit Jumbo wegen Missverständnis. (...) Grund für den Fast-Crash am 21. März 2003 waren Missverständnisse, wie aus einem gestern veröffentlichten Bericht des Büros für Flugunfalluntersuchungen (BFU) hervorgeht. (...) Im Frühling 2003 wurden im Raum Zürich zwei weitere Fast-Zusammenstösse registriert (...).

*Berichterstattung
durch Medien*

Die Medien halten es für ihre Aufgabe, über solche Ereignisse zu berichten. Finden sie bei ihren Recherchen Schwachstellen, d.h.

* Art. 321a Abs. 4 OR und Qualifizierung der Informationen als Geschäftsgeheimnis gemäss Art. 162 StGB (Schweizerisches Strafgesetzbuch, SR 311.0).

<i>Kontrollfunktion und Risiko-Offenlegung</i>	Zustände, die entsprechend der gängigen Praxis nicht vorkommen sollten, dann werden diese unbarmherzig verbreitet.
<i>Folge-Schäden durch Image-Verluste</i>	Die Medien, als Sprecher der öffentlichen Meinung, nehmen somit auf der einen Seite eine wichtige Kontrollfunktion über Risiken in unserer Gesellschaft wahr. Auf der anderen Seite wird das durch die Risiko-Offenlegung betroffene Unternehmen mit hoher Wahrscheinlichkeit einen Image-Verlust davontragen.
<i>Risikomanagement für nachhaltigen Erfolg</i>	Die Image-Verluste führen oft zu Kundenabfall und Umsatzschwund. Solche indirekten Folge-Schäden sind manchmal grösser als die direkten Schäden und dürfen bei den Massnahmen für die Risikominderung oder -vermeidung keinesfalls vernachlässigt werden.
	Ein vollständiges Risikomanagement, und dazu gehört auch der Umgang mit den Medien, ist also nicht nur Pflichtfach, sondern steht im ureigensten Interesse eines Unternehmens, wenn es nachhaltigen Erfolg verzeichnen will.

4.5

Hauptakteure im unternehmensweiten Risikomanagement

Das Management der Risiken gehört in einer Aktiengesellschaft nach schweizerischem Recht zu den „unübertragbaren und unentziehbaren Aufgaben“ des Verwaltungsrats ([Obli10], Art. 716a): „(...) der Verwaltungsrat allein entscheidet am Schluss und trägt die Verantwortung“ ([Böck04], S. 1533) in seiner Aufgabe der Oberleitung der Gesellschaft.

Verwaltungsrat, Audit-Komitee, Revisionsstelle und Interne Revision

Der **Verwaltungsrat*** wird das Unternehmen an der Spitze so strukturieren, dass die Risiken adäquat analysiert, berichtet und mit Massnahmen angemessen bewältigt werden können. Zu diesem Zweck wird er sich zusätzlich zur Revisionsstelle ein „Audit-Komitee“ und eine „Interne Revision“ einrichten.

Geschäftsleitung

Der Verwaltungsrat hat die Aufgabe, für die Geschäftsabwicklung eine **Geschäftsleitung** zu bestellen, doch wird er sich die wichtigsten Entscheide wie Strategiebeschlüsse, Formulierung wichtiger Unternehmensziele und die Allokation aufwändiger Ressourcen vorbehalten. Solche Entscheide basieren unter anderem auch auf den Vorstellungen des Verwaltungsrats über Integrität und ethische Werte (vgl. [Cose04], S. 83).

* Hier ist das Gremium für die „Oberleitung“ des Unternehmens gemeint, das in der Schweiz durch den „Verwaltungsrat“, in Deutschland durch den „Aufsichtsrat“ in den USA durch das „Board of Directors“ wahrgenommen wird.

Bezüglich der Risiken wird sich der Verwaltungsrat die Übersicht verschaffen über (vgl. [Cose04], S. 83):

- ☐ den Umfang des durch das Management effektiv eingerichteten Risikomanagements,
- ☐ das Bewusstsein über die Risiko-Bereitschaft (Risiko-Appetit),
- ☐ die Überprüfung des Geschäfts-Portfolios im Hinblick auf die Risiken und Risiko-Bereitschaft im Unternehmen,
- ☐ die grössten Risiken und ob das Management diese in angemessener Weise bewältigt.

*Ultimative
Ownership-
Verantwortung
des CEO*

Der „**Chief Executive Officer**“ (**CEO**) hat die ultimative Ownership-Verantwortung über das Risikomanagement im Unternehmen. Er trägt die Verantwortung dafür, dass alle Komponenten eines Unternehmens-Risikomanagements eingerichtet sind (vgl. [Cose04], S. 83 ff.). Dabei formuliert er die Werte, Grundsätze und wichtigsten Betriebs-Policies, welche das Fundament für das Unternehmens-Risikomanagement darstellen. Auch wird der CEO eine für sein Unternehmen geeignete Risikomanagement-Organisation zusammenstellen.

Dazu gehören beispielsweise folgende Funktionen:

- ☐ Chief Risk Officer (CRO)
- ☐ Chief Compliance Officer (CCO)
- ☐ Risk Owner
- ☐ Risk Manager
- ☐ Chief Financial Officer (CFO)
- ☐ Chief Operation Officer (COO)
- ☐ Linien-Manager

In Unternehmen mit entsprechend hohen IT-Abhängigkeiten kommen folgende Funktionen dazu:

- ☐ Chief Information Officer (CIO)
- ☐ Chief Information Security Officer (CISO)
- ☐ IT-System Owner

(Anm.: Die IT-Funktionen werden im Teil C des Buches näher betrachtet.)

An dieser Stelle betrachten wir die Funktionen eines Chief Risk Officer und eines Risk Owner noch genauer:

<i>Chief Risk Officer</i>	Der „ Chief Risk Officer “ (CRO) hat die zentrale Funktion, den Unternehmens-Risikomanagement-Prozess in Gang zu halten und zu koordinieren. Seine Aufgaben erstrecken sich von der Gestaltung und Einführung bis hin zur Aufrechterhaltung und Anpassung des Risikomanagement-Prozesses. Dazu verfügt er über die notwendigen Ressourcen und Kompetenzen.
<i>Chief Risk Officer bei Banken</i>	Bei den Banken stehen dem Chief Risk Officer und seiner Organisationseinheit oft umfassende Analyse- und Bewertungssysteme für Markt-Risiken zur Verfügung. (Aufgrund der oben gezeigten Anforderungen gibt es solche Informations-Systeme inzwischen auch für Kredit-Risiken und Operationelle Risiken.) In den Banken kommt besonders aus regulatorischen Gründen dieser Funktion ein hoher Stellenwert zu, da beispielsweise die Unterlegung mit Eigenkapital in Abhängigkeit von der Risiko-Situation dem Ziel einer hohen Eigenkapital-Rendite entgegenwirkt.
<i>Gewaltentrennung zu Geschäfts- und Supporteinheiten</i>	Besonders in grossen Unternehmen sind die „Checks and Balances“, wie sie durch das Sarbanes-Oxley Gesetz gefordert werden, sehr wichtig. Ein unabhängiger, ausserhalb der Linie direkt dem CEO unterstellter Risk Officer ist in der Lage, ähnlich wie die Interne Revision, seine Aufgaben in Gewaltentrennung zu den Managern der Geschäfts- und Support-Einheiten ausführen.
<i>Steuerung des Risiko-Assessments und der Risiko-Kontrolle</i>	Das Schwergewicht der Aufgaben dieser Stelle liegt in der Steuerung des Risiko-Assessments und der Risiko-Kontrolle. Die Aufgaben der Risiko-Behandlung hingegen sollten durch die Linie respektive die operativen Fachabteilungen ausgeführt werden. Ansonsten würde das Prinzip der Gewaltentrennung wiederum verletzt werden.
<i>Risk Owner</i>	Der „ Risk Owner “ ist eine Führungsperson und ein Entscheidungsträger in der Linie, welcher in dem ihm anvertrauten Bereich unternehmerische Verantwortung trägt. Mit seinen Entscheiden trägt er Verantwortung sowohl über die Risiken als auch über die in seinem Aufgabengebiet wahrzunehmenden Chancen. Der oberste Risk Owner ist der CEO. Risk Owner sind vor allem die Führungs-Personen von Geschäfts- und Unterstützungsprozessen oder IT-Systemen. Die Ernennungen der Owner sollten durch die Geschäftsleitungen erfolgen.
<i>Risk Manager</i>	Die Funktion eines „ Risk Manager “ wird oft in kleineren Unternehmen anstelle eines Chief Risk Officer eingesetzt. Eine wesentliche Aufgabe dieser Funktion ist es, den unternehmensweiten Risikomanagement-Prozess zu unterhalten. Oft wird diese Funktion mit der Unterhaltung des Strategie-Prozesses kombiniert. Es versteht sich von selbst, dass der Risiko-Manager die notwendi-

gen Fähigkeiten und Instrumente besitzen muss, um mit Hilfe der Risk Owner die unternehmensweiten Risiken zu erheben und sie anschliessend zu konsolidieren (vgl. [Brüh03], S. 185).

4.6

Zusammenfassung

An die Unternehmen und deren oberste Leitungs-Organen werden unter dem Begriff „Corporate Governance“ verschiedene Anforderungen bezüglich Rechten und Verantwortlichkeiten gestellt.

Kurz gefasst, muss die Unternehmensführung im Interesse des Unternehmens, der Anspruchsgruppen und vor allem der Anteilseigner handeln. Zu einem solchen Interesse gehört der sorgfältige Umgang mit den möglichen Unternehmens-Risiken.

Aufgrund von Missbräuchen und falschem Risiko-Verhalten der letzten Jahre haben Gesetzgeber und Regulatoren Vorschriften erlassen. Vorschriften dieser Art sind: Gesetz KonTraG in Deutschland, Obligationenrecht und „Swiss Code of best Practices for Corporate Governance“ in der Schweiz, Basel Capital Accord (Basel II), Sarbanes-Oxley Act (SOX) in den USA und EuroSOX in Europa.

Das KonTraG-Gesetz verlangt u.a. vom Vorstand einer Aktiengesellschaft, „geeignete Massnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“

Die Eigenkapitalvereinbarung von Basel II verpflichtet die Banken, die Kreditrisiken in Abhängigkeit vom Risiko des Kreditnehmers mit Eigenkapital zu unterlegen. Dies hat unter anderem zur Folge, dass kreditnehmende Unternehmen mit hohen Risiken (einschliesslich der operationellen Risiken) höhere Aufschläge auf Kreditzinsen zu erwarten haben. Zur Bemessung der Eigenkapital-Unterlegung für operationelle Risiken kommt entsprechend der Bank-Struktur einer der drei Ansätze zum Einsatz:

- Basisindikatoransatz
- Standardansatz (ggf. auch alternativer Standardansatz)
- Fortgeschrittene (ambitionierte) Messansätze

Für die fortgeschrittenen Ansätze, die eine risikogetreue Kapital-Unterlegung gestatten, müssen von der Aufsichtsbehörde genehmigte Risiko-Assessment-Verfahren eingesetzt werden. In einem Arbeitspapier des Baseler Ausschusses wurden für operationelle Risiken die folgenden Verfahren vorgeschlagen:

- Interner Bemessungs-Ansatz (IMA=Internal Measurement Approach)
- Verlustverteilungs-Ansatz (LDA=Loss Distribution-Approach)
- Scorecard-Ansatz (SCA=Scorecard-Approach)

Das US-amerikanische Sarbanes-Oxley Gesetz verlangt von den betroffenen Unternehmen, dass bestimmte Mindest-Standards der Informationssicherheit und der internen Kontrolle, im Zusammenhang mit der Aufbereitung der Zahlen für das „Financial Reporting“, zu erfüllen sind.

Euro-SOX ist eine EU-Richtlinie, mit der die Anforderungen an die Abschlussprüfung mit entsprechenden Regelungen hinsichtlich Qualität der Audits, der Abschlussprüfer und der Prüfungsgesellschaften harmonisiert werden. Damit sollen die finanziellen und betrieblichen Risiken sowie das Risiko von Vorschriftenverstößen auf ein Mindestmass begrenzt und die Qualität der Rechnungslegung verbessert werden. Für die IT eines Unternehmens, für das Euro-SOX Gültigkeit hat, sind, analog zu SOX, regelkonforme IT-Systeme bereitzustellen, um die geforderte „Compliance“ mit Hilfe von IT-Systemen durchzusetzen und nachzuweisen.

Auch der Datenschutz als gesetzliche Anforderung an die Unternehmen erhält eine immer höhere Wichtigkeit, dabei stellt die zunehmende Vielfalt von Beteiligten in den Dienstleistungsketten heutiger Informationsverarbeitungen sowie die Vielfalt neuer Technologien grosse Herausforderungen dar.

Die Schweiz und Lichtenstein definieren den Datenschutz (DSG) als „Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.“, wobei hier die Anwendung ausdrücklich sowohl auf natürliche als auch auf juristische Personen gilt. Die Datenschutz-Richtlinie der EU sowie die Datenschutzgesetze von Deutschland und Österreich klammern die Daten von juristischen Personen aus dem Geltungsbereich aus.

In den USA sind Gesetze und Richtlinien unter dem Begriff „Privacy“ in Kraft, dabei gilt es zu beachten, dass der Zugriff auf private Daten in vielen Fällen sogar gesellschaftlich akzeptiert wird. Zu den Datenschutzgesetzen kommen für bestimmte Branchen noch spezifische Gesetze, die dem Schutz der „Privatsphäre von Personen“ dienen (z.B. die ärztliche Schweigepflicht, das Bankgeheimnis, das Postgeheimnis oder das Fernmeldegeheimnis.)

Die technischen und organisatorischen Massnahmen, sowie die Vorgaben für die Umsetzung des Gesetzes sind in der Schweiz beispielsweise in einer „Verordnung zum Bundesgesetz über den Datenschutz enthalten“.

Auch andere gesetzliche Vorschriften nehmen sich dem Thema Risikomanagement in der einen oder anderen Form an. Die Risiken von Unternehmen und ihren Produkten werden vermehrt auch durch die Kunden und die öffentliche Meinung überwacht.

Für das Management der Risiken im Unternehmen sind vorweg einige Hauptakteure verantwortlich, so der Verwaltungsrat (Aufsichtsrat), der Chief Executive Officer und je nach Unternehmensgrösse und -ausprägung spezielle Risiko-Verantwortliche wie Chief Risk Officer, Chief Compliance Officer, Risk Owner und Risk Manager.

4.7

Kontrollfragen und Aufgaben

1. Das St. Galler Management-Modell nennt drei Kategorien von Unternehmensprozessen. Nennen Sie diese mit ihren hauptsächlichen Aufgaben.
2. Was verstehen Sie unter Corporate Governance?
3. Was hat Corporate Governance mit Risikomanagement zu tun?
4. Welche Rolle spielt das IT-Risikomanagement in den Anforderungen an die Corporate Governance?
5. Welche Rollen kommen dem Verwaltungsrat (Aufsichtsrat) und dem CEO eines Unternehmens bezüglich des Risikomanagements zu?
6. Warum ist das IT-Risikomanagement im Zusammenhang mit dem Sarbanes-Oxley Gesetz wichtig?
7. Unter welche Gesetze fällt der Schutz der unternehmens-eigenen geheimen Daten?
 - a. In der Schweiz und in Lichtenstein
 - b. In Deutschland und Österreich
8. Was ist der hauptsächliche Zweck von Euro-SOX?
9. Welchen Zweck verfolgt Basel II und Basel III?
10. Für welche Unternehmen kommt ein fortgeschrittener Messansatz nach Basel II in Frage?
11. Sind auch andere Unternehmen als Banken von Basel II betroffen? Wenn ja, warum?

Chancen und Risiken im richtigen Verhältnis wahrnehmen

Integrierter Risikomanagement-Prozess

Die Risiken, die wir in diesem Buch behandeln, wirken in der einen oder anderen Weise dem Erreichen von Unternehmens-Zielen und dem Erhalten von Unternehmens-Werten entgegen. Dies gilt auch für die Informationssicherheits- und IT-Risiken. Ein effektives Risikomanagement muss deshalb im Management-System des Unternehmens verankert sein, gilt es doch, die Chancen und die Risiken in einem ausgewogenen und für die Lebensfähigkeit des Unternehmens richtigen Verhältnis wahrzunehmen. Den Prozess eines solchen ganzheitlichen Risikomanagements bezeichnen wir als „Integrierten Risikomanagement-Prozess“.

In Anlehnung an zurzeit gebräuchliche Management-Konzepte, wie das Qualitäts-Management-System nach ISO 9001:2008, das St. Galler-Management-Konzept [Bleic92] und das „Balanced Scorecard“-Konzept [Kapl01], werden im Folgenden die Führungsaspekte und Anforderungen an ein integriertes Risikomanagement diskutiert. Diese Aspekte und Anforderungen müssen sodann auch beim Einsatz von in Abschnitt 5.5 behandelten Frameworks und Standards für Management-Systeme berücksichtigt werden. In einem integrierten Risikomanagement-Prozess wird das Risikomanagement in die Managementprozesse für das „normative“, das „strategische“ und das „operative“ Management eingegliedert (Abbildung 5.1).

Normatives Management	Langzeit-Perspektive (5 bis 20 Jahre)
Strategisches Management	Mittelfrist-Perspektive (1 bis 5 Jahren)
Operatives Management (Gewinn Management)	Kurzfrist-Perspektive (Jahresplan)

Abbildung 5.1: Grundsätzliche Ebenen der Unternehmensführung

Diese im St. Galler Management-Konzept ([Bleic92], [Rüeg02]) ausführlich behandelten Ebenen sind nicht als Ebenen einer hierarchischen Führungsstruktur, sondern als „systemische“ Ebenen zu verstehen. Dabei ist zu bemerken, dass die wesentlichen Anforderungen aus einem solchen Management-Konzept für verschiedene Unternehmensgrössen skalieren, das heisst sowohl für kleine und mittlere als auch für grosse Unternehmen tauglich sein sollten. Selbstverständlich sind die für ein kleineres Unternehmen relevanten Prozesse mit wesentlich geringerem bürokratischem Aufwand durchzuführen.

5.1

Integrierter unternehmensweiter Risikomanagement-Prozess

Das unternehmensweite Risikomanagement lässt sich als Prozess, wie in Kapitel 3 ausführlich behandelt, durchführen und in die Management-Prozesse des Unternehmens integrieren. Auch kann der Risikomanagement-Prozess als durchzuführender Teil eines übergeordneten Risikomanagement-Systems* verstanden werden. Wobei das übergeordnete Management-System† dem Aufbau und Erhalt des Risikomanagements und deren kontinuierlichen Verbesserung unter Einbezug der wichtigsten Unternehmensanforderungen und Management-Systeme im Unternehmen dient.

Zweck unternehmensweiter RM-Prozess

Bevor wir diesen Prozess in seinen Einzelheiten festlegen und beschreiben, legen wir seinen Zweck fest:

Der unternehmensweite Risikomanagement-Prozess muss sicherstellen, dass alle wesentlichen Risiken des Unternehmens systematisch identifiziert, analysiert, bewertet, behandelt und laufend überwacht werden.

Subprozesse

Dazu kann der unternehmensweite Risikomanagement-Prozess auf dezentralen Sub-Prozessen der operativen Organisationseinheiten (Geschäftsbereiche, Abteilungen, etc.) aufbauen. Umgekehrt müssen sich die dezentralen Sub-Prozesse in die Struktur und die Vorgaben des unternehmensweiten Risikomanagement-Prozesses einfügen. Die Vorgaben über die Abstimmung der

* Im Standard ISO 31000 als Framework bezeichnet

† Siehe Abschnitt 5.6 und „High level structure and identical text for management standards“ gemäss dem ISO Guide 83.

Subprozesse untereinander sowie mit dem übergeordneten Unternehmens-Risikomanagement-Prozess sind im übergeordneten Risikomanagement-System entsprechend geregelt.

In einem integrierten Risikomanagement ist der unternehmensweite Risikomanagement-Prozess Teil des Unternehmens-Management-Systems und damit auch Teil des Unternehmens-Strategieprozesses. Wie im Teil D des Buches gezeigt wird, empfiehlt es sich, die IT-Risiken auf zwei Ebenen zu behandeln: auf der strategischen Ebene, wo die generellen Ziele für die IT und die Sicherheit der Informationen zu definieren sind und auf der operativen Ebene, wo die Risiken im notwendigen Detail der einzelnen Prozesse, Systeme und Objekte analysiert und bewältigt werden. Die „Restrisiken“ der operativen Ebene werden wiederum auf der strategischen Ebene konsolidiert, wo sie allenfalls strategische Bedeutung haben.

*Fallweise oder
kontinuierlich
laufend*

Zu unterscheiden ist ein fallweise durchzuführender Risikomanagement-Prozess von einem kontinuierlich laufenden (rollenden) Risikomanagement-Prozess.

Für den kontinuierlich laufenden (rollenden) Risikomanagement-Prozesse wird im Teil D dieses Buches sowohl die Initialisierung (resp. der Aufbau des Prozesses) als auch seine fortlaufende Weiterführung und seine Anpassung an die Risikosituation des Unternehmens behandelt.

*Prozess im Ma-
nagement-System*

Es liegt nahe, das Risikomanagement im Unternehmens-Management-System ähnlich dem Qualitätssystem (ISO 9001:2000) zu organisieren. Das Risikomanagement steht mitunter im Spannungsfeld zwischen den Kundenforderungen, der Kundenzufriedenheit, dem Wettbewerb in den Märkten sowie der Anforderungen und Leistungen der Anspruchsgruppen (Stakeholders). Eine dafür prozessorientierte Organisation des Unternehmens ist in Abbildung 5.2 dargestellt (vgl. [Brüh01], S. 159).

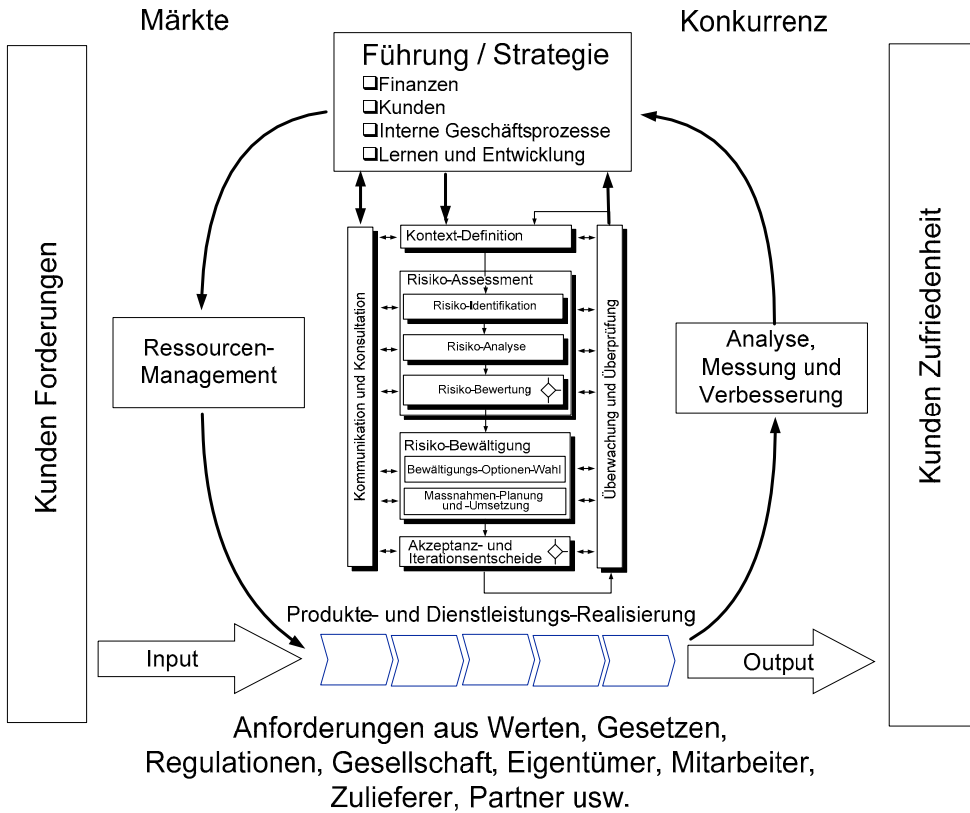


Abbildung 5.2: Risikomanagement-Prozess im strategiefokussierten Führungssystem

*Ausgewogene,
ganzheitliche
Behandlung der
Unternehmens-
Sichten*

Wie wir in den späteren Ausführungen sehen, bedarf es neben der im Qualitätssystem betonten Kundensicht die ausgewogene ganzheitliche Behandlung der Sichten „Lernen und Entwickeln“, „Interne Prozesse“, „Kunden“ und „Finanzen“. Die Ausgewogenheit dieser Sichten kann mit einem entsprechenden Strategie-Operationalisierungs-Konzept unter der Bezeichnung „Balanced Scorecards“ erreicht werden.

5.2

Normatives Management

*Generelle
Merkmale*

Das „normative Management“ beinhaltet die generellen Merkmale eines Unternehmens in der Form von Normen, Werten, Vorstellungen und Verhaltensweisen.

*Unternehmens-
Vision*

Ausgangspunkt für die Entwicklungsfähigkeit sowie als Bezugsrahmen für die vorausschauende Vorstellung eines Zukunftsbil-

des des Unternehmens ist eine **Unternehmens-Vision**. Die Unternehmens-Vision ist im Normativen-, Strategischen- wie auch Operativen-Management zu konkretisieren (vgl. [Bleic92], S. 84).

Beispiel einer Unternehmens-Vision

Beispiel der Unternehmens-Vision einer Fluggesellschaft:

Unsere Kunden sollen die beste Welt-Klasse-Airline erleben, wie wir auch die beste Qualität für jeden bieten, der mit unserem Unternehmen in Verbindung steht: Passagiere, Airlines, Konzessionäre, Lieferanten und die eigenen Angestellten.

Auf der Ebene des normativen Managements werden neben der Unternehmens-Vision die folgenden Ausprägungen unterschieden (vgl. [Bleic92], S. 68-87):

- Unternehmens-Politik
- Unternehmens-Verfassung und
- Unternehmens-Kultur

5.2.1

Unternehmens-Politik

Abstimmung der inneren und äusseren Interessen

Die Unternehmens-Politik enthält die Festlegungen für die Abstimmung der äusseren für das Unternehmen relevanten Interessen mit den inneren Interessen im Hinblick auf ein langfristiges, autonomes Überleben.

Unternehmens-grundsätze

Sie enthält die Unternehmensgrundsätze über das Verhalten bezüglich Werten, Normen und Idealen.

5.2.2

Unternehmens-Verfassung

Grundsätzliche Einstellung zu Risiken

Da es im normativen Management unter anderem um die gesetzlichen Randbedingungen und vor allem um die Voraussetzungen für ein langfristiges Überleben des Unternehmens geht, muss die grundsätzliche Einstellung des Unternehmens zu Risiken bereits in der „Unternehmens-Verfassung“ zum Ausdruck gebracht werden.

Auflagen von aussen sowie eigene Statuten und Reglemente

Die Unternehmens-Verfassung enthält die von aussen durch Gesetze und Regulative gegebenen Auflagen und die vom Unternehmen selbst geschaffenen Statuten und Reglemente. Darin festgelegt wird unter anderem die „Corporate Governance“, wie sie für das Unternehmen erforderlich ist. Im Vordergrund stehen dabei die Verantwortlichkeiten und Kompetenzen

der Geschäftsleitung sowie die wesentlichen organisatorischen Gestaltungen wie Geschäftsordnung, Rechtsform, Rechnungslegungsstandard. Daneben werden auch grundsätzliche Organisations-Konzepte wie das Management-System und das Risiko- und Qualitätsmanagement verankert.

5.2.3

Unternehmens-Kultur

Rahmen für Perzeptionen und Präferenzen

Die Unternehmens-Kultur soll die verhaltensbezogenen Werte und Normen aus der Vergangenheit in die Zukunft „transportieren“, indem sie den Rahmen für die Perzeptionen und Präferenzen der Mitglieder eines Unternehmens bei der Definition der Ziele und deren Umsetzung bildet.

5.2.4

Mission und Strategische Ziele

Mission

Die Unternehmens-Politik liefert an der Schnittstelle zum strategischen Management die sogenannte „Mission“ als wichtige Vorgabe für die im Strategie-Prozess zu definierenden strategischen Ziele.

Unternehmens-zweck

Die Mission gibt Auskunft über den Unternehmenszweck und kann mit der der Beantwortung der Frage definiert werden:

Weshalb existiert unser Unternehmen?

Die Antwort auf diese Frage sollte zumindest die **Definition der Geschäfte** des Unternehmens mit den folgenden drei Dimensionen beinhalten:

- **Produkte (resp. Dienstleistungen)**
- **Besonderheit** (in Funktionen, Aktivitäten, Qualitäten, Ressourcen) und
- **Märkte**, in denen die Geschäfte abgewickelt werden.

Eine solche Mission kann kurz in einem „Mission-Statement“ definiert werden, z.B.:

Beispiel eines Mission Statements

Wir entwerfen, entwickeln, produzieren und vertreiben qualitativ hochstehende Personal-Computer, Tablet-Computer und Smartphones weltweit für anspruchsvolle Nutzer im Business-Einsatz von Office- und Multimedia-Anwendungen.

Die Mission ist in der Regel über eine längere Zeitspanne (5 bis 10 Jahre) des Unternehmens mit entsprechend generellen Aussa-

gen angelegt. Werden die Geschäfte durch verschiedene „strategische Geschäftseinheiten“ eines Unternehmens durchgeführt, dann sollten diese ebenfalls aus der Mission hervorgehen.

*Anpassung bei
Veränderungen*

Die Mission muss insbesondere den äusseren Unternehmensverhältnissen entsprechen, d.h. bei entsprechenden Veränderungen angepasst werden.

5.2.5

Vision als Input des Strategischen Managements

*Konkretisierte
Vision für Strategiefindung*

Unter Abschnitt 5.2 wurde gefordert, dass die Unternehmens-Vision auf allen Managementebenen zu konkretisieren ist. Gerade in neueren Management-Konzepten, die dem raschen Wandel in den Unternehmens-Anforderungen Rechnung tragen sollen, wird der Strategiefindung eine sehr konkrete und teilweise sogar mit Messgrössen versehene Vision vorgeschaltet.

Die Konkretisierung der Vision kann beispielsweise so erfolgen, indem der Fokus auf messbare Operationen und auf eine grundlegende Änderung der Wettbewerbs-Situation gelegt wird.

Beispiel

Dazu das Beispiel der Federal Express: „Wir werden die Pakete bis 10:30 des nächsten Morgens liefern.“ ([Hamm93], S. 156).

Eine Konzern-Strategie mit einer Konzern-Vision wird sich aus mehreren Bereichs- oder Geschäftsfeld-Strategien zusammensetzen, die ihre eigenen konkreten Visionen aufweisen.

5.3

Strategisches Management

Das „Strategische Management“ sowie das „Operative Management“ interagieren mit der Umwelt des Unternehmens und sind in das unter Abschnitt 5.2 beschriebene Normative Management „eingebettet“.

*Horváth & Partner -
Schalenmodell*

Diese für das „Strategische Management“ wichtigen Zusammenhänge wurden im „Horváth & Partner - Schalenmodell“ veranschaulicht ([Horw04], S. 126).

*Normatives Management in der
äusseren Schale*

Das Normative Management mit Werten, die Mission, die Vision usw. befindet sich in diesem Schalenmodell als strategischer Rahmen in der äusseren Schale um das „klassische“ Strategische Management herum (Abbildung 5.3).

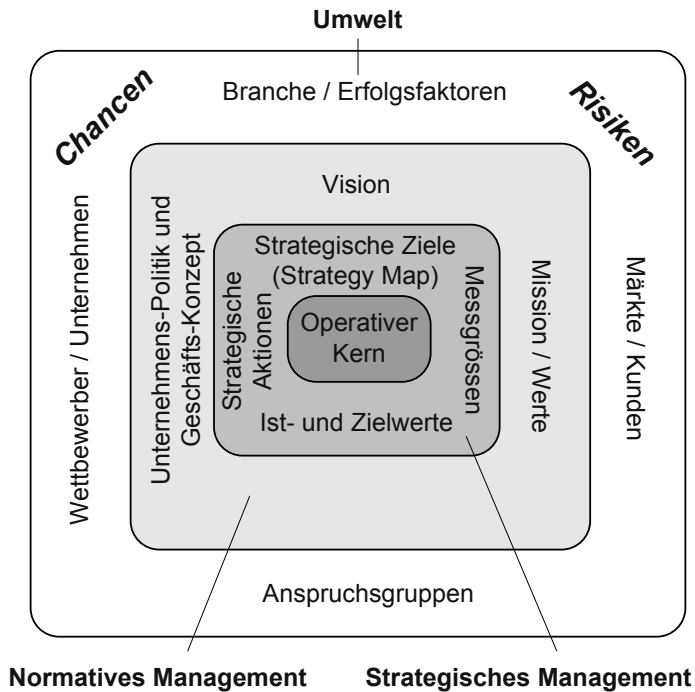


Abbildung 5.3: Einbettung des Strategischen Managements in das Schalenmodell (vgl. ([Horw04], S. 126))

Strategisches Management

Im „Strategischen Management“ behandeln wir die Elemente:

- Strategische Ziele,
- Strategien und (abgeleitete) Geschäftsziele,
- Strategische Aktionen, Politiken und Strategie-Grundsätze

Strategische Ziele

Im Rahmen des Strategischen Managements werden vor allem die „Strategischen Ziele“ gesetzt und die entsprechenden strategischen Entscheide gefällt. Die solchermaßen zu fällenden Strategie-Entscheide basieren auf der Mission und sind weitere Konkretisierungen der Vision.

Umsetzung mit strategischen Aktionen

Die Umsetzung der Strategischen Ziele und abgeleiteten Geschäftsziele erfolgt mittels „Strategischen Aktionen“. Die Richtlinien zur Umsetzung dieser Entscheide werden mittels Strategischen Plänen und Politiken (Policies) erlassen. Das „Balanced Scorecard“-Konzept definiert das Ergebnis aus dem Strategie-Prozess als Vorgabe zur operationellen Umsetzung in Form einer „Strategy Map“ (s. Abschnitt 5.4.1).

5.3.1

Strategische Ziele*Ziele*

Ziele sind aus verschiedenen Gründen für das strategische Management wichtig:

- Ziele drücken aus, was das Unternehmen durch sein Dasein und seinen Leistungsprozess erreichen soll.
- Ziele helfen, das Unternehmen in seiner Umgebung zu definieren und die strategischen Entscheidungen zu koordinieren.
- Ziele stellen Standards dar, gegen welche die Unternehmensleistung gemessen werden kann (vgl. [Jauc88], S. 65).

Nachfolgend sind einige Beispiele von „Strategischen Zielen“ aufgeführt:

Beispiele

- Rendite steigern
- Wachstum steigern
- Shareholder-Value erhöhen
- Marktposition ausbauen
- Kundenzufriedenheit erhöhen
- Kapazitätenerhöhung erreichen
- Fixkosten senken
- Flexibilität und Anpassungsfähigkeit erhöhen
- Sicherheit der Produkte und Dienstleistungen verbessern
- Strategische Partnerschaften aufbauen
- Qualität der Produkte und Dienstleistungen verbessern
- Mitarbeiterzufriedenheit verbessern
- Leistungsanreize schaffen
- Soziale Verantwortung erhöhen
- Umweltverantwortung erhöhen

Die Strategischen Ziele sollen formalisiert und spezifisch, herausfordernd aber erreichbar sein. Wenn immer möglich, sollten die Strategischen Ziele mit entsprechenden Messgrößen versehen werden.

Messgrösse / Risiko-Toleranz

Die Messgrößen sollen sowohl den Zielwert als auch die Zeitperiode für die Zielerreichung angeben. Den Zielwerten können auch „Risiko-Toleranzen“ zugeordnet werden (s. Abbildung 5.4).

Ein Strategisches Ziel könnte beispielsweise mit folgenden Messgrößen definiert werden:

Beispiel

Strategisches Ziel	Messgrösse	Zielwert / Periode	Risiko-Toleranz
Rendite steigern	ROE	15 % / in 2 Jahren	+/- 5 %

Ein Strategisches Ziel repräsentiert meist eine für das Unternehmen anzustrebende positive Veränderung. Das Erreichen des Ziels kann somit als wahrgenommene Chance ausgelegt werden. Hingegen können die negativen Folgen von Abweichungen solcher Ziele als „Risiken“ definiert werden.

Risiko-Indikatoren

Häufig werden den Zielen auch „Risiko-Indikatoren“ zugeordnet. Die Risiko-Indikatoren geben Aufschluss darüber, inwieweit der ursprünglich erwartete positive Effekt des Ziels nicht eintritt.

Oft rufen die zu erreichenden strategischen Ziele an anderen Stellen hohe Risiken hervor. So kann beispielsweise eine Kostenreduktion mittels „Strategischem Sourcing“, Risiken bezüglich Wahrung der Vertraulichkeit (Geschäftsgeheimnis, Bankgeheimnis usw.) zur Folge haben. Oder eine kurzfristige Gewinnmaximierung durch Abbau von Forschungsaufwendungen kann im langfristigen Rahmen zu existenzgefährdenden Risiken führen. Aus dem Betrachtungswinkel des Risikomanagements ist es deshalb wichtig, entsprechend langfristige strategische Ziele zur Gewährleistung einer nachhaltigen Profitabilität sowie solche Risiko-Ziele einzuführen, deren Einhaltung den Risiken entgegenwirken.

Risiko-Ziele

Prioritäten

Die Ziele können auch mit Prioritäten versehen werden. Ein solches Vorgehen hilft beispielsweise, wenn auf Grund äusserer Zwänge (z.B. hohe Zinsen oder Kreditklemme) einzelne Ziele gegenseitig in Widerspruch geraten. In einer solchen Situation könnte beispielsweise ein Profitabilitäts-Ziel über das Ziel „Erweiterung des Marktanteils“ Vorrang erhalten. Auch könnte ein Risiko-Ziel (z.B. Liquidität) Vorrang über ein Expansions-Ziel erhalten. Für eine Fluggesellschaft wäre es beispielsweise ratsam, dem Risiko-Ziel „Sicherheit der Passagiere“ eine höhere Priorität als dem Ziel „Komfort der Passagiere“ zu geben. Würden sich bei einer Fluggesellschaft „Sicherheitsprobleme“ für Passagiere häufen, dann würde dies mit hoher Wahrscheinlichkeit zu Umsatzeinbussen bis hin zur Zahlungsunfähigkeit der Fluggesellschaft

führen. Für das Unternehmens-Management ergeben sich somit folgende Beweggründe für Zielsetzungen:

*Beweggründe für
Zielsetzungen*

Zielsetzungen...

- erlauben die strategischen Aktionen aus verschiedenen Perspektiven eines Unternehmens für einen grösstmöglichen Gesamtnutzen aufeinander abzustimmen;
- erleichtern die Entscheidungsfindung;
- helfen, die Unternehmensleistung und den Erfolg zu bewerten;
- helfen, Chancen und Risiken gegeneinander abzuwägen;
- helfen, für überlebenswichtige Anforderungen (z.B. Just-in-time-Produktion) die geeigneten Organisations-Formen zu finden;
- kommunizieren den Führungskräften und Mitarbeitern, was für das Unternehmen wichtig ist und in erster Linie erreicht werden soll;
- helfen, kontraproduktive Aktivitäten und Ressourcen-Verschleiss zu verhindern;
- erlauben, die Aufgaben sachgerecht an Management und Mitarbeiter zu delegieren und diese an der sogenannten „langen Leine“ zu führen;
- machen den Führungskräften und Mitarbeitern die der Firma eigenen Verhaltensmuster und Standards bewusst;
- helfen, die Erwartungen der Kunden sowie der anderen Anspruchsgruppen (Stakeholders) zu erfüllen;
- helfen, veränderten äusseren Bedingungen (z.B. Steuer-gesetzgebung) in möglichst optimaler Weise gerecht zu werden;
- helfen, Leistung und Wirksamkeit von Unternehmens-Prozessen zu definieren und zu beurteilen.

Die angegebenen Beweggründe für Zielsetzungen sind an die interne Belegschaft adressiert. Selbstverständlich ist es für die Reputation einer Firma auch wichtig, Ziele nach aussen zu kommunizieren. Solche nach aussen kommunizierten Ziele sind jedoch meist grobe Zusammenfassungen der internen Ziele und heben die im äusseren Erscheinungsbild der Firma wichtigen Aspekte hervor.

Bildung von risikobehafteten Zielen

Die Bildung von risikobehafteten Zielen und Strategien im Strategieprozess sowie die Behandlung der Risiko-Akzeptanz ist an einem Beispiel in Abbildung 5.4 gezeigt.

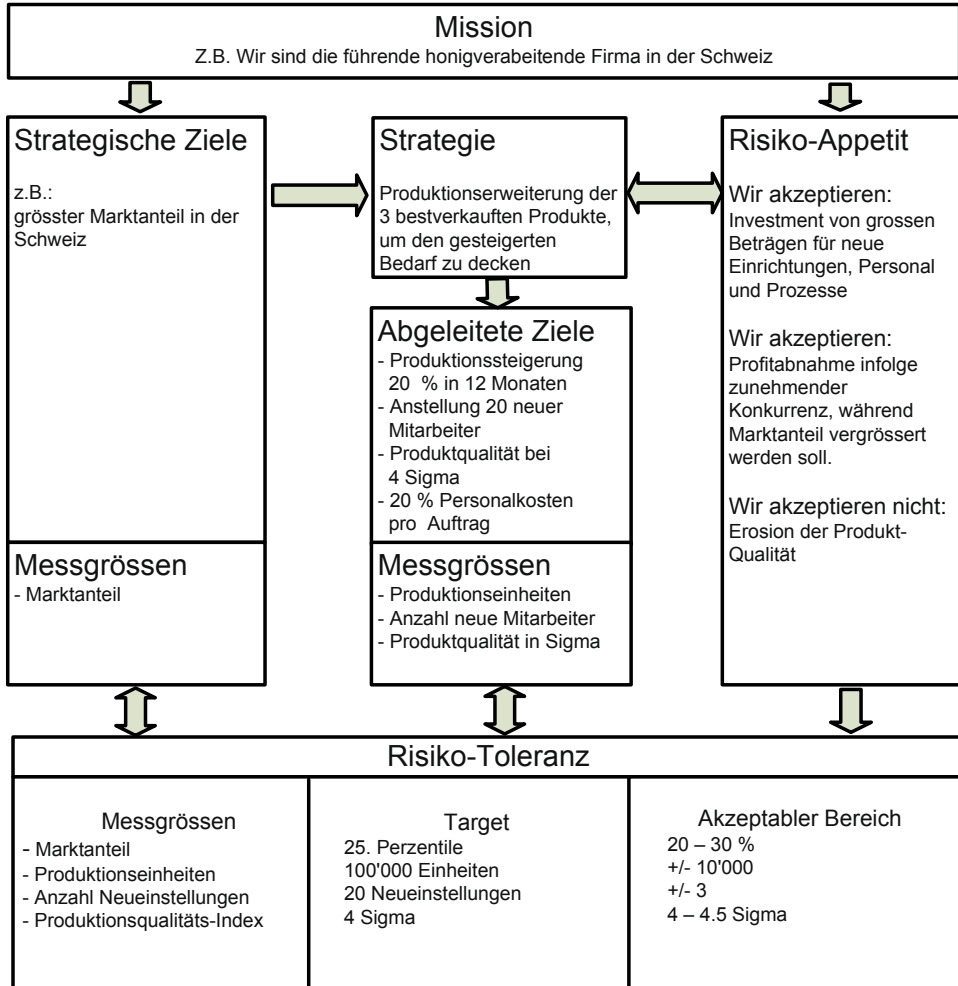


Abbildung 5.4 Beispiel der Zielbildung im Strategie-Prozess (vgl. [Cose04], S. 20)

Zur Bildung der strategischen Ziele liegen die Vorgaben des normativen Managements, der Mission der Vision sowie die Ergebnisse einer SWOT-Analyse zugrunde. Für die Ziele auf der

Ebene der Geschäftsfeld-Strategien ist zudem das entsprechende Geschäftskonzept massgeblich.

SWOT-Analyse

Mit der SWOT*-Analyse werden die Chancen und Gefahren der Umwelt sowie die Stärken und Schwächen des Unternehmens resp. des Geschäftsfeldes analysiert.

5.3.2

Strategien

Strategien sind die Mittel zur Erreichung der Ziele

Die Strategien sind Aktionen, Handlungen und Massnahmen, mit anderen Worten die Mittel, um die im vorherigen Abschnitt angeführten Ziele in einer gegebenen Situation erreichen zu können.

Die Ziele und ihre Definition sind zwar Bestandteil des Strategieprozesses, sind jedoch nicht die Strategien selbst. Diese „klassische“ Unterscheidung ist für die Gestaltung des Strategieprozesses, in welchen wir das Risikomanagement einbeziehen wollen, wichtig, zumal verschiedene Strategien mit unterschiedlichen Risiken möglich sind, um dieselben Ziele erreichen zu können[†]. Im Strategie-Prozess werden diejenigen Strategien ausgelotet und beschlossen, welche für alle Nebenbedingungen die besten Lösungen darstellen. Z.B. könnte das Ziel „hohe Flexibilität bei der Produktgestaltung“ durch die Strategie „Einführung einer neuen Organisationsform“ und/oder eines „neuen IT-Systems“ erreicht werden. Für die „Operationalisierung“ der Strategien werden diese in „strategische Aktionen“ umgesetzt. Die strategischen Aktionen werden wiederum, wie in Abschnitt 5.4 gezeigt, in Policies und Pläne umgesetzt. Die Pläne werden meist in Form von Projekten realisiert.

5.4

Strategie-Umsetzung

5.4.1

Strategie-Umsetzung mittels Balanced Scorecards (BSC)

Für ein integriertes Risikomanagement gehört die Strategiefindung und Strategieumsetzung zu den wichtigsten Bestandteilen. Gilt es doch bei der Strategiefindung die Chancen und auch die Risiken in einem Unternehmen zu erkennen und mit entspre-

* SWOT: Strengths, Weaknesses, Opportunities and Threats.

† Oft werden die gesamten Resultate des Strategie-Prozesses einschliesslich SWOT-Analysen, Strategischen Ziele und strategischen Aktionen als „Strategie“ zu bezeichnen.

	chenden Massnahmen für ein nachhaltiges Gedeihen des Unternehmens umzusetzen.
<i>Misserfolgsquoten von Strategien</i>	Das oben bereits erwähnte Konzept der Balanced Scorecard sollte insbesondere die hohen Misserfolgsquoten von Strategien bei ihrer Umsetzung reduzieren. Die Balanced Scorecard wird wie die Strategischen Ziele aus der SWOT-Analyse, den normativen Vorgaben, der Mission und der Vision des Unternehmens oder des Geschäftsfeldes abgeleitet.
<i>Perspektiven der Balanced Scorecard</i>	Dabei werden die Strategischen Ziele in vier Perspektiven eingeordnet [Kapl01]. Dies sind: • Finanzielle Perspektive • Kundenperspektive • Interne Prozessperspektive • Lernen- und Entwicklungsperspektive
<i>Ursache/Wirkungs-Beziehung</i>	Die Ziele dieser Perspektiven stehen untereinander in bestimmten Ursache/Wirkungs-Beziehungen. Beim Entwickeln der „Balanced Scorecard“ als Output aus dem Strategie-Prozess ist insbesondere auf die Ausbalancierung der kurzfristigen mit den langfristigen Zielen, der monetären mit den nichtmonetären Kennzahlen, der Frühindikatoren mit den Spätindikatoren und der internen mit den externen Gegebenheiten zu achten.
<i>Strategy Map</i>	Für die wichtige Kommunikation zur Umsetzung der Strategien dient eine sog. „Strategy Map“, welche, in graphischer Darstellung, die Ursachen-Wirkungszusammenhänge der Strategischen Ziele logisch und umfassend widerspiegelt (s. Beispiel in Abbildung 5.5).

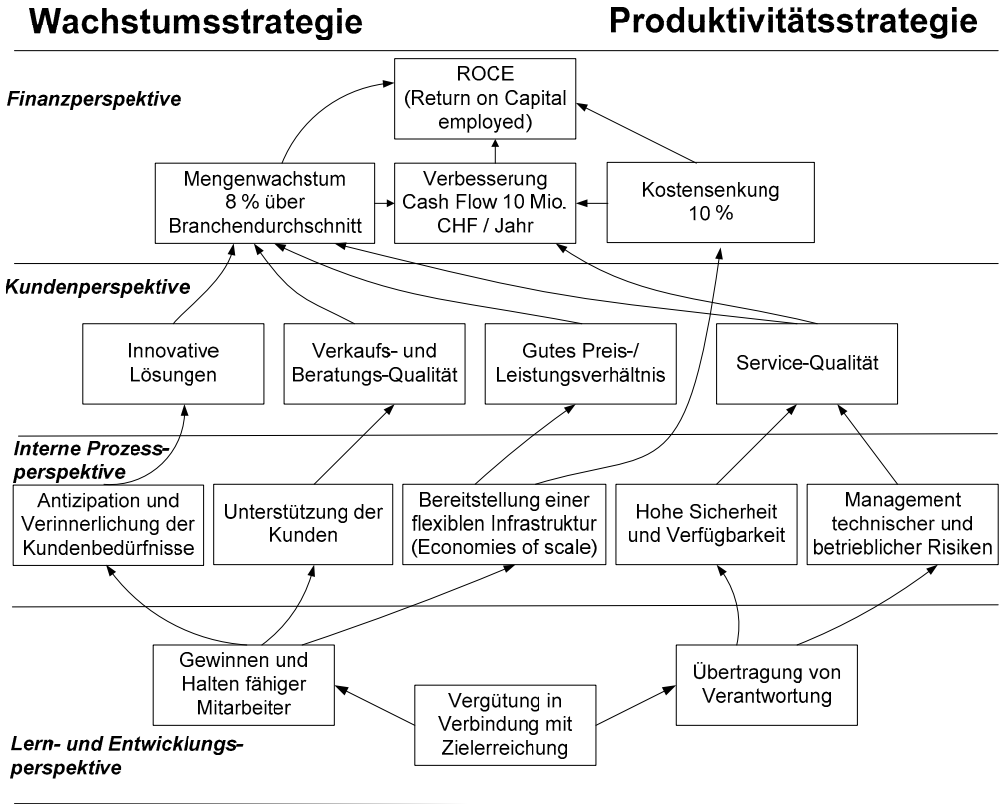


Abbildung 5.5 Beispiel „Strategy Map“ eines IT-Dienstleistungsunternehmens

Das Konzept der Balanced Scorecard (BSC) wird der Anforderung gerecht, das Risikomanagement, und speziell das Informationssicherheits- und IT-Risikomanagement, in die Management-Prozesse eines Unternehmens zu integrieren. Deshalb ist das BSC-Konzept nachfolgend in groben und wesentlichen Zügen wiedergegeben.

Dimensionen der BSC

Das BSC-System hat die folgenden drei Dimensionen [Kapl01]:

1. **Strategie:** Gemäss dem BSC-System ist es jeder Person im Unternehmen möglich, die Strategien zu verstehen und danach zu handeln;
2. **Fokus:** Sämtliche Unternehmensressourcen und -aktivitäten sind auf die Strategie ausgerichtet (s. Abbildung 5.6);

3. **Organisation:** Die BCS liefert Logik und Struktur zur Vernetzung zwischen Geschäftseinheiten, Shared Services* und einzelnen Mitarbeitern.

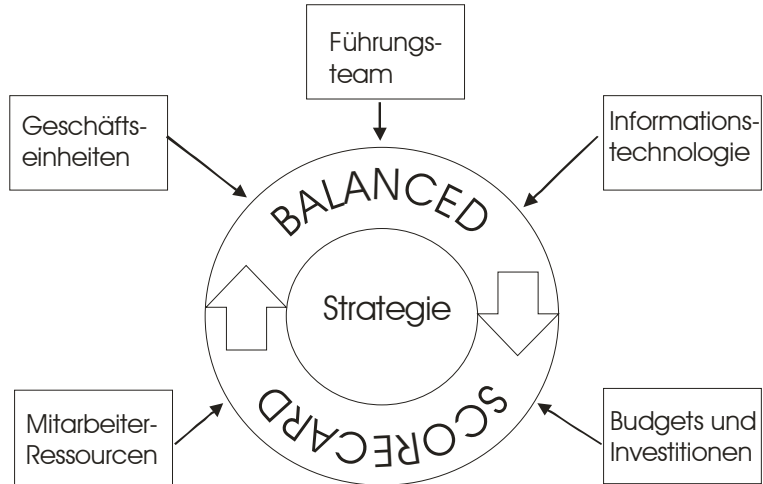


Abbildung 5.6: Ausrichtung und Fokussierung der Ressourcen auf die Strategie [Kapl01]

Fünf Grundsätze Die Ausrichtung und Fokussierung mit der BSC beruht auf folgenden fünf Grundsätzen [Kapl01]:

1. **Operationalisierung der Strategie:** Im Rahmen der BSC wird die Strategie in verständlicher Weise vermittelt, sodass sämtliche Mitarbeiter vom Top-Management bis zur Ausführungsebene die Strategie umsetzen und an der Verbesserung der Strategie mitwirken können. Das Rahmengerüst dazu ist eine logisch strukturierte und umfassende Struktur, die als „Strategy Map“ bezeichnet wird. Mit der Strategy Map wird gezeigt, wie „immaterielle Vermögen“ in materielle (finanzielle) Erfolge transformiert werden. Der Einsatz quantitativer, aber nicht finanzieller Werte in der Scorecard – wie Zykluszeiten,

* Dienstleistungen, die zusammen mit einem anderen Unternehmen erstellt oder angeboten werden.

Marktanteile, Innovationen, Kompetenzen und Kundenzufriedenheit – erlaubt es, wertschaffende Prozesse nicht nur zu vermuten, sondern zu beschreiben und zu messen.

2. **Ausrichtung der Organisation an der Strategie:** Die Kommunikationsbarrieren funktional strukturierter Organisationseinheiten werden durchbrochen. Die Unternehmensführung ersetzt formale Berichtsstrukturen durch strategische Themen und Prioritäten, welche die Kommunikation einer konsistenten Botschaft und eines konsistenten Satzes von Prioritäten über die verschiedenen Organisationseinheiten des Unternehmens ermöglicht.
3. **Strategie als „Everyone’s Everydays Job“:** Das Strategie-fokussierte Unternehmen bedarf des Verständnisses der Strategie durch alle Mitarbeiter bei der Durchführung ihrer tagtäglichen Aufgaben. Dadurch sind alle Mitarbeiter aufgefordert, zum Erfolg der Strategie beizutragen. Damit ist nicht „Top-down-Anweisung“, sondern „Top-down-Kommunikation“ gemeint.
4. **Strategie als kontinuierlicher Prozess:** Der Management-Prozess darf sich nicht alleine um das Budget und die operative Planung kümmern, sondern muss das strategische Management (d.h. die langfristigen Initiativen) nahtlos und kontinuierlich integrieren. Damit die langfristigen Aktionsprogramme nicht vor den kurzfristigen Erfolgen zu kurz kommen, sind zwei Arten von Budgets, ein „strategisches“ und ein „operatives“, denkbar. Die Strategie sollte nicht nur einmal jährlich, sondern mehrmals (monatlich oder vierteljährlich) in den Management-Meetings behandelt werden. Ein Lern- und Adaptionsprozess der Strategie, ausgehend von den ursprünglichen strategischen Hypothesen bis hin zu Feedback- und Reporting-Systemen, soll die Erkennung und Feinabstimmung der strategischen Chancen und Risiken ermöglichen.
5. **Mobilisierung des Wandels durch die Führung:** Für eine erfolgreiche Balanced Scorecard ist die Erkenntnis wichtig, dass es dabei nicht um ein Leistungsmessungs-Projekt, sondern um ein Projekt des Wandels geht. Mit der Scorecard wird die Strategie beschrieben, während das Managementsystem die einzelnen Teile des Unter-

nehmens mit der Scorecard verknüpft. Für gute Manager gibt es keinen „Stillstand“: Die Wettbewerbs-Landschaft verändert sich ständig, daher müssen sich die Strategien entfalten und sich ständig an den veränderten Chancen und Gefahren widerspiegeln. Dazu bedarf es eines ständigen Prozesses. Die Kunst des Führens besteht dabei in der feinfühligem Ausbalancierung des Spannungsfeldes von Stabilität und Veränderung.

5.4.2

Unternehmensübergreifende BSC

*Unternehmens-
weite BSC*

Unternehmen mit mehreren strategischen Geschäftseinheiten (z.B. Gruppengesellschaften) verwenden eine übergeordnete sogenannte „**Corporate Scorecard**“, mit der die unternehmensweiten strategischen Prioritäten definiert werden.

*Eigene BSC für
jede Strategische
Geschäftseinheit*

Zusätzlich definiert jede „**Strategische Geschäftseinheit**“ des Unternehmens eine eigene Strategie und eine eigene Balanced Scorecard, die auf die Corporate Strategie abgestimmt sind.

*BSC für jede Sup-
port-Einheit*

Ebenso entwickelt jede „**Support-Einheit**“ eines Unternehmens (z.B. Finance, Marketing und Information Technology) einen strategischen Plan und eine Balanced Scorecard, um die möglichen Synergien über die strategischen Geschäftseinheiten zu verwirklichen.

*BSC für strate-
gisch wichtige
externe Partner*

Pläne und Balanced Scorecards werden auch im Zusammenspiel mit **strategisch wichtigen externen Partnern** (z.B. Joint Ventures, Outsourcer, Distributors) entwickelt. Damit werden die Beziehungen zu den Partnern im Kontext zu den „Strategischen Geschäftseinheiten“ aufgezeigt.

5.4.3

Balanced Scorecard und CobiT für die IT-Strategie

*BSC zur Umset-
zung der Ge-
schäftsziele
durch die IT*

Die Informationstechnologie ist hauptsächlich „Enabler“ für die Geschäftstätigkeiten eines Unternehmens (Abbildung 5.7). Das CobiT-Framework (CobiT: Control Objectives for Information and related Technology) zeigt einen Ansatz, wie unter Zuhilfenahme der Balanced Scorecard die im Strategieprozess erarbeiteten Geschäftsziele in messbare und kontrollierbare Handlungen, bezogen auf den IT-Bereich eines Unternehmens, umgesetzt werden können [Cobm00]. Umgekehrt zeigt der Ansatz auch, wie die Leistungen der IT die Erreichung von Geschäftszielen optimal unterstützen.

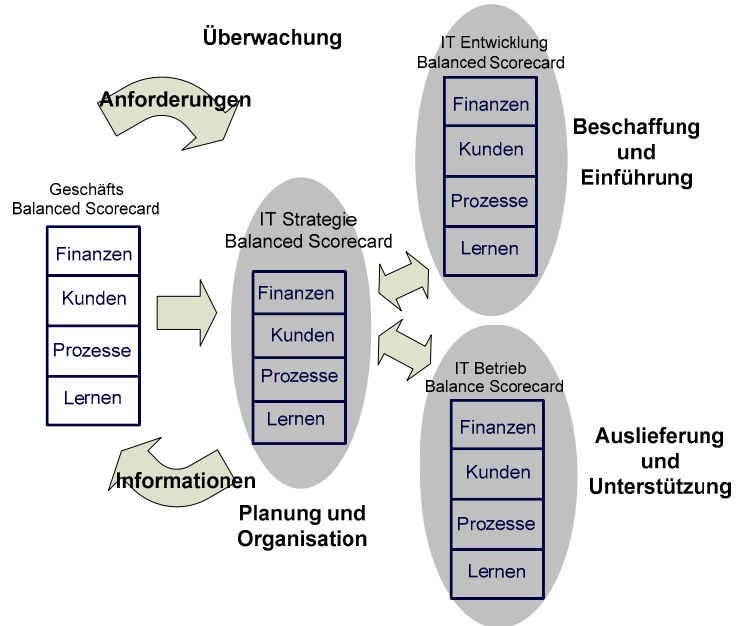


Abbildung 5.7: IT-Prozesse als Enabler für Geschäftsziele [Cobm00]

Informationskriterien

Die durch die Prozesse der IT für die Geschäftsanforderungen zu erreichenden Ziele (Goals) werden gemäss CobiT durch die sogenannten „Informationskriterien“ beeinflusst.

Informationskriterien-Profil

Die Bedeutung und das Mass eines jeden Informationskriteriums sind vom Geschäft und seinen Umgebungsanforderungen abgeleitet. Dies wird der Forderung gerecht, dass die IT in einem Unternehmen die durch die Geschäfte verlangten Informationen und Informations-Funktionen so zu liefern hat, dass die Geschäftsziele erreicht werden können. Die Anforderungen dazu werden mit einem „Informationskriterien-Profil“ eines Geschäfts festgehalten (s. Abbildung 5.8).

Das Informationskriterien-Profil widerspiegelt somit die Positionierung des Geschäfts (der Geschäftseinheit oder des Unternehmens) bezüglich seiner Informationssicherheits- und IT-Risiken.

Hat ein Informationskriterium den Wert „Null“, dann besteht für das betrachtete Geschäft für dieses Kriterium keine Anforderung. Hat ein Kriterium den Wert „Eins“ (z.B. für „Integrität“ in Abbil-

Sollanforderungen an die Informationen

dung 5.8), dann ist durch das Geschäft die höchstmögliche Einhaltung dieses Kriteriums gefordert.

In dieser Weise stellt das Informations-Kriterien-Profil die „Soll“-Anforderungen des Geschäfts an die Informationen und ihre Prozesse dar, gegen die der Ist-Zustand der Informationen und Prozesse gemessen werden kann.

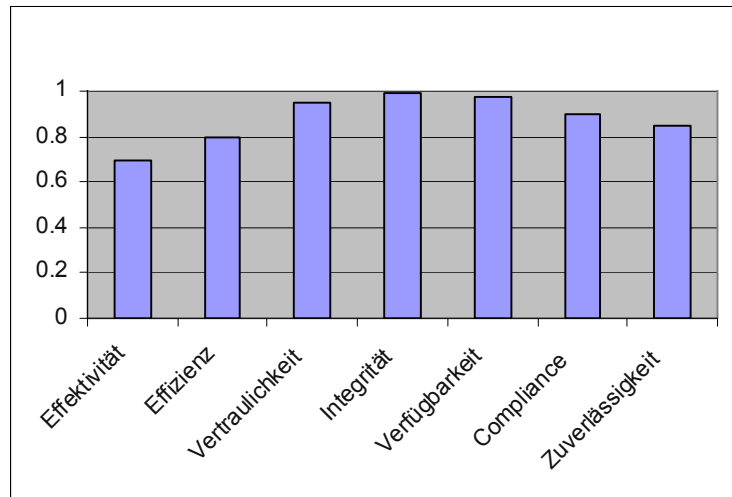


Abbildung 5.8: Beispiel „Informationskriterien-Profil“

5.4.4

IT-Indikatoren in der Balanced Scorecard

Messung durch Indicators und Critical Success Factors

Für die Zieldefinition und Messung der Strategie-Umsetzung durch die IT-Organisation verwendet CobiT [Cobm00] die beiden Indikatoren,

- Key Goal Indicator (KGI)
- Key Performance Indicator (KPI)

sowie die

- Critical Success Factors (CSF)

Messgrößen

Der „**Key Goal Indicator**“ (KGI) definiert das Mass, mit dem ein IT-Prozess die Geschäfts-Anforderungen (Business Requirements) bezüglich der Informationskriterien (s. Abbildung 5.9) erfüllt.

Damit drückt dieser Indikator den (möglichst) messbaren Erfolg des IT-Prozesses hinsichtlich der Geschäftsanforderungen aus und ist damit auf die „Finanz-Perspektive“ und auf die „Kunde-Perspektive“ der Balanced Scorecard fokussiert.

Kurz ausgedrückt ist der KGI ein Mass darüber, „was“ erreicht wurde und somit eine „nachlaufende“ auf die „Effektivität“ der IT-Prozesse abzielende Kennzahl.

Es leuchtet ein, dass der beste IT-Prozess unnütz ist, wenn er die Geschäftsanforderungen nicht erfüllen kann.

Hingegen ist der „**Key Performance Indicator**“ (KPI) ein Mass darüber, „wie gut“ ein IT-Prozess seine vorgesehene Leistung erfüllt und damit für das Erreichen eines Ziels (Goal) befähigt; er ist somit eine „vorlaufende“ auf die „Effizienz“ der IT-Prozesse abzielende Kennzahl.

Damit drückt der KPI in messbaren Begriffen eine Wahrscheinlichkeit für einen zukünftigen Erfolg oder Misserfolg aus und ist auf die „Interne Prozess-Perspektive“ und die „Lern- und Entwicklungs-Perspektive“ der Balanced Scorecard fokussiert, womit er zum Key Goal Indicator des Prozesses in einem „Ursache/Wirkungs“-Verhältnis steht.

Die „**Critical Success Factors**“ (CSF) repräsentieren die wichtigsten Dinge, die getan werden müssen, um den Erfolg des Prozesses in der Erfüllung seiner Ziele zu erhöhen. Sie sind meist messbar und werden in Begriffen des Prozesses und weniger in Begriffen des Geschäfts ausgedrückt.

Beispiel:

Die IT-Prozesse sind definiert und an der IT-Strategie und den Geschäftszielen ausgerichtet.

Befähigungsfunktion der IT

Da die IT-Prozesse in erster Linie als Unterstützungs-Prozesse für die Geschäftsprozesse anzusehen sind, kann mit den beiden Indikatoren, KGI und KPI, gezeigt werden, inwiefern die IT-

Prozesse eine „Befähigungs“-Funktion (enabling function) für die Erfüllung der Geschäftsziele ausüben (s. Abbildung 5.9).

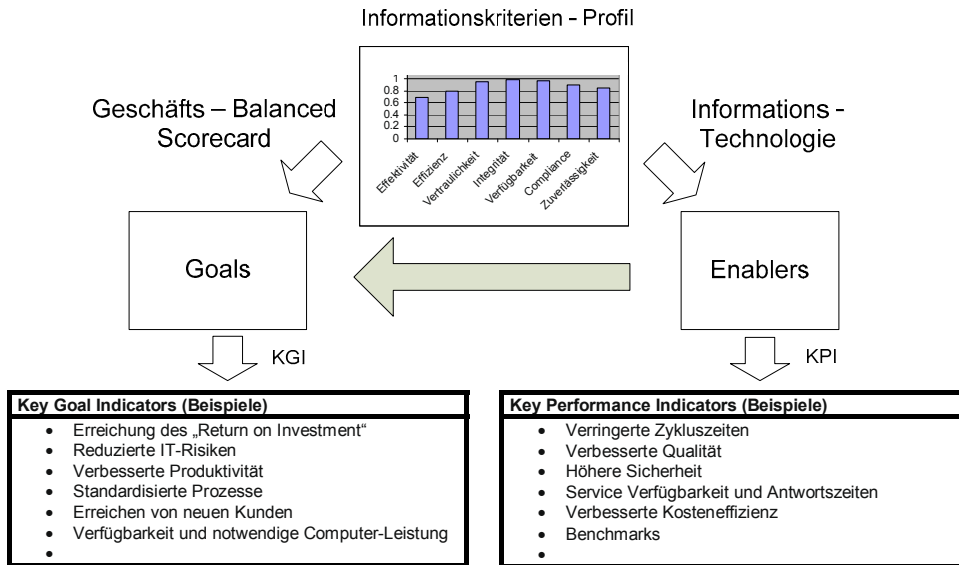


Abbildung 5.9: Messung von IT-Prozessen mit „KGI“ und „KPI“ in der BSC

Beispiel:

Bei der Festlegung der Geschäftsstrategie eines IT-Dienstleistungs-Unternehmens wird festgestellt, dass ein Geschäftsprozess an erheblichen Umsatzeinbussen leidet. Die Analyse zeigt, dass sowohl durch Kunden wahrgenommene Sicherheitsprobleme und längere System-Ausfälle als auch hohe Preise für das Umsatz-Problem massgeblich verantwortlich sind. Im Rahmen der IT-Strategie werden deshalb in einer Balanced Scorecard (s. Abbildung 5.10) die Geschäfts-Ziele, IT-Ziele sowie die für die Strategie notwendigen KGIs und KPIs nach CobIT dargestellt.

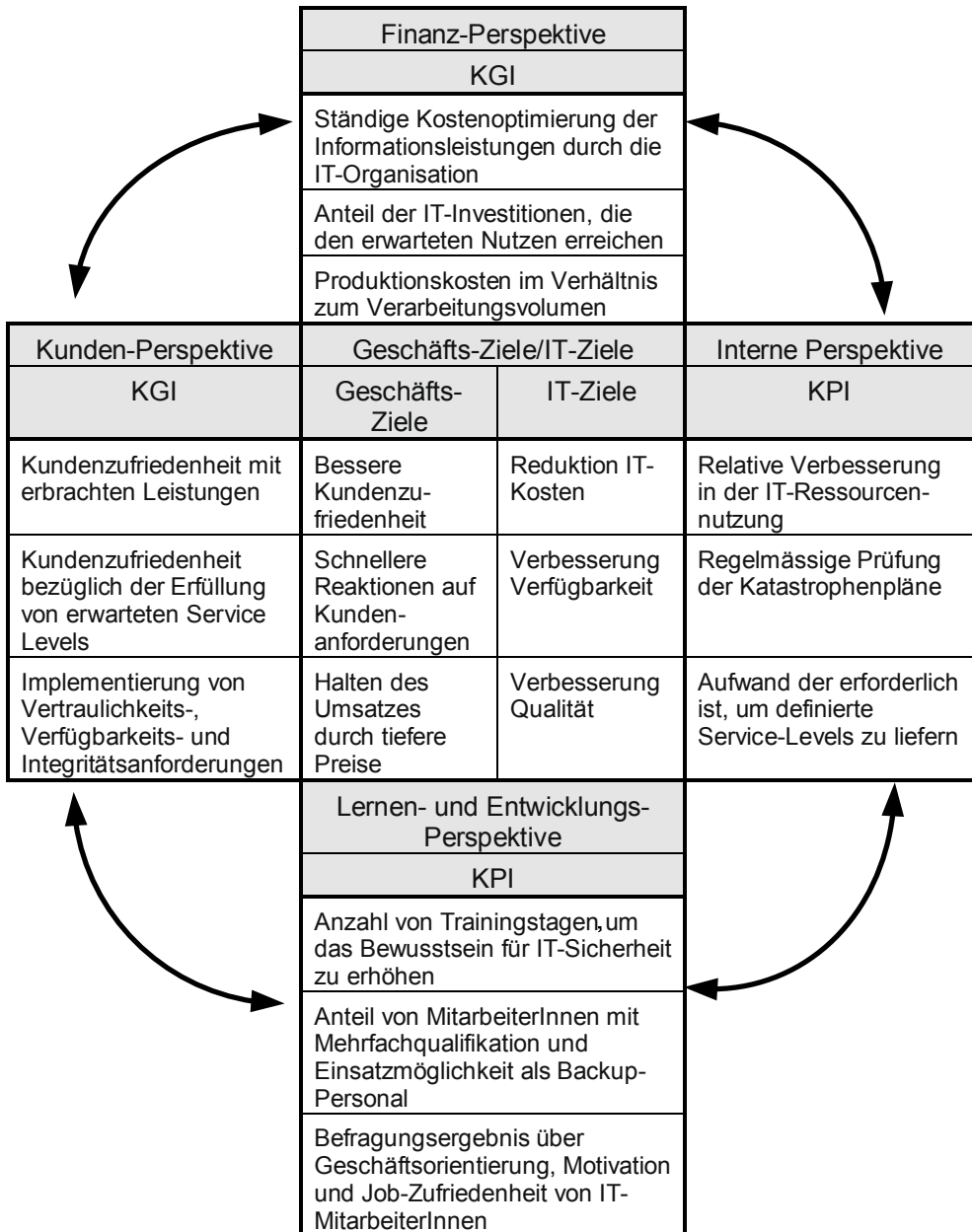


Abbildung 5.10: Beispiel für Ziele und Indikatoren in einer IT Balanced Scorecard

Risiko-Indikatoren

Als **Risk-Indikatoren** für die Zielerfüllung können die KGIs und KPIs in ihrer Aussage invertiert werden. Mittels solcher invertierten KGIs und KPIs können beispielsweise die Risiken bei der Strategie-Umsetzung mittels der Balanced Scorecard kontrolliert werden, z.B.:

- ☐ Fehlende Kostenoptimierung der Informationsleistungen;
- ☐ Ungenügende Verbesserung in der IT-Ressourcen-Nutzung;
- ☐ Wenige der IT-Investitionen erreichen das erwartete Nutzenresultat;
- ☐ Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen der Kunden ungenügend umgesetzt;
- ☐ Mangelnde Kundenzufriedenheit infolge nicht erfüllter Service Levels.

Damit zeigen solche „Risk-Indikatoren“ u.a. die „Schwachstellen“ auf, wo die strategischen Massnahmen ungenügend umgesetzt wurden.

5.4.5**Operatives Management (Gewinn-Management)***Umsetzung der Vorgaben*

Die durch das normative und strategische Management festgelegten Vorgaben bedürfen der Umsetzung durch das operative Management. Das operative Management steuert, lenkt und kontrolliert die leistungs-, finanz- und informationswirtschaftlichen Prozesse in einem Unternehmen.

Zielbezogene Problemlösungs-Prozesse

Die Problemlösungs-Prozesse des operativen Managements sind zielbezogen auf die Lenkung einzelner Aufträge, die Anpassung der Management- und Organisationsstrukturen sowie auf das Mitarbeiterverhalten in Bezug auf die situativen Gegebenheiten ausgerichtet.

Risiko-Bewältigung

Die Bewältigung der Risiken durch Dispositionen, Aktivitäten und Kontrollen fallen in die Aufgaben des Operativen Managements.

5.4.6**Policies und Pläne**

Mit der Balanced Scorecard und ihrer Strategy Map verfügen wir bereits über Instrumente, um die Strategie im Unternehmen zu kommunizieren.

*Policies:
Guides to Action*

Für das „Tagesgeschäft“ im Unternehmen braucht es zudem eine Reihe anderer Instrumente, um die Forderungen aus der Strategie und den verschiedenen Management-Prozessen zu kommunizieren und umzusetzen. Darunter nehmen die Policies (Politiken) eine wichtige Stellung ein. „Policies“ sind gemäss anglo-amerikanischer Management-Begrifflichkeit „Guides to Action“ ([Jauc88], S.30) was wir als „Leitlinien zum Handeln“ verstehen.

*Policies zur
Umsetzung von
Zielen und
Anforderungen*

Policies sind Vorgaben für das Verhalten von Führungspersonen und Mitarbeitenden und deren Handlungen im Unternehmen. Sie können sowohl als Vorgaben von der Ebene des normativen, als auch als Vorgaben von den Ebenen des strategischen wie des operativen Managements erlassen sein. Als solche kommunizieren sie, wie die Ziele und Anforderungen der jeweiligen Ebene umzusetzen sind.

Damit enthalten sie auch die Festlegungen, wie die Aufgaben, Verantwortlichkeiten, Kompetenzen und Ressourcen im Unternehmen zugeteilt werden.

Die Policies sollen bewirken (vgl. [Jauc88], S. 332), dass

- die strategischen Entscheide sowie die sonstigen verpflichtenden Anforderungen (Gesetze, Regulationen, Verträge etc.) umgesetzt werden,
- eine Basis zur Überwachung und Kontrolle gegeben ist,
- ähnliche Situationen konsistent behandelt werden können und
- die Koordination zwischen den Bereichen, Organisations- und Geschäftseinheiten erleichtert wird.

Es versteht sich von selbst, dass die auf verschiedenen Ebenen erlassenen Policies den jeweils übergeordneten Zielen und Anforderungen entsprechen müssen. Die Policies wiederholen oft die auf den verschiedenen Ebenen definierten Ziele (z.B. Ebene Strategisches Management) und kommunizieren mit Grundsätzen und weiteren Handlungsanweisungen die Umsetzung (s. Beispiel Informationssicherheits-Politik in Abschnitt 8.1.2).

Auf der Ebene des normativen Managements wird beispielsweise die allgemeine Geschäftspolitik, sowie die Sicherheits- und Risikopolitik erlassen. Folgerichtig werden solche Policies auch vom obersten Führungs- und Kontrollgremium, dem Verwaltungsrat (Aufsichtsrat) in Kraft gesetzt und deren Einhaltung kontrolliert.

<i>Policies</i>	Die Policies stellen Leitplanken dar und können je nach den sachlichen Erfordernissen enger (hart) oder weiter (weich) gefasst werden. So werden beispielsweise die gesetzlichen und regulativen Anforderungen oder die Vorgaben bezüglich der Sicherheit und des Risikomanagements in eng gefasste Policies gekleidet.
<i>Weisungen</i>	Solche „harten“ Policies werden oft auch als „Weisungen“ bezeichnet und sind im definierten Gültigkeitsbereich unter Sanktionsandrohungen einzuhalten.
<i>Ausführungsbestimmungen</i>	Andere Policies sind weiter gefasst. Solche weiter gefassten Policies können auch die Ausführungsbestimmungen für notwendige Regelungen sein. Die weiter gefassten Policies werden oft auch als „Richtlinien“ bezeichnet. Als solche können sie beispielsweise als Umsetzungsanleitungen der Strategien dienen.
<i>Pläne</i>	Zur operationellen Umsetzung der Strategien werden neben den Policies auch Pläne entworfen. Die Pläne spiegeln die konkrete Ausgestaltung der Strategie (z.B. Umsetzung einer Expansions-Strategie) in den einzelnen Bereichen des Unternehmens wieder (z.B. Geschäftsbereichen, Marketing, Finanz oder IT) Für jeden einzelnen Plan kann wiederum eine Reihe von Policies dafür sorgen, dass der Plan in der beabsichtigten Weise umgesetzt wird, um die strategischen Ziele erreichen zu können. Eine wesentliche Anforderung an die Pläne und Policies ist, dass sie untereinander keine Widersprüche enthalten.

Praxistipp:

Policies

- so kurz und prägnant wie möglich fassen
- Inhalte auf das Wesentliche beschränken
- Instrumente zur ständigen Kommunikation einsetzen, z.B. Intranet

5.4.7

Risikopolitische Grundsätze

Der Risikobezug der strategischen Unternehmens-Ziele muss mit den „Risikopolitischen Grundsätzen“ des Unternehmens im Einklang stehen.

Grundlegende Merkmale einer Risiko- und Sicherheits-Politik

Die Risikopolitischen Grundsätze sind meist innerhalb einer Policy abgefasst (z.B. in einer Risiko- und Sicherheits-Politik). Mit den Risikopolitischen Grundsätzen werden die grundlegenden

*Haltung
bezüglich Risiko-
Freude oder
Risiko-Aversion*

Merkmale der Risiko- und Sicherheits-Politik im Unternehmen festgelegt. Sie zeigen unter anderem die grundlegende Haltung der Unternehmensleitung zur Handhabung der Risiken.

Sie bringen auch zum Ausdruck, inwieweit das Eingehen von Risiken erwünscht oder unerwünscht und was die Risiko-Freude oder Risiko-Aversion des Unternehmens ist. Sie sollen die grundsätzlichen Verhaltensregeln für die Führungskräfte und die Mitarbeitenden im Umgang mit bedeutenden Risiken kommunizieren. Da die Risikopolitischen Grundsätze für das Unternehmen grundlegenden und langfristigen Charakter haben, sind sie Bestandteil der Unternehmenspolitik auf der Ebene des normativen Managements. Für einzelne Unternehmensbereiche und Teilbereiche werden die Risikopolitischen Grundsätze in spezifische Policies (Weisungen), die den operativen Anforderungen entsprechen, aufgefächert.

*Informationssi-
cherheits-Politik*

Die Informationssicherheits-Politik ist eine solche von den „Risikopolitischen Grundsätzen“ des Unternehmens abgeleitete Policy. Im Teil C (Abschnitte 8.1.2 und 8.1.3) dieses Buches wird anhand von Beispielen gezeigt, wie eine solche „Information Security Policy“ anhand mehrerer spezifischer Weisungen sinnvoll aufgebaut werden kann.

5.5

Umsetzung von Anforderungen mit Management-Systemen

Im Abschnitt 4.1 wurden bereits anhand des St. Galler Management-Modells die grundsätzlichen Funktionen von Management-Prozessen im Unternehmen beleuchtet. Verschiedene solcher Prozesse, wie der Strategieprozess, der Risikomanagement-Prozess oder der Informationssicherheits-Management-Prozess haben gemeinsam, dass den Veränderungen, die sowohl von innen als auch von aussen kommen, durch entsprechende Kontroll- und Rückkopplungsschleifen Rechnung getragen werden muss.

*Gesetze, Regulie-
rungen und
Kodizes*

Gesetze, Regulierungen und Kodizes stellen einen Teil der Anforderungen dar, denen ein Unternehmen zur Minimierung der Risiken sowohl des Unternehmens selber, als auch seiner vielfältigen Anspruchsgruppen, gerecht werden muss.

Zur Berücksichtigung und Einhaltung solcher Anforderungen, wie sie bereits im Abschnitt 4.3 und seinen Unterabschnitten diskutiert wurden, haben sich in den letzten Jahren eine Vielzahl von Rahmenwerke und Standards etabliert, die in die Management-Systeme von Unternehmen einfließen oder sogar für be-

*Rahmenwerke
und Standards*

stimmte Anforderungen komplette Managementsysteme vorgeben.

Die Betrachtung solcher Rahmenwerke und Standards ist bei der Umsetzung eines möglichst integrierten Risikomanagements wichtig, da sich der Risikomanagement-Prozess möglichst einheitlich in die verschiedenen Management-Systeme eines Unternehmens einreihen sollte.

5.5.1**Management-Systeme***Management-
Ziele nachhaltig
und nachvoll-
ziehbar*

Die **Management-Systeme** beschreiben die Aufgaben des Managements und verknüpfen „Strukturen“, „Prozesse“, „Mittel“ und „Methoden“, um die Management-Aufgaben, *Ziele setzen, steuern und kontrollieren*, erfolgreich bewältigen zu können. Als solche beinhalten sie in systematischer Weise Aktivitäten, Verantwortlichkeiten und Dokumentationen, um auch im Sinne von „Interner Kontrolle“ und „Risikomanagement“ die Management-Ziele nachhaltig und nachvollziehbar erreichen und umsetzen zu können.

Jedes Unternehmen wird implizit und vermehrt auch explizit mittels einem oder mehreren Management-Systemen geführt. Dazu sind bereits Rahmenwerke und Standards vorhanden, auf die sich Gesetzgeber, Regulatoren und Anspruchsgruppen, zur Einhaltung der Anforderungen an die Unternehmensführung, gerne beziehen.

Managementsysteme mit spezifischen Fokus sind beispielsweise:

- Risikomanagement-System (ISO 31000)
- Business-Continuity-Management-System (ISO 22301)
- Qualitäts-System (ISO 9001),
- Umwelt-Management-System ISO (14001),
- Informationssicherheits-Management-System (ISO/IEC 27001)
- Servicemanagement-System (ITIL oder ISO/IEC 20000-x)
- COSO* - Internal Control – Integrated Framework
- COSO – Enterprise Risk Management – Integrated Management Framework

* COSO: Committee of Sponsoring Organizations of the Treadway Commission

<i>Integriertes Managementsystem</i>	Ein Unternehmens-Management-System ist meist aus mehreren Einzel-Management-Systemen aufgebaut. Werden mehrere solcher Managementsysteme zusammengeführt und die Aufgaben und Aspekte ganzheitlich erfasst und umgesetzt, dann sprechen wir von einem „Integrierten Managementsystem“.
<i>Struktur der Managementprozesse</i>	Die Managementsysteme beinhalten die zur Disziplin gehörenden Grundsätze, Richtlinien und Vorgaben, sowie die für die systematische Behandlung der Management-Aufgaben notwendigen „Managementprozesse“. Die Struktur der Managementprozesse zielt darauf ab, die aktuellen und zukünftigen inneren und äusseren Veränderungen in die Führungsentscheide einzubeziehen und für eine laufende Verbesserung und Optimierung der Prozessziele zu sorgen.
<i>laufende Verbesserung und Optimierung</i>	
<i>Plan-Do-Check-Act-Zyklus</i>	Als Prinzip der Prozessabfolge bei Managementsystemen sowohl der gesamten Prozesse als auch der Teilprozesse hat sich, als Problemlösungs-Prinzip, der Plan-Do-Check-Act-Zyklus eingebürgert und auch bewährt.
<i>Deming cycle</i>	Dieses Prinzip, ursprünglich als Shewhart*-cycle und später als „Deming cycle“ bezeichnet, wurde vor allem durch den Amerikaner W. Edwards Deming, Schüler von Walter A. Shewhart, zur Verbesserung der Qualität in der japanischen Automobilindustrie erfolgreich eingesetzt. Das Prinzip dient vor allem der fortlaufenden Anpassung, Verbesserung und Optimierung des jeweiligen Management-Gegenstandes, wie Qualität oder Sicherheit. Besonders in den durch die ISO standardisierten Managementstandards ist dieses Prinzip zumindest implizit und für einige Managementaufgaben sogar explizit* gefordert.
<i>Parametrisierungen der Prozesse</i>	Die meist generisch aufgesetzten Management-Standards können durch entsprechende Parametrisierungen† der Prozesse und Teilprozesse für jegliche Unternehmen und Unternehmensgrößen eingesetzt werden.
<i>Unternehmenskultur</i>	

* Im Risikomanagement-Standard ISO 31000 ist der Aufbau und Unterhalt eines Risikomanagement-„Framework“ im Unternehmen explizit einem PDCA-Zyklus unterworfen.

† Die Teilprozesse mit Input, Aktivität und Output können beispielsweise durch die Festlegung von „Prozess-Ziel“, Prozessleistungsmessung mittels „Key Performance Indikator (KPI)“, „Prozess-Frequenz“ und „Prozess-Owner“ parametrisiert werden.

Ein wesentliches Augenmerk aller Management-System-Standards ist zudem auf die Unternehmenskultur (u.a. das Management-Commitment und Mitarbeiterverhalten) gerichtet.

5.5.2

Vereinheitlichung Management-System-Standards durch ISO

Es ist nicht verwunderlich, dass die teilweise überlappenden Vorgaben verschiedener in einem Unternehmen gleichzeitig einzusetzenden Frameworks und Standards von Management-Systemen nach einer Integration der unterschiedlichen Management-Systeme rufen.

*Einheitliche
Grundstruktur
und Kern-
definitionen*

Diesem Wunsch der Integration versucht die ISO bei der Ausarbeitung von Management-System-Standards zukünftiger oder überarbeiteter Versionen durch eine einheitliche Grundstruktur und durch einheitliche Textphrasen, basierend auf einheitlichen Kern-Definitionen, Rechnung zu tragen.

ISO Guide 83

Inwiefern sich diese neuen, auf den neuen „ISO Guide 83“ ausgerichteten Standards* in der Praxis mit anderen Managementstandards nutzbringend integrieren lassen, wird die Zukunft zeigen.

Wie bereits erwähnt, kann der PDCA-Zyklus eines übergeordneten Management-Systems auch auf die Teilprozesse eines Management-Systems angewendet werden. Eine Zusammenfassung der im ISO Guide 83 vorgegebenen High-Level-Struktur für ein integriertes Management-System ist in Abbildung 5.11 veranschaulicht.

*High-Level-
Struktur*

Durch die Abbildung 5.11 wird offenbar, dass der in Kapitel 3 ausführlich behandelte Risikomanagement-Prozess hauptsächlich in der DO-Phase der High-Level-Struktur abläuft und auf diese Weise mit dem PDCA-Zyklus des übergeordneten Unternehmens-Risikomanagement-Systems interagiert.

* Anm.: Eine neue in Bearbeitung befindliche Version von ISO/IEC 27001 basiert ebenfalls in seiner Struktur auf dem Standard „ISO Guide 83“.

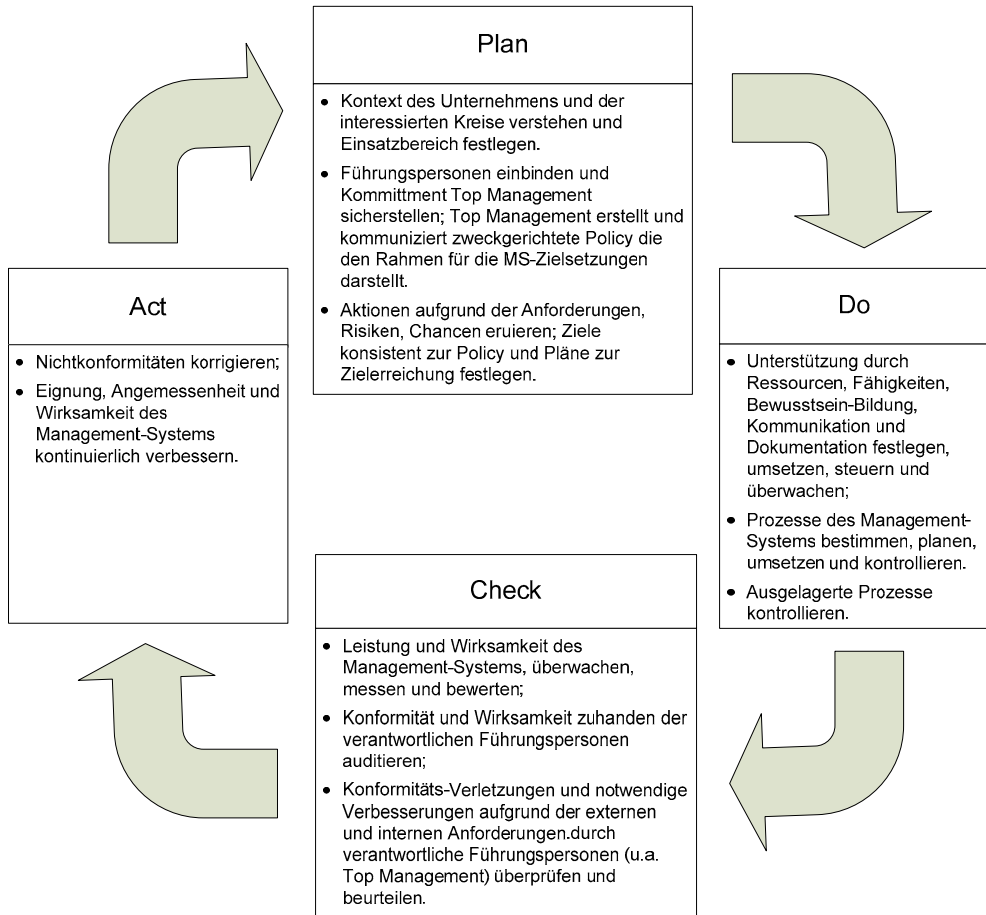


Abbildung 5.11: High-Level Struktur für Management-Systeme (vgl. [Isod11])

5.6 Zusammenfassung

Im integrierten Risikomanagement-Prozess ist das Risikomanagement in das Management-System (Führungs-System) des Unternehmens integriert. Dabei muss der unternehmensweite Risikomanagement-Prozess sicherstellen, dass alle wesentlichen Risiken des Unternehmens systematisch identifiziert, analysiert, bewertet, behandelt und laufend überwacht werden.

Neben der Kundensicht werden sowohl für die Chancen als auch für die Risiken eine ausgewogene, aufeinander abgestimmte Behandlung der Unternehmens-Perspektiven „Finanzen“, „Kunden“, „Interne Prozesse“ und „Lernen / Entwicklung“ angestrebt. Die Integration des Risikomanagements findet auf der normativen-, der strategischen- wie auch der operativen Ebene des Management-Systems statt.

Insbesondere bei der Strategiefindung und der Strategieumsetzung helfen geeignete Zielsetzungen, Messgrößen und Indikatoren (u.a. Risiko-Ziele und Risiko-Indikatoren) die Risiken in den Strategiefindungs- und -umsetzungs-Prozess einzubeziehen. Den aus den strategischen Zielen über die Strategien abgeleiteten Geschäftszielen werden neben den Messgrößen oft auch Risiko-Toleranzen zugeordnet, innerhalb derer eine Zielabweichung akzeptiert werden kann.

Die Wirkungs-Zusammenhänge für ausgewogene und effektive Zielsetzungen können mit einer „Strategy Map“ der „Balanced Scorecard“ abgebildet werden. Die „Strategy Map“ stellt gleichzeitig ein wichtiges Darstellungs-Mittel zur Strategie-Kommunikation dar. Eine geeignete Methode zum Einbringen der Informatik-Unterstützung und der Informations-Risiken in die Balanced Scorecard des Strategie-Prozesses ist durch das CobiT-Framework mittels der Informations-Kriterien und entsprechenden Indikatoren (Key Goal Indicator und Key Performance Indicator) möglich.

Die Massnahmen zur Behandlung der Risiken durch Dispositionen, Aktivitäten und Kontrollen fallen in die Aufgaben des „Operativen Managements“.

Mit Policies und Plänen werden die strategischen Entscheide umgesetzt. Die Policies stellen dabei die Leitplanken dar und können je nach den sachlichen Erfordernissen enger oder weiter gefasst werden. Policies können auf der normativen, strategischen und operativen Ebene erlassen werden. Die Pläne spiegeln die konkrete Ausgestaltung der Strategie wider. Der Risikobezug der strategischen Unternehmens-Ziele muss mit den normativen „Risikopolitischen Grundsätzen“ des Unternehmens im Einklang stehen; diese zeigen vor allem die grundlegende Haltung der Unternehmensleitung zur Handhabung der Risiken und bringen unter anderem zum Ausdruck, inwieweit das Eingehen von Risiken erwünscht oder unerwünscht ist.

Verschiedene Management-Prozesse, wie der Strategie-Prozess, der Risikomanagement-Prozess oder der Informationssicherheits-

Management-Prozess haben gemeinsam, dass den Veränderungen, die sowohl von innen als auch von aussen kommen, durch entsprechende Kontroll- und Rückkopplungsschleifen Rechnung getragen werden muss, um so für eine laufende Verbesserung und Optimierung der Prozessziele zu sorgen.

Rahmenwerke und Standards sind bei der Umsetzung eines integrierten Risikomanagements wichtig, da sich der Risikomanagement-Prozess möglichst einheitlich in die verschiedenen Management-Systeme eines Unternehmens einreihen sollte. Wo bei **Management-Systeme** generell die Aufgaben des Managements beschreiben und „Strukturen“, „Prozesse“, „Mittel“ und „Methoden“ verknüpfen, um die Management-Aufgaben, *Ziele setzen, steuern und kontrollieren*, erfolgreich bewältigen zu können; dazu beinhalten die Management-Systeme Grundsätze, Richtlinien und Vorgaben, sowie die für die systematische Behandlung der Management-Aufgaben notwendigen „Management-Prozesse“.

Als Prinzip der Prozessabfolge bei Management-Systemen, sowohl der gesamten Prozesse als auch der Teilprozesse, hat sich der **Plan-Do-Check-Act-Zyklus** eingebürgert und auch bewährt. Besonders in den durch die ISO standardisierten Management-Standards ist dieses Prinzip zumindest implizit und für einige Managementaufgaben sogar explizit gefordert.

Ein wesentliches Augenmerk aller Management-System-Standards ist zudem auf die Unternehmenskultur (u.a. das Management-Commitment und Mitarbeiterverhalten) gerichtet. Dem Wunsch der Integration mehrerer Management-Systeme versucht die ISO durch eine einheitliche Grundstruktur und durch einheitliche Textphrasen, basierend auf einheitlichen Kern-Definitionen, in einem neuen Standard „ISO Guide 83“ Rechnung zu tragen.

5.7

Kontrollfragen und Aufgaben

1. Welche Zeithorizonte haben das „Normative“-, das „Strategische“- und das „Operative“ Management?
2. Welche Unternehmens-Perspektiven sollen im Strategie-Prozess miteinander abgestimmt werden?
3. Ihr Unternehmen hat die Mission, „das führende Unternehmen für das Outsourcing von IT-Dienstleistungen in Deutschland“ zu sein.

Definieren Sie eine Strategie mit fiktiven Zahlen:

- a) strategische Ziele und Messgrößen
 - b) Strategie
 - c) Abgeleitete Geschäftsziele und Messgrößen
 - d) Risiko-Appetit
 - e) Risiko-Toleranz
4. In welchen Perspektiven der Balanced Scorecard kommen die KGIs und die KPIs zur Geltung?
 5. Erläutern Sie die Begrifflichkeit und die Aufgabe einer „Policy“.
 6. Erläutern Sie grundlegende Eigenschaften von „Managementsystemen“, wie sie derzeit standardisiert werden.
 7. Erläutern Sie die dem PDCA-Zyklus der Managementsysteme inhärente Philosophie.

Teil C

Informations- Risiken erkennen und bewältigen

6

Informationssicherheits- und IT-Risiken

Schutzobjekte

Bevor wir in die Einzelheiten der Informationssicherheits- und IT-Risiken eintauchen, besinnen wir uns auf die im ersten Teil dieses Buches getroffenen Grundlagendefinitionen.

Zum Risikomanagement bei Informationen und IT-Systemen werden vorteilhaft Schutzobjekte gebildet. In der angelsächsischen Literatur wird ein Schutzobjekt als „Asset“ bezeichnet. Mit diesem englischen Begriff wird gleichzeitig ausgedrückt, dass es um Werte geht, die es zu schützen und zu erhalten gilt. Für das in unserem Buch behandelte Informationssicherheits- und IT-Risikomanagement im Unternehmen sind diese „Assets“ Unternehmenswerte. Solche Unternehmenswerte können entweder materielle Werte (z.B. Hardware) oder immaterielle Werte (z.B. Informationen) sein.

Modellvorstellung

In diesem Kapitel wird die für das Risikomanagement von Informationen und IT-Systemen geeignete Modellbildung vorgestellt. Es wird ein Einblick in die Bedeutung der Informationssicherheits- und IT-Risiken ganz allgemein gezeigt. Dazu werden die für die Informationsrisiken und deren Behandlung wichtigen Kriterien und Begriffe erläutert. Auch wird sozusagen als Vorspann zu den in den nächsten Kapiteln zu behandelnden konkreten Methoden und Verfahren ein genereller Einblick in die Möglichkeiten des Informationssicherheits- und IT-Risikomanagements vermittelt.

6.1

Veranschaulichung der Risikozusammenhänge am Modell

Auswirkungen der Bedrohungen über Schwachstellen

Bedrohungen können sich über Schwachstellen an Objekten (Schutzobjekte) als Schäden auswirken. Die Risiken sind die mit den Eintrittswahrscheinlichkeiten (Häufigkeiten) gewichteten negativen Folgen der Abweichungen von System-Zielen.

In Abbildung 6.1 sind diese Modellvorstellungen veranschaulicht. Anhand dieser Modellvorstellungen lassen sich die wesentlichen Aspekte eines praktischen, auf die Informationssicherheit und die IT zugeschnittenen Risikomanagements erklären und einordnen. Als Schutzobjekte können sich dabei Informationen aber auch ganze Systeme, Dienstleistungen oder Prozesse anbieten.

Risiken bei Informationen

Das Sicherheits-Risiko bei den Objekten „**Informationen**“ lässt sich aufgrund der drei folgenden primären* System-Ziele bestimmen:

- „Vertraulichkeit“,
- „Integrität“ und
- „Verfügbarkeit“.

Massnahmen

Schwachstellen

Bedrohungen

Impacts

Mit dem Begriff „Massnahmen“ bezeichnen wir sämtliche Vorkehrungen, Anordnungen und Eigenschaften, die ein Schutzobjekt zu schützen vermögen. Daher bezeichnen wir die Stellen mit ungenügenden oder fehlenden Massnahmen als „Schwachstellen“. Nur über die vorhandenen Schwachstellen ist es möglich, dass sich die Bedrohungen an den Schutzobjekten (Assets) als „Impacts“ auswirken können.

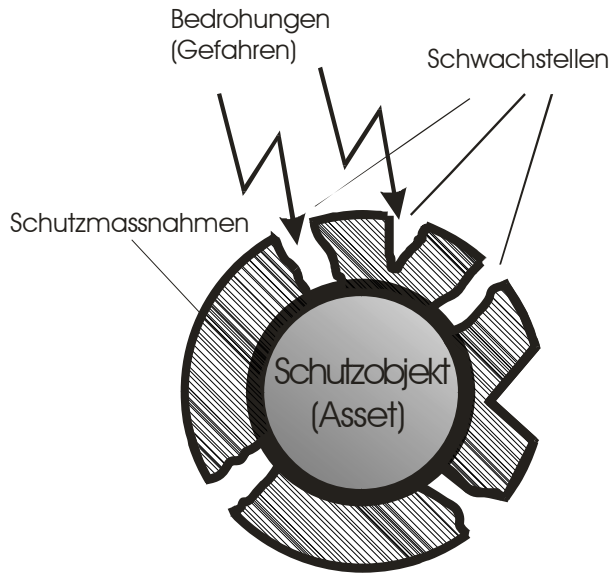


Abbildung 6.1: Modellvorstellungen für Risiken von Schutzobjekten (vgl. [Isoi03], S. 12)

* Das oft angeführte System-Ziel „Non-Repudiation“ wird nicht zu den primären System-Zielen gezählt, da es erst durch eine integrale Prozedur zur Beweisführung zustande kommt (z.B. Digitale Unterschrift). Das Ziel-System für Risiken kann jedoch auf Prozeduren und Prozesse erweitert werden.

ISO-Begriffe

Für die Variablen dieses Modells verwendet die internationale Standardisierung der ISO die in Abbildung 6.2 gezeigten Begriffe.

ISO-Begriff	Begriff im deutschsprachigen Raum
Asset	Schutzobjekt* (=alles was für ein Unternehmen, von Wert ist, z.B. Information, Software, physische Einrichtungen wie Computer, Services, Personen, nichtgreifbare Werte wie Reputation)
Threat	Bedrohung (=potentielle Ursache für ein ungewolltes Ereignis, das dem Unternehmen schaden könnte)
Control (Safeguard)	Massnahme (=Mittel zur Behandlung von Risiken, einschl. Policies, Prozeduren, Richtlinien etc.)
Vulnerability	Verletzlichkeit oder Schwachstelle (=durch Bedrohungen ausnützbare Schwäche)
Impact	Auswirkung eines Schadensereignisses (=negativen Einfluss auf die Erreichung von Geschäftszielen)
Probability	Wahrscheinlichkeit eines Ereignisses (=mathematische Variable mit numerischen Werten zwischen 0 und 1)
Frequency	Häufigkeit des Auftretens innert einer Zeitperiode
Likelihood	Wahrscheinlichkeit, relative Häufigkeit oder Häufigkeit des Auftretens innert einer Zeitperiode; objektiv oder subjektiv in quantitativen oder qualitativen Werten bestimmt, definiert oder gemessen.
Residual Risk	Restrisiko (=Risiko nach der Behandlung mit Massnahmen)

Abbildung 6.2: Begriffe der ISO-Standardisierung (vgl. [Iso09], [Iso09])

* Der Begriff „Objekt“ wird in diesem Buch synonym zu „Gegenstand“ sowohl für greifbare als auch für abstrakte Güter, Objekte und Strukturen verwendet.

6.2

Informationen – die risikoträchtigen Güter

Abhängigkeiten von Informationen

Sämtliche heutigen Unternehmen sind in der einen oder anderen Weise von Informationen abhängig oder mit Informationen konfrontiert, sei es zur Aufbereitung, Kommunikation oder zur Aufbewahrung wichtiger Sachverhalte. Die Informationen eines Versicherungsausweises dienen beispielsweise der Kommunikation und dem späteren Nachweis einer getroffenen Vereinbarung zwischen dem Versicherungsanbieter und dem Versicherungsnehmer. Oder am Beispiel eines Hochregallagers sind es die Informationen, die über digitale Steuerbefehle und Zustandswerte ermöglichen, die Lagervorgänge automatisch durchzuführen.

Eine unabsehbare Anzahl von meist abstrakten Informationsarten ist für das reibungslose Funktionieren der Prozesse in unserer technisierten Gesellschaft notwendig.

Davon einige Beispiele:

- Finanz- und Zahlungsinformationen ermöglichen die bargeldlosen Finanz- und Zahlungsströme in unserer Wirtschaft.
- Informationen im Transportwesen dienen der Planung und Kommunikation der Fahrzeiten sowie der Steuerung und Sicherung von Transport-Vehikeln, wie z.B. dem Flugzeug.
- Häuser, Maschinen, Geräte werden anhand von Informationen konstruiert und gebaut.

Die Kommunikation, Darstellung, Bearbeitung und Speicherung solcher Informationen erfolgt weitgehend mit technologischen Mitteln. Dabei sind nicht nur die Informationen selbst, sondern auch ihre „technologischen Gefäße“ (z.B. Computer, Eingabegeräte, Bildschirme, Netzwerke) für heutige Unternehmen zu lebenswichtigen Ressourcen geworden. Die Abhängigkeit von Informationen und ihren „technologischen Gefäßen“, zusammen mit der elektrischen Energie, ist in unserer industrialisierten Welt an die vorderste Stelle gerückt.

Überleben der industrialisierten Welt

In diesem Zusammenhang stellte eine durch den damaligen US-Präsidenten Bill Clinton 1997 eingesetzte Kommission fest, dass Sicherheit, Wirtschaft, die Art zu Leben und überhaupt das Überleben der industrialisierten Welt von elektrischer Energie, Kom-

munikation und Computern, die untereinander in Wechselbeziehungen stehen, abhängig ist.*

*Kritische
Infrastrukturen*

Inzwischen sind in vielen Industrie-Nationen Bemühungen im Gange, die „kritischen Infrastrukturen“ (CIP = Critical Infrastructure Protection) und darin auch die „kritischen Informations-Infrastrukturen“ (CIIP = Critical Information Infrastructure Protection) auf nationaler Ebene zu sichern [Dunn04].

*Informationen
und Daten*

Die Informationen in ihrer codierten, für IT-Systeme verständlichen Form bezeichnen wir als „Daten“. Nur die Daten zu schützen und zu sichern, würde aber zu kurz greifen, da es letztendlich die Informationen sind, die für die verschiedenen Prozesse benötigt werden.

Die Risiken schlagen hauptsächlich bei den Informationen selbst zu Buche oder bei den Übergängen (Schnittstellen) von der einen Informationsform in eine andere (z.B. bei der Postsortierung mittels Schriftenerkennung oder bei der persönlichen Anmeldung und Authentifizierung an einem System mittels eines Passworts).

*Ganzheitliches
RM in Bezug auf
Informationen*

Ein ganzheitliches Risikomanagement in einem Unternehmen muss deshalb primär an den Informationen und nicht an den Daten oder gar nur an den Informations-Systemen angesetzt werden.†

Beispiel:

In einer Bank ist das Wissen um eine Bank-Kundenbeziehung eine zu schützende Information. Die Informationen über diese Bank-Kundenbeziehung (z.B. Bonität, abgewinkelte Transaktionen, Vermögenswerte) unterliegen in der Schweiz dem Gesetz über das Bankkundsgeheimnis. Hier lediglich die Risiken bei den Daten oder den IT-Systemen und nicht bei den Informationen selbst zu betrachten, würde den Anforderungen eines ganzheitlichen, für die Bank sinnvollen Risikomanagements nicht genügen. Aus dem Blickwinkel des Unternehmens „Bank“ sind daher das „Wissen um die Bank-

* President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures. (Washington, October 1997).

† Dass in diesem Buch sowohl das Risikomanagement der Informationssicherheit als auch der IT behandelt wird, ist am Untertitel dieses Buches zu ersehen.

kundenbeziehung“, und „die Geschäftsvorgänge in ihrer Vertraulichkeit, Richtigkeit und Pünktlichkeit“ die primär zu schützenden Güter. Der Schaden einer Bank bei Bekanntwerden von Informations-Lecks kann in Strafen, Schadensersatz bis hin zu Sanktionen durch die Bankenaufsichtsbehörde sowie schweren Reputationsschäden für die Bank resultieren.

6.3

System-Ziele für Risiken Informationssicherheit und IT

*Schützenswerte
Eigenschaften*

Als schützenswerte Eigenschaften der Information definieren wir für unsere Risikobetrachtungen die folgenden System-Ziele:

- **Vertraulichkeit**

Die Informationen sind ausschliesslich den durch den Besitzer autorisierten* Personen, Entitäten oder Prozessen zugänglich.

- **Integrität (und Authentizität)**

Die Informationen werden lediglich in der vorgesehenen Weise erzeugt, verändert oder ergänzt und sind somit weder fehlerhaft noch verfälscht.

*Verfügbarkeit der
Informationen*

- **Verfügbarkeit**

Die Informationen stehen den autorisierten Personen, Entitäten oder Prozessen in der erforderlichen Weise (in vereinbarter Darstellung und Zeit) zur Verfügung.

Die Verfügbarkeit der **Informationen** hängt dabei meistens von der Verfügbarkeit der Systeme ab.

*Verfügbarkeit
(Availability)
der Systeme*

Die Verfügbarkeit der **Systeme** wird oft aus dem Mittelwert der Zeit, in der das System verfügbar ist (MTTF) und der mittleren Reparatur-Zeit (MTTR) berechnet. Mit den gebräuchlichen englischen Begriffen errechnet sich die Verfügbarkeit (Availability) mit der folgenden Formel:

$$\text{Availability} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

MTTF: Mean Time to Failure

* Der ultimative Eigentümer der Information (z.B. Bankkunde) autorisiert direkt oder über den in seinem Auftrag handelnden Dienstleister.

MTTR: Mean Time to Repair

Der Nachteil dieser Formel ist, dass sie lediglich einen Durchschnittswert angibt, aber über die „lästigen“ lang anhaltenden Ausfälle nur ungenügende Auskunft gibt. Um die lang anhaltenden Ausfälle besser zu quantifizieren oder Anforderungen an die System-Verfügbarkeit spezifizieren zu können, bietet sich der in Abschnitt 2.8.1 behandelte „Value at Risk“ in der Form eines „Systemausfall at Risk“ an. Die für eine solche Statistik benötigten Daten werden oft als „Qualitätsnachweise“ erhoben. Dabei kann es auch sinnvoll sein, die Ausfalldauern zusätzlich mit den korrespondierenden monetären Verlusthöhen zu bewerten.

Die oben genannten drei primären System-Ziele für die Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) werden oft um das folgende Ziel erweitert:

Nachweis von Informationsinhalten

- **Verbindlichkeit**

Der Benutzer der Information kann sich auf das Ergebnis seiner Informations-Interaktionen verlassen, z.B. dass die digital festgehaltenen Informationsinhalte nachweislich vom Urheber in unveränderter Weise stammen und deshalb vom Urheber auch nicht bestritten werden können (non-repudiation of origin).

Dieses über einige prozedurale Massnahmen (z.B. Digitale Unterschrift) erreichbare Ziel wird oft auch unter dem System-Ziel Integrität (und Authentizität) behandelt.

System-Ziele für Leistung, Qualität und Vertrauenswürdigkeit

Zu den oben angeführten System-Zielen bezüglich Risiken der Informationssicherheit sind weitere primäre Ziele bezüglich der Leistungsfähigkeit, Qualität und Vertrauenswürdigkeit der IT-Prozesse wichtig. Dies sind im Einzelnen (vgl. [Cobf00], S. 14):

- **Effektivität**

Es werden die für die Geschäftsprozesse relevanten und wichtigen Informationen in zeitgerechter, aktueller, fehlerfreier, konsistenter und verwendbarer Form geliefert.

- **Effizienz**

Die Bereitstellung der Informationen erfolgt mit einer optimalen Verwendung von Ressourcen.

- **Zuverlässigkeit**

Bereitstellung der geeigneten Informationen zur Steuerung der Geschäftsausübung durch das Management und zur gesetzesgetreuen und regulativen Berichterstattung im Unternehmen (Ziel nicht zu verwechseln mit der im Verfügbarkeits-Ziel enthaltenen System-Zuverlässigkeit).

- **Compliance**

Geschäfts- und IT-Prozesse erfolgen unter Einhaltung der rechtlichen, regulativen und vertraglichen Erfordernisse sowie der internen Vorgaben, z.B. auferlegte externe Geschäftskriterien und interne Policies.

In der CobiT-Terminologie werden solche primären System-Ziele auch Informationskriterien genannt, da sie vor allem den Informationsanforderungen der Geschäftsprozesse gerecht werden müssen (s. Abschnitte 5.4.3 und 5.4.4).

Mit zusätzlichen Zielen (Informationskriterien) werden auch Risiken der Beschaffung, der Leistung oder aufsichtsrechtlichen Vorgaben der IT behandelt. Im Rahmen eines IT-Risikomanagements kann es beispielsweise auch durchaus nützlich sein, System-Ziele für das Projekt-Management einzuführen.

*System-Ziele für
das IT-Projekt-
Management*

Das Zielsystem für Informationssicherheits- und IT-Risiken wird oft durch komplexe Ziele ganzer Prozesse erweitert. Die Einhaltung solcher Prozessziele wird auch im Rahmen des Risikomanagements erfasst und entsprechend behandelt.

6.4

Informationssicherheit versus IT-Sicherheit

Die Informationssicherheit ist ein primäres Anliegen des Risikomanagements im Unternehmen.

*Ziel der Informa-
tionssicherheit*

Ziel der „Informationssicherheit“ ist es, sowohl die Informationen selbst als auch die Daten, Systeme, Kommunikationen, Prozeduren und Einrichtungen zu schützen, welche die Informationen enthalten, verarbeiten, speichern oder liefern.

*Fokus der
Informationssi-
cherheit*

Der Fokus der Informationssicherheit ist somit breiter als derjenige der IT-Sicherheit (Abbildung 6.3). So trägt beispielsweise die Verfügbarkeit der IT-Systeme auch zur Verfügbarkeit der Infor-

mationen bei, geht es doch bei der Verfügbarkeit der Informationen darum, dass die Informationen zur vorgesehenen Zeit dem Benutzer zur Verfügung stehen. Somit beschränkt sich die Informationssicherheit nicht auf die Informations-Technologien, welche lediglich die „Gefässe“ für die Informationen darstellen, sondern bezieht sich auch auf Informationen in nichttechnologischer Form (z.B. Notizen auf Papier).

*Begriffe
„Informationssicherheit“ und
„IT-Sicherheit“*

Im weiteren Verlauf des Buches verwenden wir den Begriff der „Informationssicherheit“ und schliessen dabei die „IT-Sicherheit“ ein.

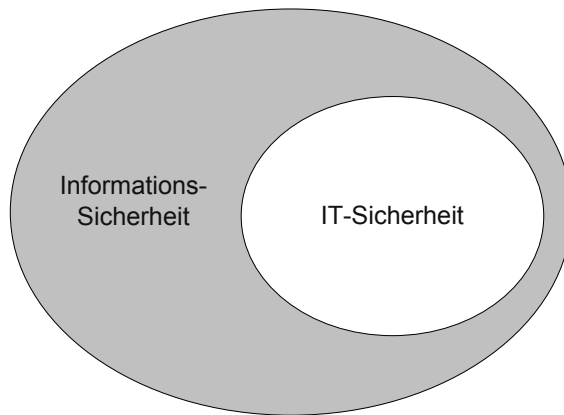


Abbildung 6.3: Fokus der Informationssicherheit

6.5

Informationssicherheits-Risiken versus IT-Risiken

Die Risiken hinsichtlich der im vorangegangenen Abschnitt behandelten Informationssicherheit bringen die Abweichungen von den Systemzielen „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ an den Informations-Objekten zum Ausdruck. Hingegen betreffen die IT-Risiken nicht alleine die Risiken über „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ in der IT, sondern auch weitere Risiken, z.B. hinsichtlich Compliance oder Effektivität der IT-Prozesse. Sie beschränken sich damit nicht auf die Informationssicherheit der IT, sondern beziehen sich auch auf Unternehmensrisiken hinsichtlich beispielsweise der IT-Ressourcen-Beschaffung und der IT-Nutzung. Die Zusammenhänge dieser

beiden Risikobereiche können gemäss der Abbildung 6.4 veranschaulicht werden.

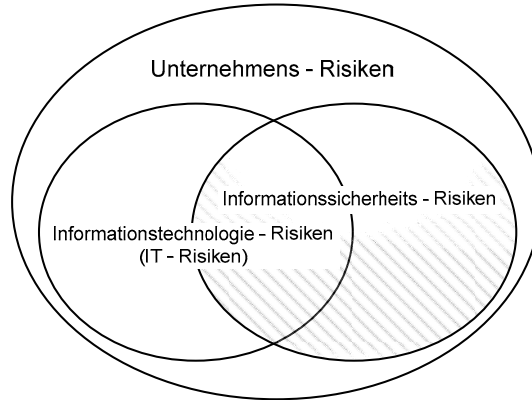


Abbildung 6.4: Zusammenhang Informationssicherheits-Risiken und IT-Risiken

Aus Sicht des Risikomanagements lassen sich die beiden Bereiche in ein gemeinsames Risikomanagement der „Informations-Risiken“ integrieren, wohlwissend dass für die beiden Risikokategorien unterschiedliche Anforderungen bestehen. Bei der Vielfalt heutiger Managementsysteme im Unternehmen ist eine solche Integration der Management-Prozesse sicherlich erstrebenswert. Auch stellt die integrierte Behandlung beider Risikobereiche einen verbesserten Bezug zu den IT-Leistungen und den vielfältigen Compliance-Anforderungen im IT-Bereich her.

Wenn wir also im weiteren Verlauf dieses Buches von „**Informations-Risiken**“ sprechen, dann betrifft dies sowohl die „Informationssicherheits-Risiken“ als auch die „IT-Risiken“.

6.6

Grundschutz und Informationssicherheits-Risikomanagement

Sprechen wir von der Sicherheit irgend einer Sache, dann knüpfen wir an den Begriff „Sicherheit“ automatisch die Vorstellung, dass die Sache „angemessen“ sicher ist, im Bewusstsein, dass es keine absolute (100 %-ige) Sicherheit geben kann. Wir gehen dabei von einer „normalen“ Bedrohungslage aus und wirken dieser mit „normalen“ Sicherheits-Massnahmen entgegen. Die bei

Grundschutz-massnahmen

einem solchen Vorgehen zum Einsatz gelangenden Massnahmen bezeichnen wir als „Grundschutzmassnahmen“ (Baseline security controls).

In Situationen mit speziellen Gefahrenpotenzialen und hohen Schadensmöglichkeiten sind solche „Grundschutzmassnahmen“ meist nicht ausreichend, da sie die spezifisch notwendige Sicherheit nur in beschränktem Umfang bieten können. In diesen Fällen ist es notwendig, die Bedrohungslage sowie die spezifischen Werte der Schutzobjekte und die Wirksamkeit der bereits vorhandenen Massnahmen in einer systematischen Art und Weise zu analysieren.

Aufgrund des Analyse-Resultats können dann die über den Grundschutz hinausgehenden Massnahmen im Hinblick auf ein „tragbares“ Restrisiko bestimmt werden.

Grundschutz, Sicherheit und Risikomanagement

Der internationale Grundschutzstandard (Code of Practice for Information Security Management) ISO/IEC 27002: 2005 drückt in seiner Einleitung diese Positionierung von Grundschutz, Sicherheit und Risikomanagement wie folgt aus [Isoc05]:

„It should be noted that although all controls in this document are important and should be considered, the relevance of any control should be determined in the light of the specific risks an organization is facing. Hence, although the above approach is considered a good starting point, it does not replace selection of controls based on a risk management.“

6.7**Zusammenfassung**

Die Risiko-Zusammenhänge von IT-Risiken können vorteilhaft an einem Modell dargestellt werden: Die Bedrohungen wirken sich über Schwachstellen an Objekten (Schutzobjekten) als Schäden aus. Die Risiken sind die mit den Eintrittswahrscheinlichkeiten (Häufigkeiten) gewichteten Folgen der Abweichungen von den System-Zielen. Die primären System-Ziele sind „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“. Weitere System-Ziele wie Verbindlichkeit, Zuverlässigkeit und Effektivität können definiert werden. Schwachstellen sind die Stellen mit ungenügenden Massnahmen. Der Fokus der Informationssicherheit ist weiter gespannt als jener der IT-Sicherheit, indem sich die Informationssicherheit nicht auf die Informations-Technologien beschränkt, welche ja lediglich die „Gefässe“ für die Informationen darstellen, sondern sie bezieht sich auch auf Informationen in nicht-technologischer Form (z.B. Notizen auf Papier). Im weiteren Verlauf des Buches wird deshalb der Begriff der „**Informations-**

sicherheit“ verwendet und dabei die „IT-Sicherheit“ eingeschlossen. Die Risiken hinsichtlich der Informationssicherheit bringen die Abweichungen von den Systemzielen „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ an den Informations-Objekten zum Ausdruck. Hingegen betreffen die IT-Risiken nicht alleine die Risiken über „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ in der IT, sondern auch weitere Risiken, z.B. hinsichtlich Compliance oder Effektivität der IT-Prozesse und beziehen sich so auch auf nicht zur Informationssicherheit gehörende Unternehmensrisiken wie der IT-Ressourcen-Beschaffung und der IT-Nutzung. Aus Sicht des Risikomanagements können diese beiden Bereiche in ein gemeinsames Risikomanagement der „Informations-Risiken“ integriert werden. Wenn also im weiteren Verlauf dieses Buches von **„Informations-Risiken“** gesprochen wird, dann betrifft dies sowohl die „Informationssicherheits-Risiken“ als auch die „IT-Risiken“.

Bei normalen Verhältnissen vermögen Grundschutzmassnahmen eine gute Sicherheit zu gewährleisten. Das IT-Risikomanagement wird aber dort wichtig, wo neue und spezifische Risiken angemessene Massnahmen notwendig machen und wo die Kosten aufgrund der Risiken und notwendigen Massnahmen gerechtfertigt werden müssen. In solchen Fällen und dort, wo IT-Risiken zu Geschäftsrisiken führen, wird ein IT-Risikomanagement erforderlich.

6.8

Kontrollfragen und Aufgaben

1. Wie hoch ist das Risiko, wenn keine Schwachstelle vorhanden ist? (Zur Veranschaulichung dient das Risiko-Modell Abbildung 6.1).
2. Wie gehen die Komponenten des Modells in die Risiko-Formel ein? (Lösungshilfe s. Abbildung 10.10)
 - a) Welche Komponenten ergeben auf welche Art das Schadensausmass?
 - b) Welche Komponente ergibt auf welche Art die Eintrittswahrscheinlichkeit?
3. Nennen Sie Gründe, die ein Informations-Risikomanagement notwendig machen.
4. Nennen Sie die primären „System-Ziele“ respektive „Informationskriterien“, die im Rahmen des Managements von „Informations-Risiken“ behandelt werden.

7

Informationssicherheits- und IT-Governance

Führungsaspekte

Zum Informations-Risikomanagement gehören an vorderster Stelle die Führungsaspekte, die in der Governance, der Aufbauorganisation und den Führungsinstrumenten zum Ausdruck kommen.

Organisatorische Positionierung des IT- Risikomanage- ments

Im Teil B dieses Buches haben wir bereits die Anforderungen eines Unternehmens-Risikomanagements aus der Sicht der Corporate-Governance behandelt. Bevor wir uns nun den Inhalten, Methoden und Verfahren des Informations-Risikomanagements widmen, halten wir fest, wo das für ein Unternehmen immer wichtiger werdende Informations-Risikomanagement im Verhältnis zur Disziplin „Informationssicherheit“ zu positionieren ist.

Weiter behandeln wir die für ein Informations-Risikomanagement wesentlichen Aspekte der IT-Governance und der Informationssicherheits-Governance.

7.1

Management von Informations- und IT-Sicherheit

Risiko als Mass der Unsicherheit

Aus der Sicht der „Informations- und IT-Sicherheit“ gilt es festzuhalten, dass hundertprozentige Sicherheit nicht möglich ist. Um über die Höhe der Sicherheit überhaupt eine Aussage machen zu können, kommt das Risiko als Mass für die „Unsicherheit“ zur Anwendung. Aussagen über das Mass der nicht erreichten Sicherheit machen zu können, wird umso wichtiger, wenn es darum geht, die Kosten von Massnahmen gegen ihren Nutzen, sprich Risiko-Verminderung, abzuwägen.

Begründung des Nutzens für Sicherheits- Massnahmen

Werden Budgets für Sicherheitsmassnahmen bei der Geschäftsleitung eines Unternehmens beantragt, dann sind die Massnahmenkosten vermehrt mit dem zu erzielenden Nutzen zu begründen. Bei der Nutzen-Argumentation genügt meist eine Erläuterung der vorhandenen Bedrohungen nicht, sondern es müssen anhand von Szenarien die eingeschätzten und nach unternehmensspezifischen Kriterien bewerteten Risiken aufgezeigt werden können. Der Management-Prozess für die Informations- und IT-Sicherheit im Unternehmen wird damit zum Risikomanagement-Prozess, wie wir ihn im Kapitel 3 in seiner allgemeinen Form bereits kennen gelernt haben. In diesem Prozess werden die Entscheide, ob

und welche Art von Sicherheitsmassnahmen eingesetzt werden, erst aufgrund der Ergebnisse aus der vorgelagerten Risiko-Analyse und Risiko-Bewertung gefällt.

*Risikosituationen
angemessen
bewältigen*

In der Realität hat also die Disziplin „Informationssicherheit“ nicht die Aufgabe, „Sicherheit per se“ zu erzeugen, sondern die zum Teil wechselnden Risikosituationen im Zusammenhang mit Informationen in einem ständigen Prozess festzustellen und den Umständen entsprechend angemessen zu bewältigen.

Aus den strategischen Optionen „Risiken verhindern“, „- reduzieren“, „- transferieren“ oder „- selbst tragen“ wird klar, dass das IT-Risikomanagement, wie auch jedes andere Risikomanagement in einem Unternehmen, nicht die alleinige Aufgabe einer Fachabteilung sein kann, sondern eine strategische Aufgabe des Unternehmens ist.

*Gute Corporate
Governance und
Management-
Praxis*

Informations-Risikomanagement ist somit ein integraler Teil guter Corporate Governance und Management-Praxis und leitet sich von den Wertvorstellungen, der Politik, den Strategien und Zielen des Unternehmens ab. Doch kann die Frage über das notwendige Mass an Sicherheit letztlich nur über das eingeschätzte und im Kontext der Unternehmensobjekte (Assets) bewertete Risiko beantwortet werden.

Die Leistung der „Informations- und IT-Sicherheit“ äussert sich daher vor allem in einem an den Geschäfts-Strategien und -Zielen ausgerichteten Informations-Risikomanagement, welches die Risiken und Massnahmenkosten im Geschäftskontext optimiert.

7.1.2

IT-Governance versus Informationssicherheits-Governance

Die ISO differenziert mit zwei verschiedenen Standards zwischen IT-Governance (ISO/IEC 38500) und Information Security Governance (ISO/IEC DIS 27014). Die beiden sich teilweise überschneidenden Governance-Bereiche, in denen jeweils das zugehörige Risikomanagement anfällt, werden im Standard ISO/IEC DIS 27014 [Isoh11] gemäss der nachfolgenden Abbildung 7.1 veranschaulicht.

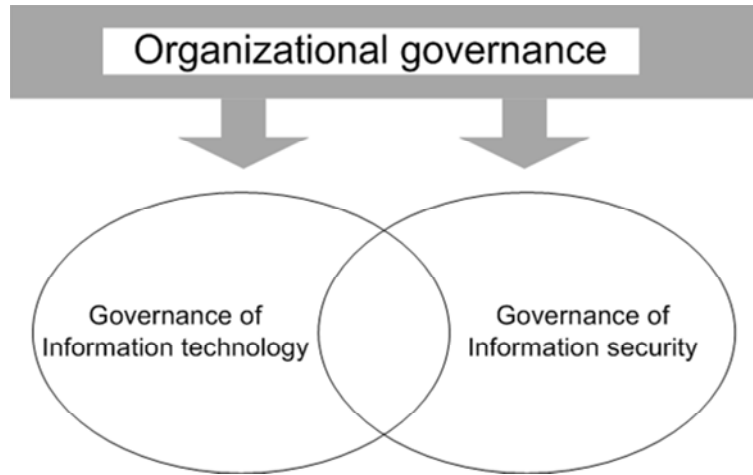


Abbildung 7.1 Zusammenhang zwischen IT-Governance und Information Security Governance

Während sich die „IT-Governance“ vor allem auf die Umsetzung der geschäftlichen Anforderungen durch die Informationstechnologie bezieht, nimmt die „Informationssicherheits-Governance“ Bezug auf die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen, die sowohl in „Gefäßen“ der Informationstechnologie (IT), als auch in nichttechnologischen „Erscheinungsformen“ existieren (z.B. Handnotizen auf Papier). Im Zuge eines „Integrierten Informations- und IT-Risikomanagements“ werden in diesem Buch beide Governance-Bereiche in ihren wesentlichen Aspekten beleuchtet, zumal die Governance-Objekte zum Teil zwar verschieden sind, aber die Methoden in beiden Bereichen einheitlich angewendet werden können.

Die IT-Governance wird im Standard ISO/IEC 38500:2008 [Isog08] wie folgt definiert:

Governance der IT ist das System, mit dem die gegenwärtige und zukünftige Verwendung der IT gesteuert und überwacht wird.

Sowohl der Standard ISO/IEC 38500:2008 für die „Governance der IT“ als auch der Standard-Entwurf ISO/IEC DIS 27014 [Isoh11] für die „Governance der Informations-Sicherheit“ beinhalten sechs ähnliche Grundsätze sowie ein ähnliches Vorgehensmodell.

Die sechs Grundsätze beziehen sich im Wesentlichen auf:

- die Verantwortlichkeiten für Aktivitäten auf sämtlichen organisatorischen Ebenen und in allen Bereichen des Unternehmens;
- die Investitionsstrategien basierend auf Geschäftsstrategien;
- die risikobasierten Entscheidungen, u.a. für den Ressourceneinsatz und die Beschaffungen;
- die Leistungskontrolle im Hinblick auf die Erfüllung der Geschäftsanforderungen;
- die Konformität mit internen und externen Anforderungen;
- die Unternehmenskultur und das personelle Verhalten in den Unternehmensprozessen.

Kurz zusammengefasst behandelt der modellhafte Prozess der Governance die für das „Steuern“, „Beurteilen“ und „Überwachen“ des Managements der IT resp. der Informationssicherheit notwendigen Aktivitäten. Diese Aktivitäten sollen der Wertschöpfung unter Berücksichtigung der Geschäftsanforderungen im Interesse der Anspruchsgruppen dienen.

7.1.3

IT-Governance nach ITGI der ISACA

Das IT Governance Institut* der ISACA widmet sich der IT-Governance, indem es Anleitungen, Frameworks und Berichte erstellt sowie Befragungen zum aktuellen Stand der IT-Governance durchführt.

* Das ITGI (IT Governance Institut) wurde 1998 durch die ISACA (Information Systems Audit and Control Association) als Forschungseinrichtung auf den Gebieten der Informationsrevision und des Informationsmanagements gegründet.

Das IT Governance Institut definiert IT-Governance wie folgt ([Itgb03], S. 10):

Definition IT-Governance

IT-Governance ist die Verantwortlichkeit des **Board of Directors**^{*} und des **Executive Management**[†]. Sie ist integraler Bestandteil der Corporate/Enterprise-Governance und besteht aus Führung, organisatorischen Strukturen und Prozessen, welche sicherstellen, dass die IT des Unternehmens die Unternehmens-Strategien und -Ziele aufrechterhält und ausbaut.

Dabei sind folgende Herausforderungen zu bewältigen:

- Ausrichtung der IT-Strategie nach der Geschäftsstrategie
- Kaskadierung der Strategie und Ziele „top-down“ in das Unternehmen
- Schaffung von Organisations-Strukturen, welche die Umsetzung der Strategien und Ziele erleichtern
- Durchsetzung eines IT Control Frameworks
- Messung der IT-Leistung

Das „IT Governance Institut“ hat für Verwaltungsräte und Geschäftsleitungen zusätzlich eine Anleitung darüber herausgegeben, wie die **„Information Security Governance“** zu verstehen ist und umgesetzt werden soll [Isac01], [Isac06][‡].

^{*} Das „Board of Directors“ hat in anglo-amerikanischen Ländern die Oberleitung und Überwachungsfunktion des Unternehmens inne. In Deutschland fällt diese Rolle dem „Aufsichtsrat“ und in der Schweiz dem „Verwaltungsrat“ zu (vgl. [Böck04], S. 1759).

[†] Das „Executive Management“ nimmt die „Führungsfunktion“ im Unternehmen ein. In Deutschland wird diese Funktion durch den „Vorstand“ und in der Schweiz durch die „Geschäftsleitung“ wahrgenommen (vgl. [Böck04], S. 1759).

[‡] Nach der ersten Ausgabe von 2001 liegt inzwischen eine zweite Ausgabe aus dem Jahre 2006 vor. Wenngleich die zweite Ausgabe verstärkt auf die Wertegenerierung durch effektive Investitionen der IT eingeht, behält die erste Ausgabe in vielen Punkten nach wie vor Gültigkeit.

7.1.4

Informationssicherheits-Governance nach ITGI der ISACA*Informationssicherheit-Governance*

Gemäss der Anleitung des „IT Governance Instituts“ über „Information Security Governance“ ist die Information Security Governance ein Subset der „Enterprise Governance“. Das Information Security Framework soll beinhalten (s. Abbildung 7.2):

- ☐ Eine Informationssicherheit-Risikomanagement-Methode;
- ☐ Ein umfassende Sicherheits-Strategie, die explizit mit den Geschäfts- und den IT-Zielen verbunden ist;
- ☐ Eine effektive Sicherheits-Organisationsstruktur;
- ☐ Eine Sicherheits-Strategie, die sich auf zu liefernde und schützende Informationswerte bezieht;
- ☐ Sicherheits-Policies, die alle Aspekte der Strategie, der Überwachung und der Regulierung adressieren;
- ☐ Eine kompletter Satz an Sicherheitsstandards für jede Policy, welche die Compliance von Verfahrensregeln und Richtlinien zu den Policies garantieren;
- ☐ Ein institutionalisierter Monitoring-Prozess, welcher die Compliance sicherstellt und Rückschlüsse auf die Wirksamkeit der Risiko-Überwachung und Bewältigung erlaubt;
- ☐ Ein Prozess, mit dem die kontinuierliche Beurteilung und Anpassung der Sicherheits-Policies, -Standards, -Verfahren und -Risiken gewährleistet wird.

Abbildung 7.2: Information Security Framework nach ITGI [Isac06]

Dabei sollten „Board of Directors“ und „Executive Management“ hinsichtlich der Informationssicherheit

- verstehen, warum Informations-Sicherheits-Bedürfnisse Bestandteil der Governance sind;
- sicherstellen, dass sich Informationssicherheit in das Governance Framework einfügt;
- bewirken, dass auf den Ebene „Board of Directors“ und „Executive Management“ über Informationssicherheit, ihre Angemessenheit und Effektivität, Bericht erstattet und entsprechende Direktiven gegeben werden.

Die Sicherheitsanforderungen und -lösungen sollen durch die Unternehmens-Anforderungen und die Unternehmens-Strategie getrieben und auf das Risikoprofil des Unternehmens abgestimmt werden. Somit unterteilt das IT Governance Institut die „IT Governance“ und die „Information Security Governance“ in die folgenden fünf grundlegenden Bereiche von „Ergebnissen“ (s. Abbildung 7.3).

☐	Strategische Ausrichtung • Gewährleistung von Transparenz und Verständnis von Kosten, Nutzen, Strategien, Policies und Service Levels der IT-Sicherheit • Entwicklung einer gemeinsamen und umfassenden Anzahl von IT-Sicherheits-Policies (Weisungen, Richtlinien, Ausführungsbestimmungen usw.) • Kommunikation der IT-Strategie, der Policies und des Überwachungs-Frameworks. • Durchsetzung der IT-Sicherheits-Policies • Definition von Sicherheitsereignissen in einer Sprache, wie sie sich auf das Geschäft auswirken • Schaffung von Klarheit über den Geschäfts-Impact der Risiken hinsichtlich IT-Zielen und Ressourcen. • Einrichtung eines IT-Kontinuitäts-Plans, der die Geschäftskontinuitäts-Pläne unterstützt
☐	Risikomanagement • Berücksichtigung und Schutz aller IT-Werte (Assets) • Ermittlung und Reduktion der Wahrscheinlichkeit und des Impacts der IT-Sicherheitsrisiken • Regelmässige Durchführung von Risiko-Assessments mit dem verantwortlichen Management und mit Schlüsselpersonen • Zugriffs-Erlaubnis auf kritische und sensitive Daten nur für berechtigte Benutzer • Gewährleistung, dass kritische und vertrauliche Informationen vor unbefugtem Zugriff geschützt sind • Identifikation, Überwachung und Berichterstattung über Sicherheits-Schwachstellen und Sicherheitsereignisse • Entwicklung eines IT-Kontinuitäts-Plans, der umgesetzt, getestet und unterhalten wird.
☐	Ressourcen-Management • Unterhalt der Unversehrtheit der Information und der Verarbeitungs-Infrastruktur • Berücksichtigung und Schutz aller IT-Werte (Assets) • Gewährleistung, dass IT-Services und –Infrastrukturen widerstandsfähig sind und sich von Fehlern, Attacken oder Katastrophen wieder • Gewährleistung von richtiger Benutzung und Leistung der Anwendungen und Technologie-Lösungen.
☐	Leistungs-Messung • Messung, Überwachung und Berichterstattung über Informationssicherheits-Prozesse sollen die Erreichung der Unternehmensziele gewährleisten. • Beispiele von Messwerten sind: Anzahl Ereignisse von öffentlichen Reputationsschäden; Anzahl von Systemen, die nicht den Sicherheitsanforderungen entsprechen.
☐	Wertbeitrag (Value Delivery) • Gewährleistung, dass den automatisierten Geschäftstransaktionen und dem Informationsaustausch vertraut werden kann • Gewährleistung, dass die IT Services entsprechend der Anforderungen verfügbar sind • Minimierung der Wahrscheinlichkeit einer Unterbrechung von IT Services • Minimierung der Auswirkungen von Sicherheits-Schwachstellen und –Ereignissen • Gewährleistung eines minimale Geschäfts-Impact im Falle von Unterbrechungen oder Veränderungen bei den IT Services • Einrichtung eines kostenwirksamen Aktion-Plans für die kritischen IT-Risiken.

Abbildung 7.3: Ergebnisse der Information Security Governance ([Isac06], S. 29-31)

*Empfehlungen
IT-Governance
Institut*

Zur erfolgreichen Umsetzung der Informationssicherheit-Governance werden in der Anleitung des „IT Governance Instituts“ eine Reihe von Empfehlungen abgegeben. Davon sind die Empfehlungen für „Best Practices“ des „Board of Directors“ und des „Executive Management“ nachfolgend aufgeführt (Abbildungen 7.4 und 7.5).

Best Practices auf der Ebene „Board of Directors“:

- ☐ Einrichtung von „Ownership“ für Sicherheit und Kontinuität im Unternehmen.
- ☐ Einrichtung eines „Audit-Komitees“, welches seine Rolle betreffend Informationssicherheit und die Zusammenarbeit mit den Revisoren (Auditors) und dem Management klar versteht.
- ☐ Sicherstellung, dass externe und interne Revisoren (Auditors) mit dem Audit-Komitee und dem Management übereinstimmen, wie die Informationssicherheit in den Audits behandelt werden soll.
- ☐ Fordern, dass der Leiter IT-Sicherheit die Anliegen und den Fortschritt an das Audit-Komitee berichtet.
- ☐ Entwicklung von Krisen-Management-Praktiken, in welche das „Executive Management“ und das „Board of Directors“ von einer vereinbarten Eskalationsstufe an einbezogen werden.

Abbildung 7.4: Informationssicherheit-Governance auf der Ebene „Board of Directors“ ([Isac01], S. 18)

Die Anleitung enthält eine Anzahl weiterer wertvoller Hinweise zur Positionierung und Umsetzung von Informationssicherheit.

*Information
Security
Maturity Model*

So wird darin das mit dem CobiT-Framework eingeführte „Information Security Maturity Model“ empfohlen. Nach diesem Maturity-Modell können die Unternehmen in Form einer Selbst-Beurteilung den Grad ihres erreichten Informationssicherheitsstandes in einer Skala von fünf Stufen einreihen (Abbildung 7.6).

Best Practices auf der Ebene „Executive Management“:

- ☐ Einrichtung einer Sicherheits-Funktion, welche das Management bei der Entwicklung von Policies und das Unternehmen bei deren Umsetzung unterstützt.
- ☐ Erstellung einer messbaren und transparenten Sicherheits-Strategie, basierend auf Benchmarking, Maturity-Modellen, Gap-Analysen und fortlaufendem Leistungs-Reporting.
- ☐ Einrichtung eines klaren, pragmatischen Geschäfts- und Technologie-Kontinuitäts-Plans, welcher kontinuierlich getestet und up-to-date gehalten wird.
- ☐ Entwicklung von klaren Policies und detaillierten Richtlinien, unterstützt durch einen periodischen und erklärenden Kommunikations-Plan, mit dem alle Mitarbeiter erreicht werden können.
- ☐ Ständige Auswertung von „Vulnerabilities“ durch Überwachung von System-Schwachstellen (CERT), Intrusion- und Stress-Tests sowie Tests des Notfall-Plans.
- ☐ Einrichtung von robusten Geschäfts-Prozessen und Support-Infrastrukturen zur Vermeidung von Ausfällen, insbesondere aufgrund von „Single point of failures“.
- ☐ Härtung von Sicherheits-Servern und anderen kritischen Servern sowie Kommunikations-Plattformen mit entsprechend starken Sicherheits-Massnahmen.
- ☐ Einrichtung und rigorose Überwachung von Sicherheits-Grundschatz-Massnahmen (Security Baselines Controls).
- ☐ Durchführung von Sicherheits-Verständnis-Programmen und häufigen Penetration-Tests.
- ☐ Anpassung der Zugriffs-Autorisation an die Geschäftsvorgänge und die Authentifizier-Methode an das Geschäfts-Risiko.
- ☐ Einbezug der Sicherheit in die Mitarbeiter-Qualifikationen mit entsprechenden Belohnungen und Disziplinar-Massnahmen.

Abbildung 7.5: Informationssicherheits-Governance auf der Ebene „Executive Management“ ([Isac01], S. 18-19)

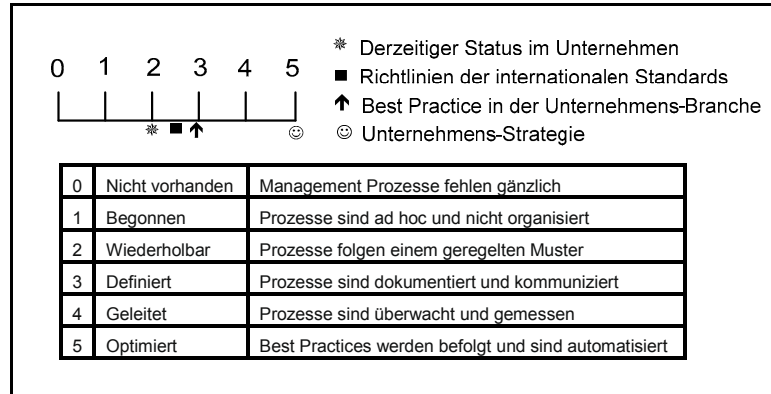


Abbildung 7.6: Informationssicherheit-Maturity-Modell

7.2

Organisatorische Funktionen für Informations-Risiken

Im Abschnitt 4.5 haben wir die wichtigen organisatorischen Funktionen im Rahmen eines Unternehmens-Risikomanagements behandelt. Für die IT-Governance fallen insbesondere dem CIO (Chief Information Officer) und dem CSO (Chief Security Officer) wichtige Rollen zu. Um dem Schutz der Informationen besonderen Nachdruck zu verleihen, ist auch oft die Funktion eines CISO (Chief Information Security Officer) anzutreffen.

Die Bedeutung des Risikomanagements für die Informationssicherheit haben wir im vorangegangenen Kapitel bereits behandelt. Ebenfalls behandelt wurden die Anforderungen an eine IT-Governance auf den Ebenen des Verwaltungsrats und der Geschäftsleitung.

In den folgenden Abschnitten behandeln wir einige organisatorischen Funktionen, die spezifisch die Informationssicherheit und damit das Informations-Risikomanagement im Unternehmen steuern.

Dies sind vor allem:

- ☐ Chief Information Officer
- ☐ Chief Information Security Officer und
- ☐ Prozess- und System-Owner bei IT-unterstützten Prozessen
- ☐ IT-Administratoren und IT-Sicherheits-Administratoren

7.2.1 Chief Information Officer (CIO)

*Verantwortlichkeit
für Information-
Technologie*

Um dem hohen Stellenwert der Informationen gerecht zu werden, setzen Unternehmen mit hohen Abhängigkeiten von Informationen (z.B. Banken, Versicherungen, Verwaltungen) einen Verantwortlichen für die Informations-Technologie (IT) auf der obersten Management-Ebene des Unternehmens ein. Diese meist dem CEO (Chief Executive Officer) des Unternehmens direkt unterstellte Führungsperson wird oft als Chief Information Officer bezeichnet. Häufig ist dieser Chief Information Officer auch Mitglied der Geschäftsleitung. Diese Führungsperson übernimmt im Auftrag des Verwaltungsrates und der Geschäftsleitung vor allem Verantwortlichkeiten über „strategische“ und „zentrale“ Fragen im Zusammenhang mit Konzeption, Aufbau, Betrieb, Nutzung und Abbau von Informations-Technologien im Unternehmen. In vielen Fällen obliegt diesem CIO auch gleichzeitig die operative Verantwortung für die Informationstechnologie im Unternehmen.

*Strategische
Belange*

Die Zuordnung der Verantwortlichkeiten zu einem CIO ist stark von der Struktur des Unternehmens abhängig. So werden in einem Unternehmen mit komplexen und wechselhaften Informations-Anforderungen dem CIO in erster Linie die strategischen IT-Belange zugeordnet.

*Operative
Aufgaben*

Hingegen werden in einem Unternehmen mit einfacheren und stabilen Informationsanforderungen dem CIO meist sowohl die strategischen als auch die operativen Aufgaben und Verantwortlichkeiten der Unternehmens-IT übertragen.

*CIO als
Katalysator*

In jedem Falle muss der CIO die Rolle eines Katalysators zwischen den Geschäfts-Anforderungen und den IT-Lieferungen des IT-Bereichs einnehmen können. In seiner strategischen Aufgabe wird er Owner der IT-Strategie-Risiken, IT-Technologie-Risiken und IT-Projektrisiken sein.

7.2.2 Chief (Information) Security Officer

*Garant der Ge-
schäftsleitung*

Die Funktion eines (unternehmensweiten) Chief Information Security Officer beruht, wie die des CIO, auf dem hohen Stellenwert der Information und der IT-Systeme in vielen Unternehmen. Zudem bedarf es auf Grund der wichtigen Informationssicherheits- und IT-Risiken und der zum Teil komplexen Risiko-Zusammenhänge einer Funktion mit der notwendigen Fachkompetenz, die für die Geschäftsleitung Garant dafür ist, dass den

	Informations-Risiken in angemessener Weise Rechnung getragen wird.
<i>Bezeichnung Chief Information Security Officer</i>	Die Bezeichnung „Chief Information Security Officer“ ist deshalb beliebt, weil sie zum einen eine deutliche Abgrenzung gegenüber anderen Sicherheitsaspekten im Unternehmen trifft (z.B. der physischen Objekt-Sicherheit) und zum anderen die Sicherheit der IT-Systeme als Voraussetzung für die Informationssicherheit in das Verantwortlichkeitsgebiet einzubeziehen vermag. Die Abgrenzung gegenüber den anderen Sicherheitsaspekten wird oft so getroffen, dass dem CISO die Informationssicherheit bezüglich Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und IT-Systeme obliegt.
<i>Policy-Erstellung, Durchsetzung und Kontrolle</i>	Seine Aufgaben werden sich auf die Strategiefindung bezüglich Informationssicherheit und Informations-Risiken im Strategie- und Risikomanagement-Prozess sowie die Sicherheits-Policy-Erstellung und deren Durchsetzung und Kontrolle im Unternehmen konzentrieren. Mit diesen Aufgaben legt der CISO, im Rahmen der Management-Prozesse, die Leitplanken für die operativen Verantwortlichkeiten betreffend Informationssicherheit fest.
<i>Bewilligungs- und Anordnungsbefugnisse</i>	In seiner Kontroll- und Überwachungsfunktion können ihm durch den Verwaltungsrat oder die Geschäftsleitung auch Bewilligungs- und Anordnungsbefugnisse für besondere Prozess-Schritte oder Situationen (z.B. während der System-Entwicklung oder bei akuten Gefahren) zugeteilt sein. Aus der Führungs-Pyramide der Informationssicherheit (s. Abbildung 8.1) sind weitere Führungs-Verantwortlichkeiten ersichtlich, wie das Erlassen von Sicherheitsstandards, das Definieren einer Sicherheits-Architektur oder die Abnahme von Sicherheitskonzepten.
<i>Steuerung und Koordination IT- RM-Prozesse</i>	In das Aufgabengebiet des CISO gehört auch die Steuerung und Koordination der Informations-RM-Prozesse (s. Abschnitt 12.1.3). Damit fällt ihm die Aufgabe eines „Prozess-Owners“ des Informations-Risikomanagement-Prozesses zu. Natürlich ist er damit nicht gleichzeitig Owner der Informations-Risiken oder der Informations- und IT-Prozesse selbst.
<i>Verantwortlichkeiten CISO</i>	Dem CISO sollte neben den Verantwortlichkeiten über den Informations-RM-Prozess, über die Sicherheits-Anweisungen und deren Durchsetzungen und Kontrollen, nicht gleichzeitig die Verantwortlichkeiten der Sicherheitsausführung und -umsetzung zugeordnet werden; dies aus Gründen der Gewaltentrennung, wie es im Abschnitt 7.2.5 näher dargelegt wird.

7.2.3

Business-Owner, IT-Owner und IT-Administratoren

Bei der Behandlung des Risikomanagements aus unternehmenssicht haben wir bereits den Risk-Owner als einen der Hauptakteure im unternehmensweiten Risikomanagement angeführt.

Ownership-Prinzip

Das Ownership-Prinzip als Führungsfunktion hat sich auch bei den Informations-Risiken bewährt. So weist beispielsweise das „IT Governance Institute“ in seinen Anleitungen über die „IT Security Governance“ auf die Einrichtung von „Ownership“ für Sicherheit und Kontinuität im Unternehmen hin.

Owner für Informations-Risiken

Als Owner für Informations-Risiken eignen sich Führungskräfte in der Linie, welche die Verantwortung über eine bestimmte Prozesskette oder ein IT-System (IT-Infrastruktur oder IT-Applikation) tragen.

Geschäftsprozess-Owner / IT-Prozess-Owner

Dabei kommen einerseits **Owner von Geschäftsprozessen** in Frage, welche mit den von den Geschäftsprozessen benötigten Informationen und den Konsequenzen allfälliger Informations-Risiken vertraut sind. Andererseits braucht es **Owner für die IT-Prozesse, IT-Systeme und IT-Infrastrukturen**. Diese sog. „IT-Owner“ tragen für die ihnen zugeteilten IT-Prozesse, IT-Systeme oder IT-Infrastrukturen, zusätzlich zu Ihrer Linienverantwortung, die Verantwortung, dass sie die Risiken dieser Bereiche kennen und angemessen behandeln müssen.

Neben solchen Ownern mit definierten Führungs- und Prozessverantwortlichkeiten (z.B. Risiko-, Kosten- und Leistungsverantwortung) sind für den gesicherten Betrieb der IT-Systeme noch sogenannte Administratoren (oder Sicherheits-Administratoren) im Einsatz. Diese Administratoren nehmen Verwaltungsaufgaben wahr, wie die Erfassung und Verwaltung von Zugriffsrechten oder die Registrierung, Auswertung und Weiterleitung von Sicherheits-Ereignissen.

Administratoren erfüllen mit Policies vorgegebene Fachaufgaben

Innerhalb des Informations-Risikomanagement-Prozesses haben sie meist keine Führungsaufgaben, sondern erfüllen die mit Policies vorgegebenen Fachaufgaben. Sowohl Owner als auch Administratoren führen ihre Aufgaben zur Informationssicherheit und zum Informations-Risikomanagement nicht in jedem Falle vollamtlich aus. Gerade in kleineren Unternehmen können diese Funktionen auch in Personalunion mit anderen Funktionen ausgeübt werden.

7.2.4**Information Security Steering Committee**

Die Informationssicherheit berührt sämtliche Aspekte eines Unternehmens. Demnach ist es wichtig, sowohl das Assessment möglicher Risiken mit ihren Ursachen als auch die umzusetzenden Massnahmen breit mit den entsprechenden Kenntnisträgern und den Verantwortlichen im Unternehmen abzustützen.

Das „IT Governance Institut“ schlägt ein „Steering Committee“ unter Beteiligung des CEO, des CFO, des CIO des CSO und CISO sowie Vertreter des Personaldienstes (HR) und des internen Audits vor ([Isac06], S. 22).

Ein solches Steering Committee soll hauptsächlich die Kommunikation der Management-Absichten und die Ausrichtung des Sicherheits-Programmes an den Unternehmenszielen gewährleisten. Auch soll das Bewusstsein im Unternehmen hinsichtlich einer guten Risiko- und Sicherheitskultur durch das Komitee und seine Mitglieder gefördert werden.

7.2.5**Checks and Balances durch Organisations-Struktur***Gewaltentrennung*

Wie aus den obigen Rollenbeschreibungen erkennbar ist, sollten insbesondere die Verantwortlichkeiten für den Risikomanagementprozess und die Risikoverantwortlichkeiten in den Geschäfts- und IT-Prozessen im Sinne einer „Gewaltentrennung“ personell getrennt sein. So ist beispielsweise von der Unterstellung eines CISO mit dem oben skizzierten Aufgaben- / Verantwortlichkeitsprofil unter die Führungs-Linien der IT-Organisation oder eines Geschäftsfeldes abzuraten. In einer solchen Unterstellung würde er die im Interesse des Gesamt-Unternehmens notwendigen Kontrollen und aufwändigen Sicherheitsmassnahmen nur schwerlich durchsetzen können.

Principal/Agent-Situation

Aufgrund der Informations-Asymmetrie zwischen dem für die Unternehmens-Risiken verantwortlichen Verwaltungsrat und den für eher kurzfristige Kosteneinsparungen belohnten Linien-Manager eines Geschäftsfeldes oder IT-Prozesses wird es zwangsläufig zu einer „Principal/Agent“-Situation kommen. Dabei werden sich die Linien-Manager in der Regel für die kurzfristigen Einsparungen durch Nichtrealisierung nachhaltiger Sicherheits-Massnahmen entscheiden (vgl. [Bitr04], S. 54); dies auf dem Hintergrund, dass sich grössere IT-Risiken meist erst in der langen Sicht materialisieren.

Organisatorische Einordnung CISO

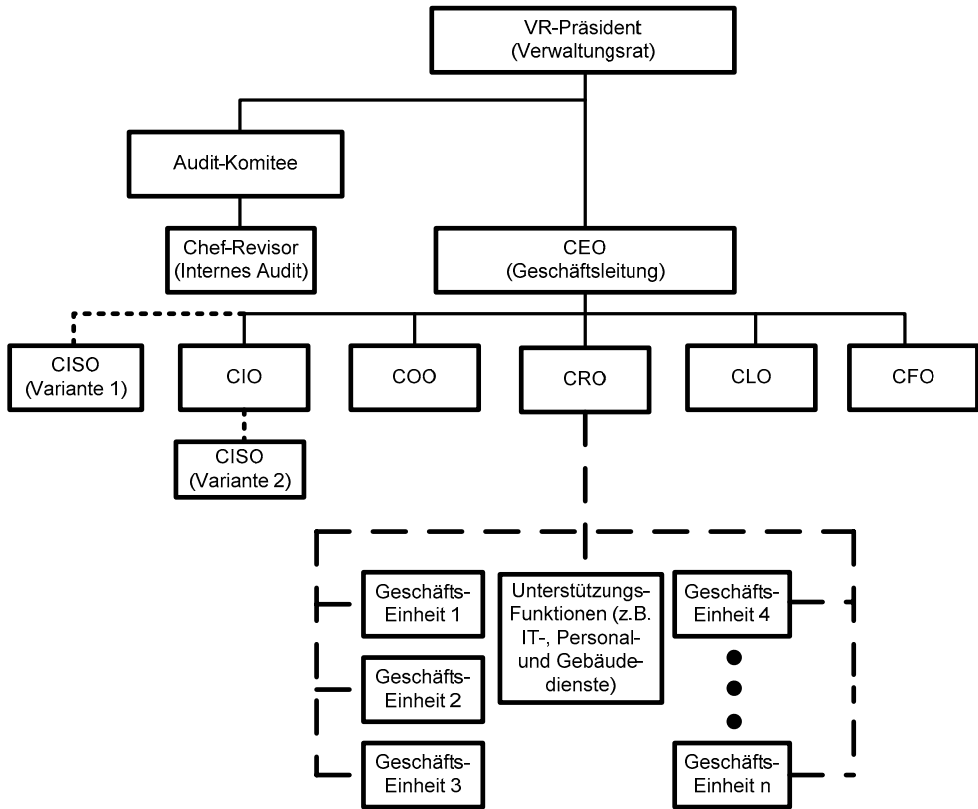
Die organisatorische Einordnung sollte deshalb dem CISO den direkten Berichtsweg zu den obersten Kontroll- und Führungsin-

stanzen gewährleisten. Mit der notwendigen Bewegungsfreiheit und Unbefangenheit wird er somit im Auftrag der obersten Kontroll- und Leitungsinstanzen die Informationssicherheit im Unternehmen durchsetzen und kontrollieren können (vgl. [Delt03], S. 10). Bei Berücksichtigung der Gewaltentrennung sind Unterstellungen des CISO unter den Verwaltungsrat, den CEO oder den CIO mögliche Varianten*.

Chief Risk Officer Die übergeordnete Steuerung, Koordination und Kontrolle des Gesamt-Risikomanagement-Prozesses erfolgt durch den „Chief Risk Officer“. Die Umsetzung des Risikomanagements liegt bei den Risiko-Eignern (Risk Owner) der operativen Geschäfts- und Unterstützungsfunktionen.

Eine Organisations-Struktur mit den bereits unter Abschnitt 4.4 erwähnten Funktionen und mit zwei gebräuchlichen Varianten der Einordnung des CISO ist in der Abbildung 7.7 veranschaulicht. In dieser Abbildung sind zudem die wesentlichen organisatorischen Funktionen gezeigt, die in ihren jeweiligen Führungs- und Fachgebieten das Risikomanagement steuern und kontrollieren.

* Die Unterstellung des CISO unter den CIO ist durch Regulatoren oder Gesetzgebungen nur bedingt erlaubt, z.B. in Deutschland, wenn der Datenschutz durch eine nicht dem CIO unterstellte Person gewährleistet wird.



Legende:

VR: Verwaltungsrat
 CEO: Chief Executive Officer
 CRO: Chief Risk Officer
 CISO: Chief Information Security Officer
 CIO: Chief Information Officer
 COO: Chief Operation Officer
 CLO: Chief Legal Officer
 CFO: Chief Financial Officer
 Audit-Komitee
 Chef-Revisor und Internes Audit

Abbildung 7.7: Risikomanagement-Funktionen in einem grossen Unternehmen

7.3

Zusammenfassung

Die Leistung der „Informations- und IT-Sicherheit“ äussert sich vor allem in einem an den Geschäfts-Strategien und -Zielen ausgerichteten Informations-Risikomanagement, welches die Risiken und Massnahmenkosten im Geschäftskontext optimiert.

Die ISO differenziert mit zwei verschiedenen Standards zwischen IT-Governance und Information Security Governance. Zu den beiden sich teilweise überschneidenden Governance-Bereichen gehört jeweils ein entsprechendes Risikomanagement.

Während sich die **„IT-Governance“** vor allem auf die Umsetzung der geschäftlichen Anforderungen durch die Informationstechnologie bezieht, nimmt die **„Informationssicherheit-Governance“** Bezug auf die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen, die sowohl in „Gefässen“ der Informationstechnologie (IT), als auch in nichttechnologischen „Erscheinungsformen“ existieren (z.B. Handnotizen auf Papier).

Das IT Governance Institut definiert IT-Governance als Verantwortlichkeit des Verwaltungsrats und der Geschäftsleitung und somit als integralen Bestandteil der Corporate-Governance. Aufgrund der Wichtigkeit der Informationssicherheit hat das IT Governance Institut auch eine Anleitung für „Informationssicherheit-Governance“ herausgegeben. Darin kommen „Best Practices“ hinsichtlich Informationssicherheit für die Ebene des Verwaltungsrats und für die Ebene der Geschäftsleitung zum Ausdruck. Z.B. „Die Sicherheitsanforderungen werden durch die Unternehmensanforderungen getrieben.“

Die Funktion des „Chief Information Officer“ übernimmt im Auftrag des Verwaltungsrates und der Geschäftsleitung wichtige Verantwortlichkeiten bei strategischen Fragen der IT sowie die für das gesamte Unternehmen zentralen IT-Fragen. Die Zuordnung seiner Verantwortlichkeiten hängen stark von der Struktur des Unternehmens ab. In vielen Fällen trägt er gleichzeitig die operative Verantwortung für die Informationstechnologie im Unternehmen.

Die Funktion des „Chief Information Security Officer“ beruht, wie die des „Chief Information Officer“, auf dem hohen Stellenwert der Informationstechnologie im Unternehmen. Mit seinen Aufgaben, vor allem bei der Strategiefindung und der Policy-Ausarbeitung für die Sicherheit der Informationen und Informationssysteme legt er die Leitplanken für die Informationssicherheit fest. Für die operationelle Durchsetzung und Kontrolle der

Informationssicherheit können ihm durch den Verwaltungsrat oder die Geschäftsleitung auch Bewilligungs- und Anordnungsbe-fugnisse für besondere Aufgaben und Situationen zugeteilt sein.

Als Owner für die Informations-Risiken eignen sich Führungs-kräfte, welche in der Linie die Verantwortung über eine be-stimmte Prozesskette oder ein IT-System (IT-Infrastruktur oder IT-Applikation) innehaben.

Neben den Ownern als Führungspersonen mit bestimmten Pro-zessverantwortlichkeiten (z.B. Kosten- und Leistungsverantwor-tung) sind für den gesicherten IT-Betrieb sogenannte Administratoren (oder Sicherheitsadministratoren) im Einsatz. Diese Administratoren nehmen Verwaltungsaufgaben wahr, wie die Erfassung und Verwaltung von Zugriffsrechten oder die Re-gistrierung, Auswertung und Weiterleitung von Sicherheits-Ereignissen.

Ein „Steering Committee“ für Informationssicherheit mit wichti-gen Mitgliedern der Unternehmensführung (z.B. CEO, CIO und CSO) soll hauptsächlich die Kommunikation der Management-Absichten und die Ausrichtung des Sicherheits-Programms an den Unternehmenszielen gewährleisten.

Bei der organisatorischen Einbindung der verschiedenen Risiko-Rollen in die Organisations-Struktur eines Unternehmens ist auf „Checks and Balances“ zu achten.

7.4

Kontrollfragen und Aufgaben

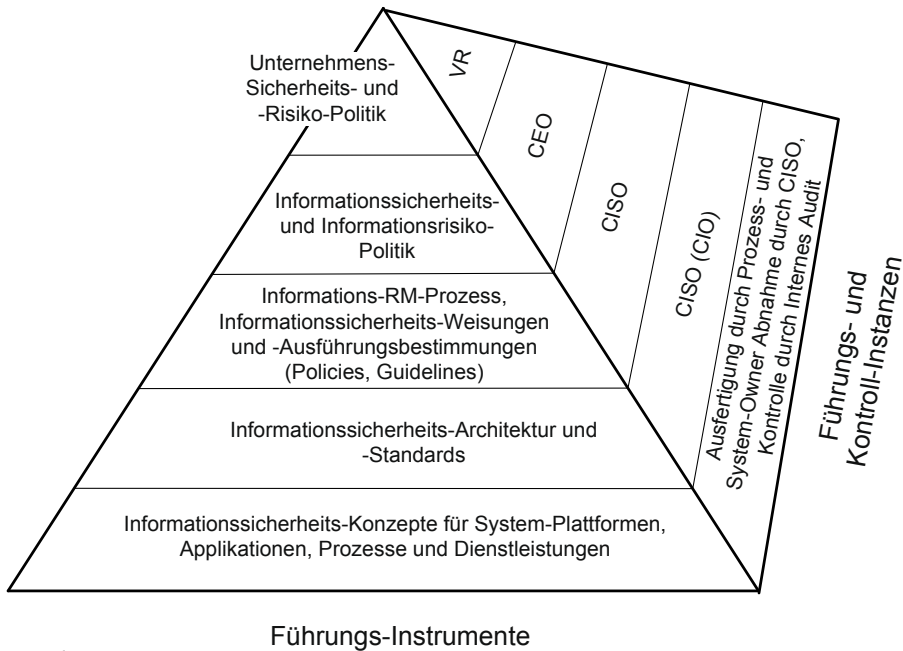
1. Wie definieren Sie IT-Governance?
2. Nennen Sie mindestens fünf Resultate, welche eine „Informa-tion Security Governance“ liefern sollte.
3. Nennen Sie mindestens je drei der Best Practices zur Infor-mation Security Governance auf der Verwaltungsrats- und auf der Geschäftsleitungs-Ebene.
4. Mit welchen organisatorischen Dispositionen können „Checks and Balances“ für die Informationssicherheit herbei-geführt werden?
5. Welche Probleme können entstehen, wenn der Chief Infor-mation Security Officer innerhalb der Linie einer Informatik-Abteilung unterstellt wird?
6. Definieren Sie den Unterschied zwischen „Information Secu-rity Governance“ und „IT Governance“.

8

Informationssicherheits-Risikomanagement in der Führungs-Pyramide

*Steuerung und Kontrolle
Informations-
Risikomanagement*

Die Steuerung des Informationssicherheits-Risikomanagements in einem Unternehmen lässt sich anhand einer Pyramide darstellen. Die Pyramide symbolisiert dabei, die von oben nach unten zunehmende Verfeinerung der zu steuernden und kontrollierenden Aspekte. Auf den einzelnen Ebenen der Pyramide sind sodann die Führungsinstrumente der jeweiligen Führungs- und Kontrollinstanzen angeordnet (Abbildung 8.1).



Legende:

VR: Verwaltungsrat
CEO: Chief Executive Officer
CISO: Chief Security Officer
CIO: Chief Information Officer

Abbildung 8.1: Führungspyramide mit Instrumenten und Führungsinstanzen

Der Output aus einer Ebene fließt top-down als Input in die nächst tiefer gelegene Ebene ein. Der Top-down-Ansatz garantiert eine den Unternehmens-Anforderungen entsprechende Standardisierung der Prozesse und Massnahmen. Selbstverständlich werden tiefer gelegene Ebenen aufgrund der aktuellen operativen Realität den Inhalt der höher gelegenen Ebenen wiederum beeinflussen.

8.1

Ebenen der Führungspyramide

In diesem Abschnitt werden die Inhalte der Führungsinstrumente für die Sicherheit auf den einzelnen Ebenen beleuchtet. Ebenfalls werden Anhaltspunkte für die Verantwortlichkeiten bezüglich Inkraftsetzung, Ausführungsverantwortung und Kontrolle der einzelnen Ebenen gegeben.

In kleineren Unternehmen können aneinander angrenzende Ebenen und deren Instrumente miteinander verschmolzen werden. In grossen Organisationen mit komplexen Führungsstrukturen sind sogar zusätzliche Ebenen mit entsprechenden Instrumenten möglich.

8.1.1

Risiko- und Sicherheits-Politik auf der Unternehmens-Ebene

Übergeordnete Sicherheits- und Risiko-Ziele

Die Risiko- und Sicherheits-Politik ist ein durch den Verwaltungsrat (Aufsichtsrat) genehmigtes Papier. Dieses gibt die für das Unternehmen gültigen übergeordneten Sicherheits- und Risiko-Ziele sowie die dazu wichtigsten Grundsätze wieder.

Risiko- und Sicherheits-Organisation

Die Risiko- und Sicherheits-Politik legt zudem in groben Zügen die Risiko- und Sicherheitsorganisation und die einzelnen Risikobereiche sowie die Abgrenzungen untereinander fest. Informationssicherheit ist in der Regel einer dieser Risikobereiche, Finanzrisiken ein anderer. Ebenfalls in der Risiko- und Sicherheits-Politik enthalten sind die Grundzüge für den integrierten unternehmensweiten Risikomanagement-Prozess.

Grundzüge RM-Prozess

Die Ziele und Grundsätze beziehen sich auf die Unternehmens-Mission und die Unternehmens-Ziele und bringen wichtige Werte und Haltungen (ggf. auch ethische Grundsätze) zu Risiken und zur Sicherheit im Unternehmen zum Ausdruck. Solche Punkte können z.B. der Schutz von Kunden-Vermögen oder das Unterhalten von Ausweich-Standorten und Katastrophen-Organisationen sein.

*Wesentliche
Risiko-Gebiete*

Die wesentlichen Risiko-Gebiete des Unternehmens sollen in dieser Risiko- und Sicherheits-Politik angesprochen sein. Diese Politik ist übergeordnet und langfristig angelegt und ist damit ein Führungsinstrument des „Normativen Managements“. Folgerichtig wird auch der Verwaltungsrat massgeblich den Inhalt bestimmen und die Politik genehmigen. Sowohl die Strategiefindung als auch die operativen Aktivitäten des Unternehmens werden sich im Rahmen dieser Risiko- und Sicherheits-Politik bewegen.

*Untergeordnete
Risiko- und
Sicherheits-
Politiken*

In grösseren Unternehmen sind für kritische Risikogebiete untergeordnete Risiko- und Sicherheits-Politiken angezeigt, welche die fachspezifischen Ziele, Grundsätze und Verantwortlichkeiten des Gebiets aufzeigen. In ein solches Gebiet fallen die Informationssicherheits-Risiken.

8.1.2

Informationssicherheits-Politik und ISMS-Politik

*Fachspezifische
Risiko- und
Sicherheits-Politik*

Für das Informationssicherheits-Risikomanagement empfiehlt es sich, eine solche fachspezifische Risiko- und Sicherheits-Politik zu erstellen. Herkömmlicherweise wird eine solche Politik als Informationssicherheits-Politik bezeichnet (vgl. [Isoc05], S. 7). Vermehrt werden jedoch darin alle Aspekte sowohl der Informationssicherheit als auch des Informationssicherheits-Risikomanagements einbezogen.

Die Rahmenbedingungen für die Informationssicherheits-Politik sind durch die übergeordnete Risiko- und Sicherheits-Politik des Unternehmens vorgegeben.

*Informationssi-
cherheits-Politik
an alle
Mitarbeiter*

Bei der Entwicklung einer Informationssicherheits-Politik sollte darauf geachtet werden, dass sie an alle Mitarbeiter gerichtet ist und deshalb verständlich und möglichst kurz gehalten werden sollte. Es sollen also nur die wichtigsten Aussagen enthalten sein. Für detaillierte Weisungs- und Ausführungsinhalte sollten, wie der nächste Abschnitt zeigt, pro Weisungs-Gebiet separate Weisungen und Ausführungsbestimmungen erstellt werden. Abbildung 8.2 zeigt beispielhaft Aufbau und Inhalte einer solchen Informationssicherheits-Politik.

Grundsätzliches:

- ☐ Geschäfte des Unternehmens und Rolle der Informationen und der IT
- ☐ Umwelt u.a. für Unternehmen wichtige Märkte und Technologien
- ☐ Hauptsächliche Bedrohungen
- ☐ Anspruchsgruppen (z.B. Kunden, Partner, Lieferanten) und deren Sicherheitsbedürfnisse
- ☐ Anforderungen gesetzlicher, regulatorischer und vertraglicher Art
- ☐ Für Informations-Sicherheit relevante Ziele und Grundsätze aus Unternehmens-Risiko-Politik
- ☐ Hinweis auf Risiko- und Sicherheitskultur, -bewusstsein, -kommunikation und Schulung
- ☐ Hinweis auf Mass der angestrebten „Unternehmens-Sicherheitsreife“ (entspr. Maturity Modell)
- ☐ Begriffsdefinition Informationen, IT-Systeme und deren Komponenten

Politik-Punkte:

- ☐ Gegenstände, Umfang und Abgrenzung der Informations-Sicherheit
 - Informationen
 - IT-Systeme, IT-Prozesse über den gesamten Lebenszyklus
 - IT-Benutzer
 - Nicht zur Informations-Sicherheit gehörende Funktionen (z.B. physische Objekt-Sicherheit)
- ☐ Sicherheits- und Risikoziele und generelle Aussagen über deren Einhaltung
 - Vertraulichkeit (Datenschutz, Bankkundengeheimnis, Geschäfts-Geheimnis)
 - Integrität
 - Verfügbarkeit
 - Allenfalls auch Authentizität, Non-Repudiation und Zuverlässigkeit
- ☐ Risiko-Management
 - Methode und Hinweise auf Prozess-Beschreibungen,
 - Bewertungs-Schemata
 - Risiko-Strategie
 - Angabe des Frameworks, nach dem Kontrollziele überprüft werden (z.B. COBIT)
- ☐ Referenzierung der Prozesse für Geschäftskontinuität und IT-Notfall-Planung
- ☐ Referenzierung der Sicherheits-Vorschriften
 - für Outsourcing
 - für Externe und Vertragspartner
- ☐ Bereitstellung der erforderlichen Mittel und Ressourcen
- ☐ Bezugnahme auf weitere Weisungen über einzelne Risiko-Bereiche

Verantwortlichkeiten und Kompetenzen:

- ☐ Leiter von Geschäftseinheiten
- ☐ CISO
- ☐ CIO
- ☐ IT-Prozess- und IT-System-Owner
- ☐ Internes Audit

Geltungsbereich:

- ☐ Z.B. ganzes Unternehmen

Inkraftsetzung:

- ☐ Datum
- ☐ Unterschrift CEO

Abbildung 8.2: Aufbau und Inhalte einer Informationssicherheits-Politik

Zur risikobasierten Behandlung der Informationssicherheit im Unternehmen hat sich seit einiger Zeit mit dem Standard ISO/IEC 27001 ein standardisiertes Managementsystem etabliert (s. Abschnitt 9.3.1). Der Rahmen eines solchen, für eine kontinuierliche Verbesserung ausgelegten Managementsystems wird mittels einer sogenannten „Informationssicherheits-Management-Politik“ (ISMS Policy) festgelegt. Dieses Politikpapier behandelt vor allem die Managementaspekte der Informationssicherheit und ist der zuvor erwähnten „Informationssicherheits-Politik“ übergeordnet.

*ISMS-Politik,
Informationssicherheits-Politik
und Geschäfts-
kontinuitäts-
Politik*

Doch können die beiden Politik-Papiere, die ISMS-Politik und die Informationssicherheits-Politik, auch in einem einzigen Dokument zusammengefasst werden. Oft ist auch die Erstellung einer Geschäftskontinuitäts-Politik angezeigt (s. Abschnitt 13.3.2). Diese Politik kann ebenfalls in die ISMS-Politik integriert werden. Ein solchermassen gestaltetes „Politik-Papier“ ist den weiter detaillierten Vorschriften (s. Abschnitt 8.1.3) übergeordnet.

8.1.3

Weisungen und Ausführungsbestimmungen

Die Zusammenhänge der Informationssicherheit und des Informationssicherheits-Risikomanagements sind oft nicht einfach zu verstehen und zu kommunizieren. Doch hängt die Sicherheit zu einem grossen Teil vom Verhalten der Mitarbeiter und den Benutzern der IT-Systeme ab. Auch bedürfen die Beschaffung, der Aufbau, der Betrieb und nicht zu vergessen die Entsorgung der IT-Systeme klarer, auf die Organisation (Unternehmen) abgestimmter Sicherheits-Vorschriften.

Weisungskonzept

Ein gut gestaltetes Weisungskonzept stösst bei Management und Mitarbeitern meist auf Befürwortung, da es klare Auskunft über wichtige Fragen im Arbeitsprozess gibt. Die mit den Weisungen zu regelnden Aspekte enthalten, ähnlich der Gesetzgebung, oft grundlegende, langfristige Festlegungen. Meist sind zusätzliche Anleitungen oder Anweisungen darüber notwendig, wie einzelne Weisungsinhalte durch die „Betroffenen“ mit den entsprechenden Einrichtungen konkret umzusetzen sind. Solche Informationen können in zusätzlichen Anweisungen oder „Ausführungsbestimmungen“ enthalten sein.

*Ausführungs-
bestimmungen*

Derartige „Ausführungsbestimmungen“ können einer Weisung als integraler Bestandteil „unterstellt“ werden. Oft werden diese Ausführungsbestimmungen auch als Standards, Verfahrensregeln oder Richtlinien bezeichnet. Häufig besteht bereits ein generelles

Weisungskonzept*, in welches die Informationssicherheits-Weisungen und Ausführungsbestimmungen integriert werden können. In Abbildung 8.3 ist ein solches Konzept für Weisungen und Ausführungsbestimmungen ansatzweise skizziert.

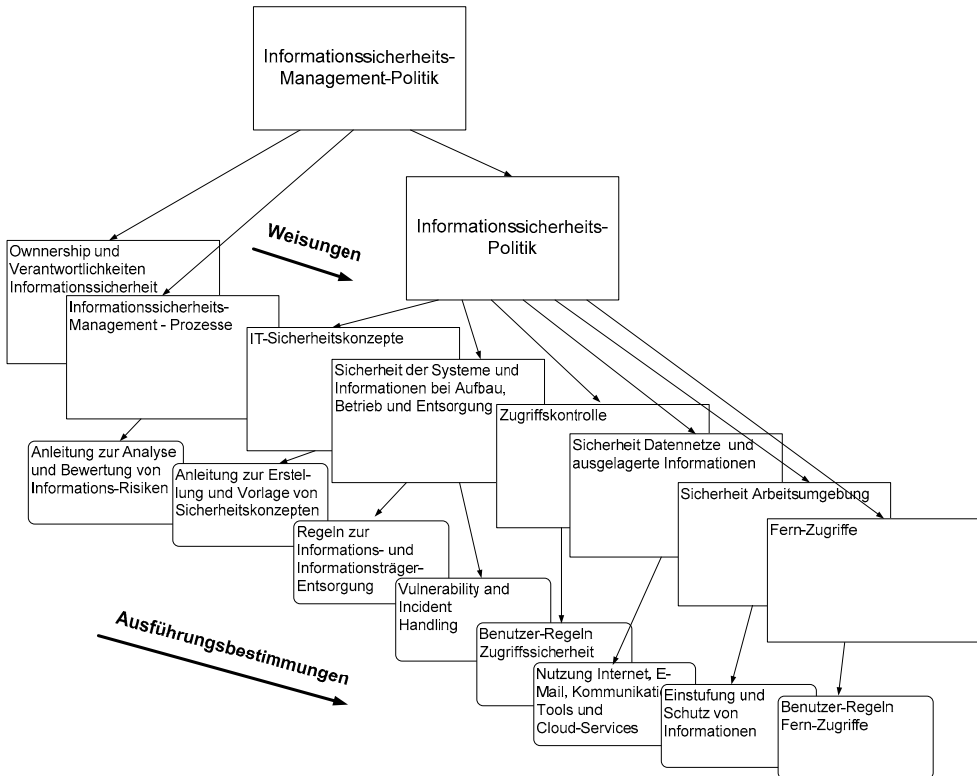


Abbildung 8.3: Konzept der Weisungen und Ausführungsbestimmungen

Die Bereiche, für die Weisungen und Ausführungsbestimmungen erstellt werden, unterscheiden sich von Unternehmen zu Unternehmen. Auch gibt es kein allgemeingültiges Konzept dafür, welche Bereiche mit engen Vorschriften und welche mit größe-

* Im angloamerikanischen Sprachgebrauch entsprechen die Weisungen den „Policies“ und die Ausführungsbestimmungen den „Standards, Procedures and Guidelines“.

ren Vorschriften zu behandeln sind. Auch der Sprach-Stil, in welchem die Weisungen kommuniziert werden, ist von der Unternehmens-Kultur, den Geschäftsprozessen und dem Stellenwert von Risikomanagement und Sicherheit im Unternehmen abhängig.

Akzeptanz der Weisungen

Die Akzeptanz der Weisungen ist sicherlich umso höher, wenn die offensichtlich wichtigen Sicherheits-Aspekte darin zum Vorschein kommen, und den aktuellen Bedrohungen in ausgewogener und konsistenter Weise begegnet werden.

Selbstverständlich kann die Segmentierung in Weisungen und Ausführungsbestimmungen auch an die Kapitel und Abschnitte des „Code of Practice“ gemäss ISO/IEC 27002 angelehnt werden, doch ist dabei ebenfalls auf Verständlichkeit und Relevanz der Inhalte in Bezug auf die adressierten Personen zu achten.

8.1.4

Informationssicherheits-Architektur und -Standards

Sicherheits-Infrastruktur

Bei mittleren bis grösseren Unternehmen empfiehlt es sich, aufgrund der für das Unternehmen typischen System-Situation, eine eigene System-Architektur, eigene Sicherheits-Standards und eine standardisierte Sicherheits-Infrastruktur aufzubauen. Eine solche standardisierte Sicherheits-Infrastruktur verhilft der Übersichtlichkeit, Konsistenz und Kontinuität der Massnahmen und nicht zuletzt der Effizienz mit niederen Kosten.

Beispiel:

Betreibt ein Unternehmen unterschiedliche Kundensysteme und müssen diese Systeme aufgrund des Vertraulichkeits-Ziels weitgehend voneinander isoliert sein, dann können mit einer entsprechenden Sicherheits-Architektur die erforderlichen Sicherheits-Dienste und -Mechanismen proaktiv vorgesehen werden (s. Abbildung 8.4).

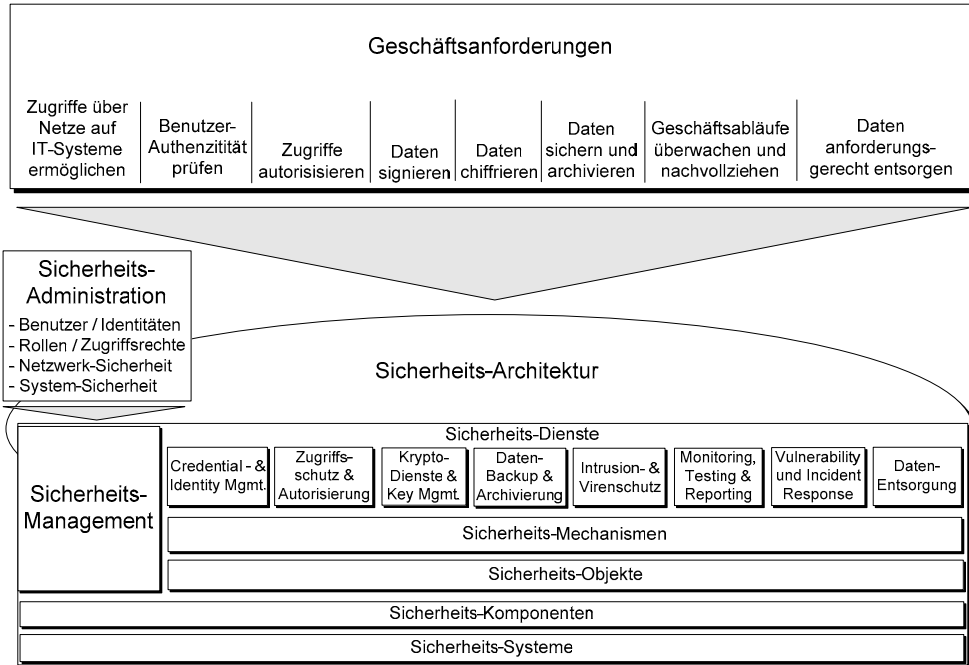


Abbildung 8.4 Aufbau einer Informationssicherheits-Architektur

Unternehmens-Sicherheits-Standards

Auch wird sich das Unternehmen auf ganz bestimmte Sicherheitssysteme beschränken und diese zu „Unternehmens-Sicherheits-Standards“ erklären. Damit können Rationalisierungspotentiale ausgeschöpft werden. Solche unternehmensspezifische Standards könnten beispielsweise bestimmte Authentisierungs-Mittel oder eine Proxy-Infrastruktur sein, mit der auf das Internet zugegriffen werden kann.

Standards in Stärkegraden und Schnittstellen-Arten

Um den spezifischen Risiken und Kosten-Beschränkungen bei einzelnen Systemen gerecht werden zu können, werden Standards für Sicherheits-Dienste in verschiedenen „Stärkegraden“ und „Schnittstellen-Arten“ konzipiert. So wird beispielsweise ein zentral eingesetzter Authentisierungs-Server folgende unterschiedliche Authentisierungs-Methoden mit unterschiedlichen Stärken unterstützen:

- „Passwort-Authentisierung“,
- Soft-Zertifikat- und
- Hard-Token-Authentisierung.

Weitere Beispiele für solche „risiko-gerechten“ Sicherheitsdienste sind:

- ☐ Unterschiedliche Sicherheits-Zonen im internen Datennetz, in welche die Applikations-Server je nach Sicherheitsbedürfnis (Vertraulichkeit, Integrität und Verfügbarkeit) platziert werden;
- ☐ Sicherheitsdienste für Kryptographie, Signatur, Zugriffskontrolle, Back-up etc. zum angemessenen Schutz von Informationen, die aufgrund der vorliegenden Vertraulichkeits- und Integritäts-Einstufungen ausgewählt und eingesetzt werden können (s. Muster einer entsprechenden Ausführungsbestimmung im Anhang A.3);
- ☐ Rollenbasiertes Zugriffs-Kontrollsystem;
- ☐ Viren-Schutz auf sämtlichen Client- und Server-Systemen mit definierten Update-Perioden;
- ☐ Anforderungsgerechtes Ressourcen-Sharing (z.B. Unterschiedliche SAN*-Kategorien oder Storage-Arrays);
- ☐ Patch-Verteilungs- und Einspiel-Mechanismen basierend auf Kritikalität;
- ☐ Werkzeuge für Incident-Management (z.B. Intrusion-Detection).
- ☐ Gesichertes Cloud-Computing-Interface

* SAN = Storage Area Network

Vom Anwendungszweck her können wir die Informationssicherheits-Architektur in einem Unternehmen pragmatisch wie folgt definieren (s. auch Abbildung 8.5):

Die Informationssicherheits-Architektur in einem Unternehmen ist ein Baukasten-System mit abgestimmten, standardisierten Bausteinen unterschiedlicher Sicherheitsdienste mit abgestuften Stärken und den Anforderungen entsprechenden Schnittstellen.

Technische Konzeption einer Sicherheits-Policy

Die Informationssicherheits-Architektur ist somit die technische Konzeption eines vorab definierten, in sich schlüssigen Informationssicherheits-Weisungskonzepts (Policy) und zielt auf eine rationelle Umsetzung der Sicherheitsmassnahmen in Form von Komponenten und Systemen ab. Die Policy gibt vor, wo und aufgrund welcher Kriterien einzelne Architektur-Bausteine eingesetzt werden. Die einzelnen Architektur-Bausteine sind für den Anwender bezüglich ihrer Leistungen und Schnittstellen-Definitionen beschrieben.

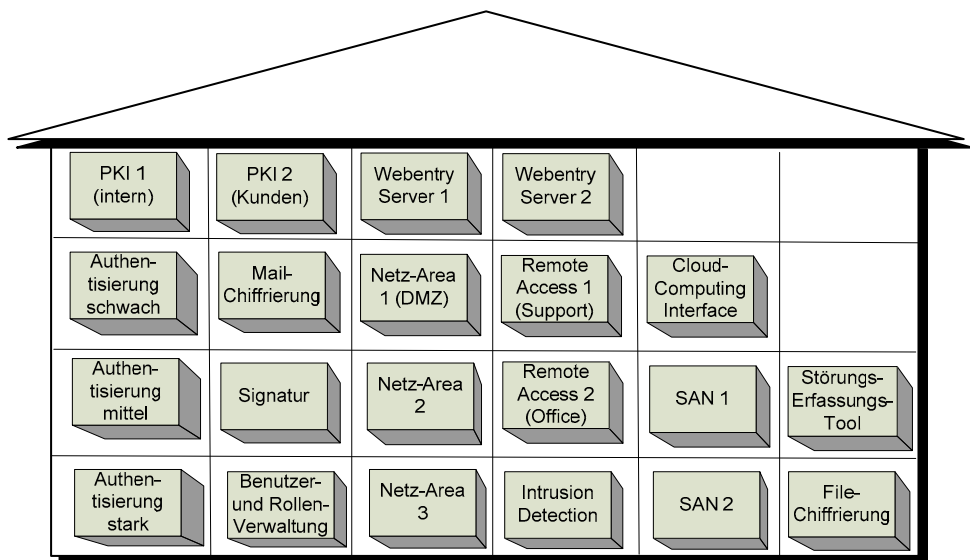


Abbildung 8.5: Beispiel einer IT-Sicherheits-Architektur mit ihren Bausteinen

<i>Baseline Security Standards</i>	Ein verbreitetes Vorgehen besteht auch darin, die System-Plattformen (z.B. UNIX-Server) mit eigenen, für das Unternehmen zugeschnittenen „Baseline Security Standards“ aufzusetzen und zu betreiben. Diesen Standards gehorchend werden beispielsweise beim Aufsetzen der Server, unter dem Begriff „Härtung“, die gefährlichen Betriebssystem-Funktionen sowie die gefährlichen Zugriffs-Funktionen und Netzwerk-Ports beim Installations-Vorgang präventiv unterbunden.
<i>Öffentlich verfügbare Sicherheits-Standards</i>	Im Rahmen der unternehmensinternen Standardisierung werden vermehrt auch öffentlich verfügbaren Sicherheits-Standards (z.B. ISO/IEC 27002, CobiT oder BSI IT-Grundschutz-Kataloge) oder Teile daraus als Unternehmens-Standards erklärt.
<i>Sicherheits-Infrastruktur</i>	Ein grösseres Unternehmen wird sich in der Regel eine eigene „Sicherheits-Infrastruktur“ aufbauen und betreiben. Zu einer solchen Sicherheits-Infrastruktur gehören beispielsweise die zentralen Zugriffs-Kontrollsysteme, die Webentry-, Proxy- und Firewall-Systeme sowie die Intrusion-Detection- und Content-Filter-Systeme. Da diese Infrastruktur-Einrichtungen den einzelnen Plattformen und Applikations-Systemen zur Verfügung gestellt werden, sollten diese Einrichtungen mit ihren Sicherheits-Diensten und Schnittstellen-Spezifikationen als „unternehmensspezifische Standards“ in Kraft gesetzt werden.
<i>Standard-Sicherheits-Einrichtungen erleichtern Risikomanagement</i>	Bezüglich des Risikomanagements erleichtern solche Standard-Sicherheits-Einrichtungen die Durchführung des Risikomanagement-Prozesses, indem die Risiken für eine ganze Population gleichartiger Systeme nur einmal analysiert und die Massnahmen nur einmal konzipiert werden müssen.

Praxistipp:

Standard-Sicherheits-Einrichtungen schaffen nicht nur Transparenz für die Risikobeurteilung, sondern ermöglichen auch die Einsparung von Massnahmenkosten.

8.1.5

IT-Sicherheitskonzepte

Die Informationen sind die Kernelemente von IT-System-Plattformen, -Applikationen, -Prozessen und IT-Dienstleistungen. Die Risiken und der Schutz der Informationen und der damit verbundenen Prozesse werden vorteilhaft im Rahmen eines Sicherheitskonzepts analysiert, konzipiert, und dokumentiert. Das

Sicherheitskonzept garantiert ausgewogenes Massnahmenpaket

Sicherheitskonzept dient somit der spezifischen Analyse und Lösung eines Sicherheitsproblems.

Das Sicherheitskonzept ermöglicht, durch eine ganzheitliche Betrachtung der Unternehmens-IT mit allen Prozessen und Beteiligten, ein ausgewogenes Massnahmenpaket, flankiert mit den notwendigen Sicherheits-Richtlinien, -Vorschriften und organisatorischen Regelungen.

Sicherheitskonzept trägt Ausnahmeregelungen Rechnung

Es ist nützlich, wenn die im Sicherheitskonzept getroffenen Festlegungen für das betrachtete System Weisungscharakter haben. Bei einem entsprechend (durch den CISO) abgenommenen Sicherheitskonzept können für den spezifischen Fall auch Aspekte genereller Weisungen durch Festlegungen im Sicherheitskonzept übersteuert werden. Somit kann ein für den Einzelfall ausgefertigtes Sicherheitskonzept eine allfällig benötigte Ausnahmeregelung darstellen.

Der Aufbau und die Inhalte eines solchen Sicherheitskonzepts, sowie sein Stellenwert für ein Informations-Risikomanagement sind im Abschnitt 10.1 ausführlich behandelt.

8.2

Zusammenfassung

Die Steuerung des Informationssicherheits-Risikomanagements in einem Unternehmen lässt sich anhand einer Führungspyramide darstellen. Die Führungspyramide zeigt die Führungs-Instrumente und die dafür zuständigen Führungs- und Kontrollinstanzen.

Eine **Risiko- und Sicherheits-Politik** wird auf der obersten Ebene des Unternehmens durch den Verwaltungsrat erlassen und legt in groben Zügen die Risiko- und Sicherheits-Organisation und die einzelnen Risiko-Bereiche mit ihren Abgrenzungen fest. Darin enthalten sind auch die übergeordneten Ziele und Grundsätze zu den Risiken und zur Sicherheit im Unternehmen.

In die fachspezifisch abgegrenzte **Informationssicherheitspolitik** werden vermehrt Aspekte des Informationssicherheits-Risikomanagements einbezogen. Insbesondere sind daraus die Grundsätze und Ziele der Risiko- und Sicherheits-Politik, das System der Sicherheits-Weisungen und -Prozesse sowie die entsprechenden Verantwortlichkeiten ersichtlich. Da dieses Politik-Papier an die Mitarbeiter gerichtet ist, bedarf es einer knappen und verständlichen Sprache.

Zur risikobasierten Behandlung der Informationssicherheit im Unternehmen hat sich in jüngster Zeit mit dem Standard ISO/IEC

27001 ein standardisierter Managementprozess etabliert. Der Rahmen eines solchen, für eine kontinuierliche Verbesserung ausgelegten, Managementprozesses wird mittels einer sog. „**Informationssicherheits-Management-Politik**“ festgelegt. Die beiden Politik-Papiere, die ISMS-Politik und die Informationssicherheits-Politik, können in einem einzigen Dokument zusammengefasst werden. Eine Geschäftskontinuitäts-Politik kann ebenfalls in die ISMS-Politik integriert werden. Ein solchermassen gestaltetes „Politik-Papier“ ist den weiter detaillierten Vorschriften übergeordnet.

Die **Informationssicherheits-Weisungen und -Ausführungsbestimmungen** enthalten die Vorschriften und Anleitungen für die verantwortlichen Führungspersonen und Mitarbeitenden bezüglich der Informationssicherheit und der Durchführung und Umsetzung des Informationssicherheits-Risikomanagement-Prozesses. Die Weisungen und Ausführungsbestimmungen werden in einem für das Unternehmen gebräuchlichen Weisungskonzept kommuniziert.

Die **Informationssicherheits-Architektur und die Informationssicherheits-Standards** ermöglichen, insbesondere in Unternehmen mit grossen und komplexen „IT-Landschaften“, die notwendige Übersicht aus Risiko-Sicht sowie effiziente und kostengünstige Lösungen. Dazu müssen in der Sicherheitsarchitektur die oft wiederkehrenden Dienste und Mechanismen entsprechend standardisiert sein. Liefert eine Sicherheits-Architektur Sicherheits-Dienste und -Mechanismen mit verschiedenen Stärken und Schnittstellen, dann verhilft dies, die Massnahmen besser an den aktuellen Risiken zu orientieren. Bei den Sicherheitsstandards können für bestimmte Bereiche des Unternehmens eigene Standards (z.B. Baseline Security Standards) in Frage kommen, die sowohl der Kosteneffizienz als auch der erforderlichen Sicherheit Rechnung tragen.

Die **IT-Sicherheitskonzepte** dienen vor allem der individuellen sicherheitsmässigen Behandlung von IT-Systemplattformen, einzelnen Applikationen und einzelnen Prozessen. Das Sicherheitskonzept behandelt dabei die Risiken, Anforderungen, Massnahmen und Massnahmen-Umsetzungen analog zu den Aufgaben in einem Risikomanagement-Prozess.

Die Sicherheitskonzepte bewegen sich in der Regel im Rahmen der Vorgaben von Weisungen, Ausführungsbestimmungen, Architekturen und Standards. Es ist jedoch nützlich, dass die im Sicherheitskonzept getroffenen konkreten Festlegungen ebenfalls

Weisungscharakter haben. Für Ausnahmefälle ist es auch sinnvoll, wenn formal abgenommene Sicherheitskonzepte einzelne Punkte aus Weisungen oder Ausführungsbestimmungen übersteuern können.

8.3

Kontrollfragen und Aufgaben

1. Warum sollte die allgemeine Risiko- und Sicherheits-Politik eines Unternehmens durch den Verwaltungsrat (Aufsichtsrat) erlassen werden?
2. Erläutern Sie Sinn und Zweck von Informationssicherheits-Weisungen (Information Security Policies) und Informationssicherheits-Ausführungsbestimmungen.
3. Wie wird die Informationssicherheits-Architektur für ein Unternehmen sinnvollerweise aufgebaut?
4. Weshalb kann es allenfalls notwendig werden, mit einem auf einen konkreten Fall bezogenes Sicherheitskonzept die Inhalte von Weisungen und Ausführungsbestimmungen zu übersteuern?

9

Informations-Risikomanagement mit Standard-Regelwerken

In diesem Kapitel wird die Bedeutung der Standard-Regelwerke in der Informationssicherheit behandelt und gezeigt, wie solche Regelwerke dem Informations-Risikomanagement* dienen. Die hier als „Standard-Regelwerke“ bezeichneten Regelwerke sind nationale oder internationale Standards oder Rahmenwerke und Referenzmodelle, die den Status eines „De-facto-Standards“ erlangt haben. Einige der heute für die Informationssicherheit und das Informations-Risikomanagement gültigen Standard-Regelwerke werden übersichtsweise mit ihrem Ursprung und Einsatzzweck sowie mit einigen wichtigen Merkmalen vorgestellt. Viele dieser Regelwerke weisen für ihren Anwendungszweck Überschneidungen untereinander auf. Dennoch verfügt jedes Regelwerk über bestimmte Aspekte bevorzugte Gesichtszüge [Grue04]. Auch bestehen Unterschiede in der Anwendungsbreite und Unterstützungstiefe. Die Regelwerke der Reihe ISO/IEC 2700x sowie CobiT werden hinsichtlich der für das Informations-Risikomanagement wichtigen Aspekte näher behandelt. Für eine weitergehende und tiefere Behandlung ist auf die Originalquellen und die zahlreich vorhandene Spezialliteratur verwiesen.

9.1

Grundschutz-massnahmen

Bedeutung der Standard-Regelwerke

Immer mehr kommen für Aufbau und Erhalt der Informationssicherheit „Standard-Regelwerke“ und vor allem „Grundschutz-massnahmen“ zum Einsatz. Im englischen Sprachgebrauch sind die Grundschutzmassnahmen unter dem Begriff „Baseline Security Controls“ bekannt. Die Grundschutzmassnahmen existieren oft als nationale oder internationale Standards und erfahren als solche eine breite Abstützung, sowohl was ihre Erstellung als auch ihre Anwendung betrifft.

* Wir sprechen hier von „Informations“-Risikomanagement, da einige Regelwerke definitionsgemäss sowohl dem „Informationssicherheits“-Risikomanagement als auch dem „IT“-Risikomanagement dienen.

Best Practices

Viele der heute verfügbaren Standard-Regelwerke entstehen aus weit verbreiteten Praktiken, den sog. „besten Praktiken“ oder „guten Praktiken“ („best/good practices“). Sie enthalten die breit abgestützten Anleitungen und Massnahmen (Controls), die in der Praxis zum Einsatz gelangen sollen. Grössere Unternehmen unterhalten oft ihre eigenen Massnahmenkataloge, die den spezifischen Anforderungen des Unternehmens oder der Branche sowohl bezüglich der spezifischen Risikolage als auch bezüglich der Einbettung in die firmeneigene IT-Architektur und Management-Prozesse sowie in die übrigen firmenspezifischen Standards Rechnung tragen. Im Teil B des Buches wurden bereits die an ein Unternehmen gestellten Anforderungen aufgezeigt, für die der Einsatz von Standard-Regelwerken geradezu prädestiniert ist.

Regelwerke für Realisierung und Kontrolle

Einige der Standard-Regelwerke geben zusätzlich Anleitungen und Hinweise, wie die Umsetzung der Massnahmen in der Praxis überprüft werden kann. Sie sind somit Regelwerke sowohl für die Realisierung als auch für die Überwachung, Überprüfung und Berichterstattung (Review / Audit).

Aus verschiedenen Gründen empfiehlt es sich, in einem Unternehmen allgemeine oder auch branchenspezifische „Grundschutz-Standards“ einzusetzen.

Solche Gründe sind beispielsweise:

- Übersichtlichkeit
- Vergleichbarkeit mit anderen Unternehmen
- Überprüfbarkeit
- Gütesiegel bei Service-Angeboten (z.B. bei Offerings)
- Argumentationshilfe in der Kostendebatte

Auswahl eines Regelwerks

Die Auswahl eines bestimmten Regelwerks oder eines Grundschutz-Standards wird oft aufgrund der von aussen an das Unternehmen gestellten Anforderungen erfolgen.

Solche Anforderungen können beispielsweise sein:

- Anforderungen von Kunden;
- Gesetzliche und/oder regulative Anforderungen wie Sarbanes-Oxley Act in den USA oder Payment Card Industries (PCI) für Zahlkarten-Informationsverarbeiter.

Ausreichender Basisschutz

Wie der Begriff „Grundschutz-Standards“ zum Ausdruck bringt, bieten diese Standards einen für typische IT-Systeme und Anwendungen (insbesondere bei Standardanwendungen wie E-Mail, Internet-Zugriff, Büroanwendungen) ausreichenden Basisschutz. Bei diesem Basisschutz werden jedoch die spezifischen

Spezifische Risiken

Informationssicherheits-Risiken für ein System oder eine Anwendung nicht ausdrücklich und oft auch nicht angemessen berücksichtigt. Mit entsprechenden Klauseln machen die Grundschutz-Standards auf diesen Umstand aufmerksam oder verlangen gar die Durchführung eines „Risiko-Assessments“ zur Ermittlung von allenfalls zusätzlich notwendigen spezifischen Massnahmen.

Die angemessene Berücksichtigung von spezifischen Risiken, die einer umfassenden Risiko-Analyse bedürfen, kann anhand eines Analysevorgehens, wie es die Abbildung 9.1 zeigt, gewährleistet werden. Dabei wird mit einer einfachen Impact-Analyse festgestellt, ob die Kritikalität der Schutz-Objekte eine umfassende Risiko-Analyse erfordert oder ob der Grundschutz ausreicht.

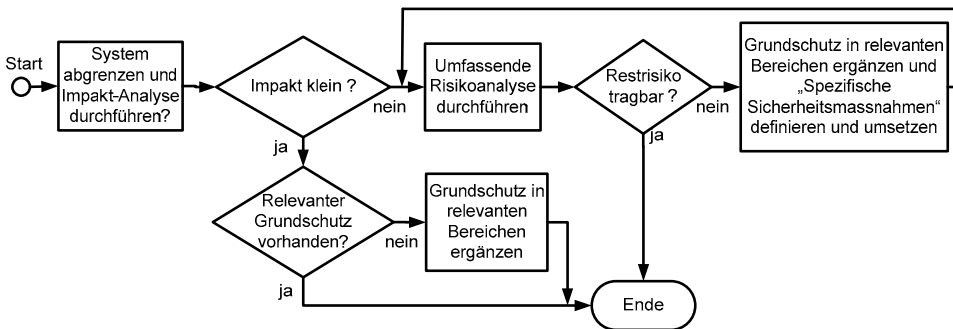


Abbildung 9.1: Kombination Grundschutzmassnahmen und risikobasierter Ansatz

Viele der Standard-Regelwerke widmen sich nicht nur der Sicherheit im Sinne eines Grundschatzes, sondern dem Management der IT-Prozesse und der Informationssicherheit im Rahmen des Führungssystems im Unternehmen. Wir verwenden deshalb für alle diese Standards, De-facto-Standards, Grundschatzkataloge, Rahmenwerke und Referenzmodelle im Weiteren kurz die Bezeichnung „Regelwerke“.

9.2

Übersicht über wichtige Regelwerke

Die im Rahmen dieses Buches interessanten Regelwerke sind meist der IT-Governance, der Informationssicherheits-Governance oder der Informationssicherheit zugeordnet.

Aus diesem Blickwinkel finden zurzeit folgende Regelwerke breite Anwendung:

- ☐ ISO/IEC 2700x (eingehende Behandlung in Abschnitt 9.3)
- ☐ CobiT (eingehende Behandlung in Abschnitt 9.4)

- ❑ BSI-Standards und IT-Grundschutz-Kataloge (eingehende Behandlung in Abschnitt 9.5)

Die mit den nachfolgenden Tabellen 9.1 bis 9.5 übersichtsmässig behandelten Regelwerke decken aus einer bestimmten Anwendungsperspektive spezifische Gebiete der IT und der Informationssicherheit ab und treffen in diesen Anwendungsgebieten für das Informations-Risikomanagement relevante Aussagen.

Tabelle 9.1: ISO / IEC 15408 Common Criteria

Regelwerk	Common Criteria (CC) seit 1999 ISO/IEC 15408 (CC / ITSEC) Inzwischen ist der Standard in drei Teilen veröffentlicht: ISO/IEC 15408-1:2009 Part 1: Introduction and general model ISO/IEC 15408-2:2008 Part 2: Functional Requirements ISO/IEC 15408-3:2008 Part 3: Assurance Requirements
Herkunft	CC ist das Ergebnis, die Standards ITSEC (Europa), U.S. TCSEC (USA) und CTCPEC (Canada) in einem internationalen Standard zusammen zu führen.
Einsatzzweck	Kriterien, mit denen nachgewiesen werden kann, dass ein IT-Produkt oder IT-System (Target of Evaluation) die Anforderung seines „Security Target“ erfüllt.
Wichtige Merkmale	Bei der Evaluation beschafft sich der „Evaluator“ detaillierte Kenntnisse über die Funktionen und die Sicherheit des Produkts in der vorgesehenen Betriebsumgebung. Ebenso untersucht der „Evaluator“ die Benutzerführung, wie das Produkt entwickelt ist und wie es sich gegenüber Störungen von aussen verhält. Das Evaluationsergebnis wird in 7 Stufen (EAL1* bis EAL7) bewertet: EAL1 (E0-E1)*: funktionell getestet EAL2 (E1): strukturell getestet EAL3 (E2): methodisch getestet und überprüft EAL4 (E3): methodisch entwickelt, getestet und durchgesehen EAL5 (E4): semiformal entworfen und getestet EAL6 (E5): semiformal verifizierter Entwurf und getestet EAL7 (E6): formal verifizierter Entwurf und getestet Es ist anzumerken, dass das Verfahren sehr aufwendig ist, und über EAL3 hinausgehende Evaluationen in nützlicher Frist kaum umsetzbar sind.

* Die frühere Stufenbezeichnung war EAL0 bis EAL6

* Die Bezeichnungen in Klammern nehmen Bezug auf den parallelen ITSEC-Standard

Geht es um Informationssicherheit, Informations-Risiken oder auch um andere Risiken im Unternehmen, so macht sich immer mehr die Erkenntnis breit, dass Massnahmenkataloge alleine die Umsetzung nur ungenügend bewirken können. Wie die im Folgenden behandelten Regelwerke zeigen, wird deshalb die Auswahl, Einsetzung und Überwachung von Massnahmen durch entsprechende Management-Systeme unterstützt oder gar zwangsläufig gesteuert.

Tabelle 9.2: ITIL V3 (IT Infrastructure Library)

Regelwerk	IT Infrastructure Library V3, derzeit publiziert als 2011 Edition
Herkunft	Herausgegeben durch die IT Service Management Foundation. Entwickelt durch die Office of Governance Commerce (OGC) im Auftrag der britischen Regierung.
Einsatz- zweck	„Best practice“ als De-facto-Standard für IT-Serviceprozesse.
Wichtige Merkmale	Unterstützt eine prozessorientierte Strukturierung von Betreiber-Organisationen für IT- und Telekommunikations-Dienste unter Einbezug der Benutzer. Gegenüber früheren Versionen wurde mit der Version V3 die frühere Strukturierung in „Service Support“ und „Service Delivery“ durch die Strukturierung mit einem „Service Lifecycle“ abgelöst. Dieser besteht aus den hauptsächlichen Phasen: „Service Strategy“, „Service Design“, „Service Transition“, „Service Operation“ und „Continual Service Improvement“. Den Sicherheitsaspekten wird durch Prozesse wie „Availability Management“, „IT Service Continuity Management“, „Information Security Management“, unter Anlehnung an ISO/IEC 27002, umfassend Rechnung getragen (z.B. eigene Prozesse für „Access Management“ und „Incident Management“). Für das Risikomanagement ist ein eigenständiger Prozess vorgesehen. Dafür wird das Framework „Management of Risk“ der OGC empfohlen.

Tabelle 9.3: ISO/IEC 20000

Regelwerke	ISO/IEC 20000-1:2011 (second edition): Service management Part 1: Service management system requirements; ISO/IEC 20000-2:2005: Service management Part 2: Code of practice.
Herkunft	Ursprünglich als britische Standards BS 15000-x entwickelt und an den Prozessbeschreibungen ausgerichtet, wie sie durch ITIL des Office of Government Commerce (OGC) definiert wurden.
Einsatzzweck	Integrierter Prozess-Ansatz für Service- Prozesse, die den Geschäfts- und Kundenanforderungen wirksam Rechnung tragen.
Wichtige Merkmale	Der Teil 1 enthält den Servicemanagement-Prozess basierend auf einem PDCA-Zyklus sowie die Teilprozesse und die „Muss-Kriterien“ zur Erlangung einer Zertifizierung durch eine „Registered Certification Body“. Der gesamte Service-Lieferungsprozess ist, ähnlich den ITIL-Richtlinien, in die wesentlichen Teilprozesse, wie „Capacity Management“, sowie die wichtigen die Verfügbarkeit und Sicherheit betreffenden Prozesse aufgeteilt, wie „Service continuity and availability management“ oder „Information security management“. Der Teil 2 zeigt wie die Anforderungen von Teil 1 im Einzelnen mit „Best practice“-Vorschlägen erfüllt werden können. Die Anforderungen an das „Information security management“ widerspiegeln einige wesentliche Elemente aus dem Standard ISO/IEC 27001 (z.B. Risks to information assets) oder beziehen sich auf den Standard ISO/IEC 27002.

Tabelle 9.4: NIST 800-14, NIST 800-27 und NIST 800-30

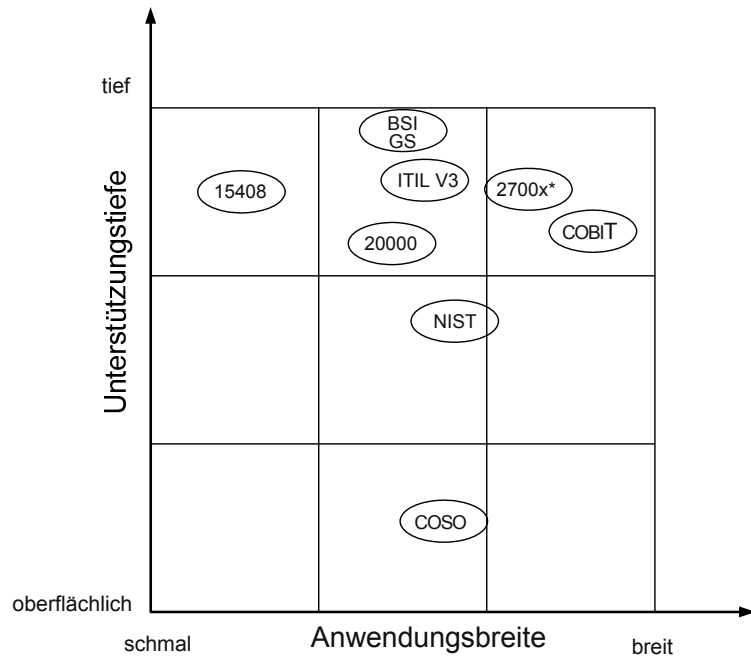
Regelwerke	NIST 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems [Swan96]; NIST 800-27: Engineering Principles for Information Technology Security; NIST 800-30: Risk Management Guide for Information Technology Systems.
Herkunft	Spezial-Publikationen des amerikanischen „National Institut of Standards and Technology“ (NIST) der Reihe 800-x über IT-Sicherheit.
Einsatzzweck	Richtlinien und Empfehlungen vorwiegend für US-Regierungsorganisationen zur Verbesserung der Informationssicherheit bestimmt, aber auch von anderen Unternehmen (öffentliche oder private) sinnvoll anwendbar.
Wichtige Merkmale	Die „Principles“ and „Practices“ bilden bei den Standards NIST 800-14 und NIST 800-27 in Check-Listen-Form die wesentlichen Komponenten eines IT-Sicherheits-Programms. Das Risikomanagement ist in die einzelnen Phasen der Lebenszyklen von Informationssystemen integriert. Im Gegensatz zu NIST 800-27, der die IT-Sicherheitsaspekte der Systeme selbst adressiert, fokussiert der SP 800-14 auf die Computersicherheit aus der Unternehmens-Perspektive, sowohl bei der Entwicklung neuer Systeme als auch bei der Ausarbeitung von Policies und Praktiken. Der derzeit im Entwurf für eine neue Version befindliche Standard NIST 800-30 bezweckt ein ganzheitliches Assessment von Informationssicherheits-Risiken in einem Unternehmen. Das Assessment kann auf den drei Ebenen eines Unternehmens, der „Unternehmensebene“, der „Geschäftsprozessebene“ oder der „Informationssystemebene“ durchgeführt werden.

Tabelle 9.5: COSO Internal Control-Integrated Framework

Regelwerke	„Internal Control-Integrated Framework“ und „Enterprise Risk Management – Integrated Framework“ als Ergänzung.
Herkunft	Dokument des „Committee of Sponsoring Organizations of the Treadway Commission“ ist seit 1992 von der „Securities and Exchange Commission“ anerkannter Standard für interne Kontrollen.
Einsatzzweck	Die „Reports“ mit einem „Framework“ [Cosa02] als Hauptdokument, sind vor allem dazu bestimmt, die interne Kontrolle hinsichtlich der Finanzberichterstattung zu verbessern und die Unternehmens- und Profitabilitäts-Ziele sowie die Compliance zu erreichen.
Wichtige Merkmale	Interne Kontrolle als Prozess mit den Komponenten „Kontroll-Umgebung“, „Risiko-Assessment“, „Kontrollaktivitäten“, „Information/Kommunikation“ und „Überwachung“ gestaltet. Innerhalb dieser Kontrollkomponenten sind Anforderungen vorgegeben, die mit „Evaluation-Tools“ ermittelt und bewertet werden können. Die IT-Anforderungen sind nicht umfassend behandelt, jedoch können die darin enthalten wesentlichen Konzepte und Definitionen auch auf die IT und vor allem auf die IT-Governance angewendet werden.

Schwerpunkte von Regelwerken Die Regelwerke berücksichtigen verschiedene Schwerpunkte, z.B. bezüglich „Planung und Organisation“, „Beschaffung und Einführung“, „Auslieferung und Unterstützung“ sowie bezüglich „Überwachung“. Auch bestehen wesentliche Unterschiede in der Anleitung zur Kontrolle, zum Risikomanagement und zur Massnahmen-Konzeption.

Die wichtigsten Regelwerke (z.B. CobiT, ISO/IEC 27002 oder ITIL) verfügen über Vergleichs-Tabellen. In Anlehnung an die durch das IT Governance Institute getroffene Klassifizierung [Itgi04] können die Regelwerke, wie in Abbildung 9.2 gezeigt, bezüglich ihrer Unterstützungstiefe und ihrer Anwendungsbreite eingeordnet werden.



Legende:

- Unterstützungstiefe: Technischer und betrieblicher Detaillierungsgrad
- Anwendungsbreite: Vollständigkeit der adressierten Sicherheitsanliegen
- 2700x*: ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27005.

Abbildung 9.2 Einordnung der Regelwerke bezüglich Vollständigkeit (vgl. [Itgi06], S. 71)

Die Anwendungsbreite ist oft eingeschränkt durch die Fokussierung auf einzelne Teilbereiche im Lebenszyklus der Informationen oder Informationstechnologien. Viele Regelwerke behandeln lediglich die Sicherheitsziele „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ unter Auslassung spezifischer Leistungs-Ziele, aufgrund der Geschäftsanforderungen an die Informationen und die IT wie „Effektivität“ oder „Compliance“.

9.3

Risikomanagement mit der Standard-Reihe ISO/IEC 2700x

In der vorherigen Übersicht über Standard-Regelwerke der Informationssicherheit wurden einige wichtige heute vorhandene Standards der Standard-Reihe ISO/IEC 2700x kurz erwähnt. Da

die Standard-Reihe 2700x den Anspruch erhebt, das Informationssicherheits-Management aus der Perspektive der Informationstechnologie vollständig abzudecken, wird auf dieses Regelwerk nachfolgend näher eingegangen.

Mit der ISO/IEC 2700x Familie ist ein Rahmenwerk für ein **Informationssicherheits-Management-System** (ISMS) beabsichtigt, das sowohl den Anforderungen eines Grundschutzes als auch dem Management der Sicherheit und der Risiken der Information im Unternehmen Rechnung trägt.

Im Rahmen dieses Buches über Informations-Risikomanagement interessieren vor allem die folgenden drei Standards:

- ISO/IEC 27000:2009* (Overview and vocabulary)
- ISO/IEC 27001:2005† (Information security management systems – Requirements),
- ISO/IEC 27002:2005‡ (Code of practice for information security management) und
- ISO/IEC 27005:2011 (Information security risk management).

Zentral innerhalb dieser Standardreihe ist der ISMS-Standard ISO/IEC 27001, der analog zu ISO 9001 der Standard-Reihe ISO 900x des Qualitätsmanagements die Prozesse vorgibt, mit denen eine ständige Kontrolle und Verbesserung der Managementvorgänge und der Informationssicherheit erreicht werden kann. Das Risikomanagement ist dabei Teil des Informationssicherheits-Management-Systems und kann Teil des Unternehmens-Risikomanagements sein. Wie sich das Unternehmens-Risikomanagement nach dem PDCA-Zyklus in die Unternehmensführung integrieren lässt, wurde bereits im Abschnitt 5.1 (vgl. Abbildung 5.2) gezeigt. Bevor wir im Kapitel 12 auf das Zusammenspiel des Informations-Risikomanagements und der Führungsprozesse im Unternehmen näher eingehen, tauchen wir in die Standard-Reihe ISO/IEC2700x tiefer ein.

Des besseren Überblicks willen sind in Abbildung 9.3 die im Kontext des Informations-Risikomanagements hauptsächlich

* Die Ausgabe ISO/IEC 27000:2009 wird derzeit überarbeitet.

† Die Ausgabe ISO/IEC 27001:2005 wird derzeit überarbeitet.

‡ Die Ausgabe ISO/IEC 27002:2005 geht ohne Änderung aus der Umbezeichnung des heutigen Standards ISO/IEC 17799:2005 hervor und wird derzeit überarbeitet.

interessierenden interessanten ISO-Papiere der 2700x-Familie aufgezeigt.

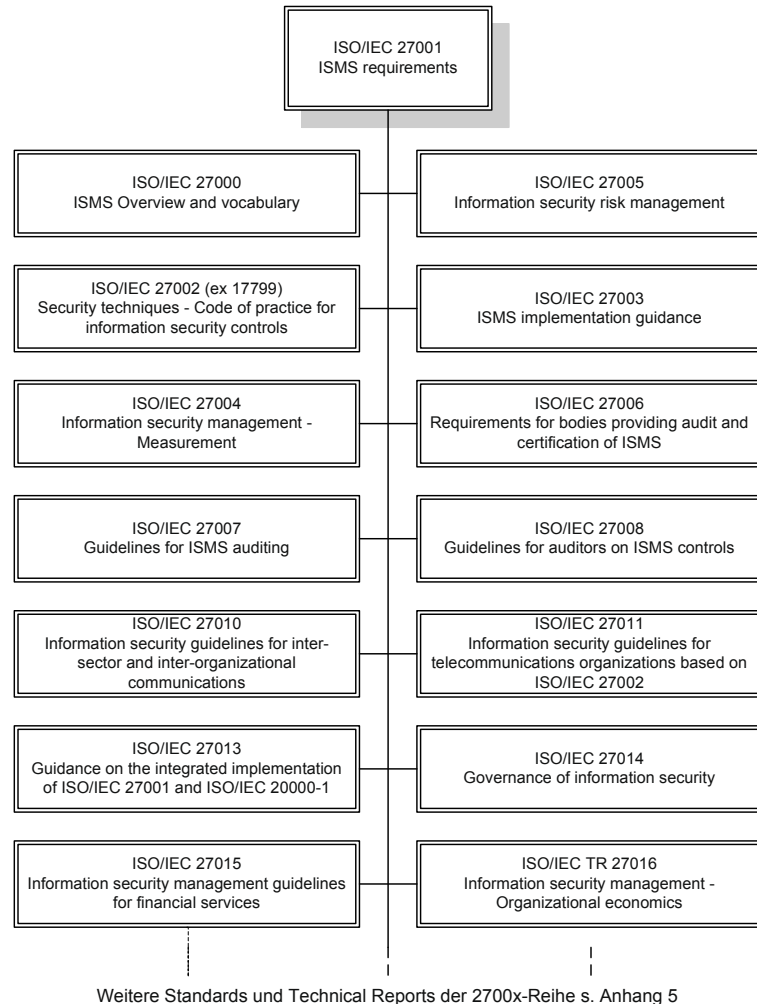


Abbildung 9.3: ISO/IEC2700x-Familie

9.3.1

Informationssicherheits-Management nach ISO/IEC 27001

Der Standard ISO/IEC 27001 kurz „ISMS-Standard“, ist das Herzstück der 2700x-Reihe und dazu bestimmt, ein Informationssicherheits-Management-System (ISMS) in einem Unternehmen aufzubauen und aufrecht zu erhalten. Das ISMS soll die Auswahl

von geeigneten und angemessenen Prozessen und Massnahmen zum Schutze der Informationen und deren Werte im Unternehmen sicherstellen und dafür Vertrauen schaffen.

Der Standard beschreibt in Anlehnung an die Management-Standards ISO 9001:2000 und ISO 14001:2004 ein als Prozess gestaltetes Management-System zur Einrichtung und Aufrechterhalten von Informationssicherheit im Unternehmen. Der Prozess basiert auf dem aus dem Qualitätsmanagement bekannten „Plan-Do-Check-Act“-Modell (PDCA), welches ursprünglich durch die Qualitätsmanagement-Pioniere Walter A. Shewhart und W. Edwards Deming als „Lernzyklus“ mit den Phasen „Plan-Do-Study-Act“ eingeführt wurde (s. Abbildung 9.4).

Mit dem Standard ISO/IEC 27001 wird ein Informationssicherheits-Management bezweckt, welches den spezifischen Geschäftsrisiken eines Unternehmens oder bestimmter Unternehmensteile Rechnung trägt und zudem in andere verwandte Management-Systeme integriert werden kann.

- In der **„Plan“-Phase** des PDCA-Zyklus werden demzufolge die Risiken im Einklang mit der Unternehmensstrategie und den Geschäftsanforderungen (rechtlich, regulatorisch oder vertraglich) erhoben und bewertet. Für das „Risk Assessment“ wird jedoch beispielhaft der „Technical Report“ ISO/IEC TR 13335-3^{*} angeführt. Bei den zu planenden Massnahmen zur Risiko-Bewältigung wird auf den „Code of Practice“ ISO/IEC 17799:2005 verwiesen (neue Bezeichnung ISO/IEC 27002).
- Die **„Do“-Phase** enthält die Anweisungen für die Umsetzung und den effektiven Betrieb des ISMS und der Massnahmen einschliesslich der dafür notwendigen Management-Aktionen.
- Die **„Check“-Phase** dient vor allem der Überwachung der Effektivität des ISMS, der Risiken, und der Effektivität der Massnahmen sowie den laufenden Kontrollen.
- Die **„Act“-Phase** enthält den laufenden Unterhalt und die korrektiven und präventiven Aktionen zur Verbesserung des ISMS hinsichtlich der beabsichtigten Ziele sowie die

* Die Standards und Technical Reports der Reihe ISO/IEC 13335-x wurden inzwischen inhaltlich sukzessive in Standards der Reihe ISO/IEC 2700x überführt.

Kommunikation der Aktionen und Verbesserungen an alle interessierten Stellen (Anspruchsgruppen).

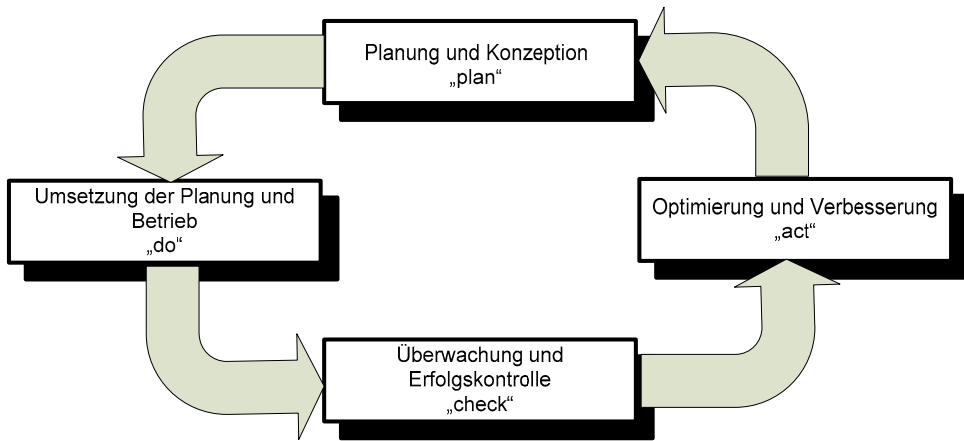


Abbildung 9.4: PDCA-cycle für ISMS nach ISO/IEC 27001 (Deming cycle)

Wie bereits beim britischen Vorgängerstandard BS 7799-2 sind auf der Basis des nun internationalen Standards ISO/IEC 27001 Zertifizierungen durch akkreditierte Unternehmen möglich (in der Schweiz z.B. SQS, Swiss TS oder KPMG).

Tabelle 9.6: Übersicht über ISO/IEC 27001

Regelwerk	ISO/IEC 27001:2005 Information security management systems – Requirements
Herkunft	„British Standards Institute“ BS 7799-2
Einsatz-zweck	Aufbau eines Informationssicherheits-Management-Systems (ISMS) und seiner Verankerung im Unternehmen
Wichtige Merkmale	Prozessansatz (PDCA: Plan - Do - Check - Act) zur Entwicklung, Umsetzung, Durchführung, Überwachung, Aufrechterhaltung und zur kontinuierlichen Verbesserung eines organisationsbezogenen ISMS. Der Standard soll zudem ermöglichen, das ISMS mit verwandten Managementsystemen (ISO 9001:2000 und BS ISO 14001:2004) abzugleichen oder zusammenzuführen.

Der Standard erfährt im Rahmen dieses Buches besondere Beachtung, da er ein „risikobasiertes“ Sicherheitsmanagement verfolgt und die wesentlichen Prozessschritte für den Aufbau und die nachhaltige Aufrechterhaltung der Informationssicherheit im Unternehmen vorgibt. Nachfolgend werden die für eine Zertifizierung als zwingend zu befolgenden Kapitel 4 bis 8 des Standards ISO/IEC 27001:2005 grob dargestellt*:

Das Kapitel 4 des Standards behandelt den eigentlichen Prozess des ISMS und beginnt im Unterkapitel 4.1 mit:

Generellen Anforderungen:

Das Unternehmen muss ein dokumentiertes ISMS

- einrichten,
- verwirklichen,
- betreiben,
- überwachen,
- nachprüfen,
- unterhalten und verbessern.

Diese Aktivitäten müssen im Kontext der gesamten Geschäftsaktivitäten und der Risiken des Unternehmens erfolgen.

Das nächste Unterkapitel 4.2 des Standards beschreibt die Einrichtung und Verwaltung des ISMS. Die einzelnen Überschriften und Klauseln in diesem Unterkapitel können dem PDCA-Zyklus zugeordnet werden und erfüllen zudem die Aktivitäten eines Risikomanagement-Prozesses.

In den nachstehenden Tabellen 9.7 bis 9.10 sind die Standard-Klauseln der Unterkapitel 4.2.1 bis 4.2.4 in die hauptsächlichen Schritte eines Risikomanagement-Prozesses eingeordnet.

* Die in diesem Buch wiedergegebene Erläuterung des Standards beschränkt sich auf die für das Risikomanagement wesentlichen Aspekte und erhebt nicht den Anspruch auf Detailgenauigkeit, wie sie beispielsweise für eine Zertifizierung nötig ist.

Tabelle 9.7: Einrichtung des ISMS (Phase „plan“, 4.2.1)

Festlegung Kontext	Das Unternehmen unternimmt folgende Aktivitäten: a) Definition des Einsatzbereichs (Scope) und der Abgrenzungen des ISMS. b) Definition einer ISMS-Policy (diese ist der „Informationssicherheits-Policy“ übergeordnet, kann aber im selben Dokument abgefasst sein). Darin ist u.a. die Ausrichtung des ISMS am strategischen Risikomanagement-Kontext des Unternehmens gefordert. c) Definition einer Risiko-Assessment-Methode für vergleichbare und reproduzierbare Ergebnisse: 1. die Methode muss dem ISMS, der Geschäfts-Informationssicherheit sowie den gesetzlichen und regulatorischen Anforderungen angepasst sein; 2. es müssen Kriterien zur Akzeptanz von Risiken entwickelt und die akzeptablen Höhen der Risiken identifiziert sein.
Risiko-Assessment	d) Risiko-Identifikation 1. Identifikation der Assets innerhalb des Einsatzbereichs des ISMS sowie die Owner der Assets. 2. Identifikation der Bedrohungen auf die Assets. 3. Identifikation der Schwachstellen, welche durch die Bedrohungen ausgenutzt werden könnten. 4. Identifikation der Impacts, die durch Verluste der Vertraulichkeit, Integrität oder Verfügbarkeit der Assets entstehen können. e) Analyse und Bewertung der Risiken 1. Bestimmung der Geschäft-Impacts (resultierend aus Verlust von Vertraulichkeit, Integrität und Verfügbarkeit der Assets) 2. Bestimmung der realistischen Eintritts-Wahrscheinlichkeit 3. Einschätzung der Risiko-Höhe 4. Entscheidung, ob die Risiken akzeptiert werden können (s. Kriterien in c2) oder ob Bewältigungs-Massnahmen ergriffen werden müssen.

Tabelle 9.8: Einrichtung ISMS und Risiko-Behandlung (Phase „do“ in 4.2.1)

Risikobehandlungs-Optionen und -Massnahmen	f) Identifikation und Auswahl geeigneter Optionen zur Behandlung der Risiken 1. Geeignete Massnahmen zur Milderung; 2. Bewusstes und objektives Akzeptieren der Risiken, basierend auf den Unternehmens-Policies und den vorgegebenen Akzeptanz-Kriterien (s. c2); 3. Risiko-Vermeidung; 4. Transfer der resultierenden Geschäftsrisiken zu anderen Parteien (z.B. Versicherungen oder Dienstleister). g) Auswahl von Massnahmen-Zielen und Massnahmen zur Risiko-Behandlung (angemessene Massnahmen aus ISO/IEC 27002 und/oder zusätzliche Massnahmen). h) Genehmigung des vorgeschlagenen Restrisikos durch das Management. i) Autorisierung der Umsetzung und des Betriebs des ISMS durch das Management. j) Erstellung einer schriftlichen „Erklärung zur Anwendbarkeit“ der Risikobewältigung. Dieses „Statement of Applicability“ enthält die Massnahmen-Ziele und entsprechenden Massnahmen sowie die Begründung für die Wahl oder Nichtverwendung von Massnahmen: 1. Massnahmenziele und Massnahmen in 4.2.1g ausgewählt mit Begründung für deren Auswahl; 2. Massnahmenziele, die durch bestehende Massnahmen bereits erfüllt werden; 3. Nicht eingesetzte Massnahmenziele und Massnahmen aus ISO/IEC 27002 mit entsprechender Rechtfertigung.
--	--

Tabelle 9.9: Umsetzung und Betrieb des ISMS (Phase „do“, 4.2.2)

Massnahmenplanung und -Umsetzung	Das Unternehmen unternimmt folgende Aktivitäten: a) Formulierung eines Risiko-Behandlungs-Plans (Management-Aktivitäten, Ressourcen, Verantwortlichkeiten und Prioritäten). b) Umsetzung des Risiko-Behandlungs-Plans zur Erfüllung der Massnahmenziele (Mittel-aufbringung und Zuordnung von Rollen und Verantwortlichkeiten). c) Umsetzung der ausgewählten Massnahmen zur Erreichung der Massnahmenziele (s. 4.2.1 g) d) Bestimmung, wie die Wirksamkeit der eingesetzten Massnahmen gemessen und die Resultate verglichen und reproduziert werden können (s. 4.2.3 c). e) Umsetzung von Ausbildungs- und Awareness-Programmen. f) Verwaltung des ISMS-Betriebs. g) Verwaltung der ISMS-Ressourcen. h) Umsetzung von Verfahren und Massnahmen zur unverzüglichen Erkennung von sicherheitsrelevanten Vorfällen und zur Abwehr von Schadensereignissen (s. 4.2.3 a).
----------------------------------	--

Tabelle 9.10: Überwachung und Nachprüfung des ISMS (Phase „check“, 4.2.3)

Überprüfung und Überwachung	Das Unternehmen unternimmt folgende Aktivitäten: a) Ausführung von Überwachungs- und Nachprüfungs-Verfahren (z.B. unverzügliche Fehlererkennung, unverzügliche Identifikation von versuchten und erfolgreichen Sicherheits-Verstößen und -Ereignissen, Ermöglichung der Management-Kontrolle, dass die Aktivitäten und Massnahmen erwartungsgemäss umgesetzt werden.) b) Regelmässige Nachprüfung der Wirksamkeit des ISMS unter Berücksichtigung von Audits, Ereignissen, Wirksamkeitsmessungen sowie von Vorschlägen und Rückmeldungen aller interessierten Stellen. c) Messung der Massnahmenwirksamkeit, um die Erfüllung der Sicherheitsanforderungen zu überprüfen. d) Nachprüfung des Risiko-Assessments in geplanten Zeitabständen und Nachprüfung, ob sich das Restrisiko im akzeptablen Rahmen hält (zu berücksichtigen sind dabei: Veränderungen des Unternehmens, der Technologie, der Geschäftsziele und -prozesse, der Bedrohungen, der Wirksamkeit der Massnahmen und der externen Einflüsse, z.B. aufgrund gesetzlicher, regulatorischer oder vertraglicher Veränderungen). e) Durchführung interner Audits des ISMS in geplanten Zeitabständen. f) Regelmässige Nachprüfung des ISMS durch das Management, um die Richtigkeit des Einsatzbereiches und das Erkennen von Verbesserungen sicherzustellen. g) Anpassung der Sicherheitsplanungen an die Resultate der Überwachungs- und Nachprüfungs-Aktivitäten. h) Aufzeichnung aller Aktivitäten und Ereignisse, die einen Einfluss auf die Wirksamkeit oder Leistung des ISMS haben.
-----------------------------	--

Tabelle 9.11: Unterhalt und Verbesserung des ISMS (Phase „act“, 4.2.4)

Kommunikation, Feedback	Das Unternehmen unternimmt folgende Aktivitäten: a) Umsetzung der festgestellten Verbesserungen des ISMS. b) Durchführung der geeigneten korrektiven und präventiven Aktionen. c) Kommunikation der Aktionen und Verbesserungen an alle interessierten Stellen in einem den Umständen entsprechenden Detaillierungsgrad und, wo nötig, Vereinbarung des weiteren Vorgehens. d) Sicherstellung, dass die Verbesserungen die beabsichtigten Ziele erreichen.
-------------------------	--

Die weiteren Klauseln des Standards enthalten jeweils generelle Aussagen für das gesamte ISMS, so werden im Unterkapitel 4.3 die Anforderungen an die Dokumentation aufgeführt; diese betreffen sowohl die Entscheidungen und Politiken des Managements als auch die Vorgehensweisen und Massnahmen sowie das Festhalten von Fakten, welche sowohl die Übereinstimmung mit den Anforderungen als auch die Wirksamkeit des Betriebs nachweisen. In den Kapiteln 5 bis 8 werden sodann die Voraussetzungen stipuliert, in die ein funktionsfähiges ISMS eingebettet sein muss:

- o Management-Verantwortlichkeiten (in Kapitel 5),
- o Anforderungen an ein internes Audit (in Kapitel 6),

- Überwachung des ISMS durch das Management (in Kapitel 7) und letztlich
- Aktionen zur Verbesserung des ISMS (in Kapitel 8).

Der Anhang A des Standards enthält die Massnahmenziele und Massnahmen des Standards ISO/IEC 27002 und hat für den Standard ISO/IEC 27001 „normative“ Bedeutung: Wie die Ziffern „g“ und „j“ in der Tabelle 9.8 zeigen, sind doch vorrangig die Massnahmen aus dem Anhang A auf ihre Anwendbarkeit zur Risikobewältigung zu überprüfen. Diese Überprüfung muss mit einer schriftlich festgehaltenen „Erklärung zur Anwendbarkeit“ (Statement of Applicability) belegt werden. Der mögliche Aufbau einer solchen „Erklärung zur Anwendbarkeit“ ist in der nachfolgenden Tabelle 9.12 dargestellt.

Tabelle 9.12: Aufbau einer „Erklärung zur Anwendbarkeit“

Paragraph	Massnahmenziel (Control Objective 27002)	Massnahme (Control 27002)	Anwendbar ja / nein	Bemerkungen: 1) Begründung Massnahmenwahl 2) Bereits bestehende Massnahmen 3) Nichtverwendung von Massnahmen aus Anhang A und Begründung 4) Referenz-Dokument
Anhang A				
A.5	Security Policy			
A.5.1	Information security policy	A.5.1.1 Information security policy document	ja	Dokument Nr. 001 Inf.- Sicherheits-Politik
		A.5.1.2 Review of the information security policy	ja	In Inf.-Sicherheits-Politik festgelegt; Dokument Nr. 002
A.6	Organisation of information Security			
A.6.1	Internal Organisation	A.6.1.1 Management commitment to information security	ja	In ISMS-Politik und in Inf.-Sicherheits-Politik festgelegt; Dokumente Nr. 001 und 002
		A.6.1.2 Information security coordination	ja	In ISMS-Politik und in Inf.-Sicherheits-Politik festgelegt; Dokumente Nr. 001 und 002
...	...	...	...	...

9.3.2

Code of Practice ISO/IEC 27002

Der internationale Standard ISO/IEC 27002 (frühere Bezeichnung 17799), „Code of practice for information security management“, baut auf dem Standard BS 7799-1 auf und ist in seiner ersten Ausgabe (ISO/IEC 17799:2000) fast identisch mit diesem. Die inzwischen erweiterte zweite Ausgabe weist in Kapitel 4 auf die Notwendigkeiten sowie die grundlegenden Aspekte eines Risiko-Assessments hin. Da es sich bei dem Standard nach wie vor um ein Massnahmen-Regelwerk und nicht um einen Management-System-Standard handelt, ist die konkrete Ausführung eines Risiko-Managements darin nicht behandelt. Hingegen berücksichtigt die heutige Ausgabe ISO/IEC 27002 zusätzlich wichtige aktuelle Sicherheitsgebiete wie beispielsweise das „Information security incident management“.

Tabelle 9.13: Übersicht über ISO/IEC 27002

Regelwerk	ISO/IEC 27002:2005 (ex 1779:2005) Code of practice for information security management.
Herkunft	„British Standards Institute“ BS 7799-1, Gegenüber der vorherigen Ausgabe ISO/IEC 1779:2000 neu strukturiert, erweitert und aktualisiert. ISO/IEC 17799:2000 hatte geringfügige Abweichungen vom Standard BS 7799-1.
Einsatz-zweck	Massnahmen zum Erreichen und Aufrechterhalten eines zielorientierten Informationssicherheitsniveaus im Unternehmen.
Wichtige Merkmale	Umfasst 11 Sicherheitsbereiche mit insgesamt 39 Haupt-Kategorien und entsprechenden Massnahmen-Zielen. Zur Erfüllung dieser Massnahmen-Ziele stehen 133 Massnahmen (controls) zur Verfügung. Die Auswahl der Massnahmen soll aufgrund der Sicherheitsanforderungen erfolgen, u.a. basierend auf einer Risikobeurteilung und den Geschäftsanforderungen (z.B. gesetzlich, regulatorisch, vertraglich).

Die Kapitel des Dokuments der Ausgabe 27002 (ex 17799:2005) sind wie folgt gegliedert:

ISO/IEC
27002:2005

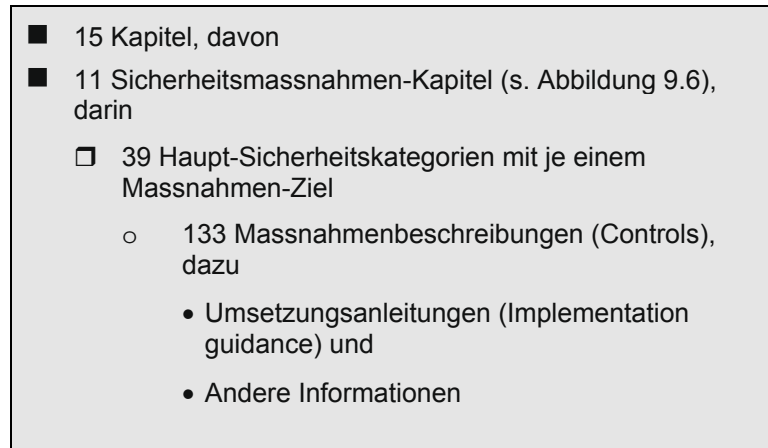


Abbildung 9.5: Gliederung im Standard ISO/IEC 27002

Die für konkrete Massnahmenziele und Massnahmen heranzuziehenden Kapitel 5 bis 15 von ISO/IEC 27002:2005 mit ihren 39 dazugehörigen Haupt-Sicherheitskategorien sind in Abbildung 9.6 dargestellt.

Dieser in hohem Masse generische Standard findet für kleine wie grosse Unternehmen Anwendung und hat in den letzten Jahren sicherlich die Informationssicherheit in starkem Masse geprägt.

Obligatorische
Überarbeitung
von ISO/IEC
27002

In der derzeit laufenden obligatorischen Überarbeitung in der ISO wird jedoch der Bedarf an einigen inhaltlichen Anpassungen sichtbar, um der aktuell gültigen „Best Practice“ wiederum gerecht werden zu können. Hingegen wird sich der grundlegende Aufbau des Standards, abgesehen von einigen notwendigen Ergänzungen und Anpassungen, in einer neuen Version wahrscheinlich wenig verändern.

5. Security Policy - Information Security Policy 6. Organizing Information Security - Internal Organization - External Parties 7. Asset Management - Responsibility for assets - Information classification 8. Human resources security - Prior to employment - During employment - Termination or change of employment 9. Physical and environmental security - Secure areas - Equipment security 10. Communications and operations management - Operational procedures and responsibilities - Third party service delivery management - System planning and acceptance - Protection against malicious and mobile code - Back-up - Network security management - Media handling - Exchange of information - Electronic commerce service - Monitoring	11. Access control - Business requirement for access control - User access management - User responsibilities - Network access control - Operating system access control - Application and information access control - Mobile computing and teleworking 12. Information systems acquisition, development and maintenance - Security requirements of information systems - Correct processing in applications - Cryptographic controls - Security of system files - Security in development and support processes - Vulnerability management 13. Information security incident management - Reporting information security events and weaknesses - Management of information security incidents and improvements 14. Business continuity management - Information security aspects of business continuity management 15. Compliance - Compliance with legal requirements - Compliance with security policies and standards - Information systems audit considerations
---	---

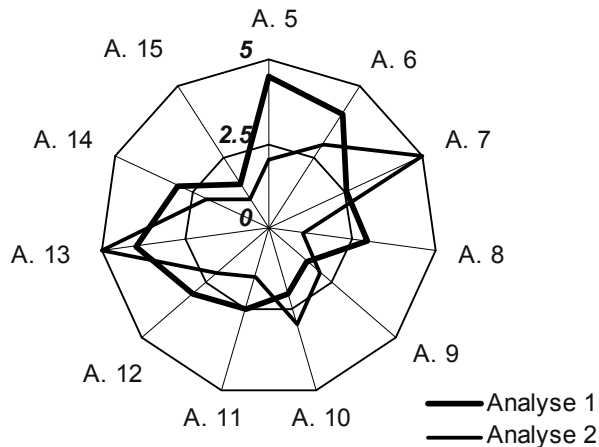
Abbildung 9.6: Kapitel und Kategorien in ISO/IEC 27002:2005

*Massnahmen-
katalog für
ISO/IEC 27001*

Neben der Verwendung als Massnahmenkatalog für den Standard ISO/IEC 27001 wird das Regelwerk ISO/IEC 27002:2005 (Code of Practice for Information Security Management) auch für Sicherheitsüberprüfungen verwendet. Dabei wird die Erfüllung (resp. Nichterfüllung) der Massnahmen-Ziele durch Massnahmen des Standards bewertet. Fälschlicherweise wird dieses Vorgehen, trotz der dabei fehlenden Bewertung der Assets (Schutzobjekte), oftmals als „Risiko-Analyse“ bezeichnet. In der in diesem Buch

verwendeten Risiko-Begrifflichkeit handelt es sich jedoch lediglich um eine anhand des Standards durchgeführte „Schwachstellen-Analyse“, da ausschliesslich das Vorhandensein von im Standard aufgeführten Massnahmen beurteilt wird.

Die Abbildung 9.7 zeigt das Beispiel einer solchen Schwachstellen-Analyse. Dabei resultiert die Bewertung pro Kapitel aus der Zusammenfassung der Detailbewertungen der Zielerfüllung pro Unterkapitel (Sicherheitskategorie) des Standards.



Legende:

Kapitel-Überschriften mit festgelegten Sicherheitszielen			
A. 5	Sicherheits-Politik	A. 11	Zugangs- und Zugriffskontrolle
A. 6	Organisation der Informationssicherheit	A. 12	Beschaffung, Entwicklung und Wartung von Informationssystemen
A. 7	Management von organisationseigenen Werten	A. 13	Management von Informationssicherheitsvorfällen
A. 8	Personelle Sicherheit	A. 14	Management der Kontinuität des Geschäftsbetriebes
A. 9	Physische und umgebungsbezogene Sicherheit	A. 15	Einhaltung von Vorgaben und Verpflichtungen
A. 10	Betriebs- und Kommunikationsmanagement		

Noten für Zielerreichung pro Kapitel: sehr gut = 5; keine = 0.

Abbildung 9.7: Schwachstellen-Analyse mit ISO/IEC 27002:2005

*Vergleich mit
anderen Organi-
sationen*

Dennoch genießt dieses Verfahren für bestimmte Anwendungsfälle hohe Akzeptanz. So kann es beispielsweise bei Vergleichen mit anderen Organisationen (Benchmarking) oder bei Vergleichen von IT-Infrastrukturen herangezogen werden. Natürlich darf dabei nicht vergessen werden, dass das Verfahren nicht die echten Restrisiken, sondern lediglich Mängel in der Compliance zu einem Massnahmen-Katalog aufzeigt.

9.3.3

Informationssicherheits-Risikomanagement mit ISO/IEC 27005

*Informationssi-
cherheits-RM-
Prozess*

Der Standard beschreibt in generischer Weise den Informationssicherheits-Risikomanagement-Prozess. Dieser Prozess ist weitgehend an den in der ISO in Entwicklung begriffenen allgemeinen Risikomanagement-Prozess (ISO 31000) und das im ISO bereits standardisierte Vokabular ISO IEC Guide 73:2009 angelehnt.

Tabelle 9.14: Übersicht über ISO/IEC 27005

Regelwerk	ISO/IEC 27005:2011 Information security risk management
Herkunft	ISO/IEC 27005:2011 Information wurde im ISO ursprünglich unter der Bezeichnung ISO/IEC 13335-2 entwickelt. Der im Juni 2008 erstmalig in Kraft gesetzte neue Standard ISO/IEC 27005 ersetzt zudem die bereits existierenden Technical Reports ISO/IEC TR 13335-3:1998 und ISO/IEC TR 13335-4:2000.
Einsatz- zweck	Unterstützt als Richtlinie die im Standard ISO/IEC 27001 vorgegebenen Konzepte für eine angemessene Umsetzung der Informationssicherheit basierend auf einem Risikomanagement-Ansatz.
Wichtige Merkmale	Vorgehen basierend auf einem Risikomanagement-Prozess, welcher sowohl auf den Risikomanagement-Standard ISO 31000 als auch auf den ISMS-Standard ISO/IEC 27001 ausgerichtet ist. Die Einzelschritte des Prozesses sind in der Form „Input“, „Action“, „Implementation guidance“ und „Output“ mit den wesentlichen Inhalten erläutert. Die Anhänge A bis E geben reichlich Anleitung für die Durchführung der einzelnen Prozessschritte.

Wie die Abbildung 9.8 zeigt, entspricht der Prozess im Wesentlichen dem in diesem Buch verwendeten generischen Risikoma-

nagement-Prozess. In der aktuellen Ausgabe ISO/IEC 27005:2011 wird die Kongruenz mit dem Risikomanagement-Standard ISO 31000 durch eine zusätzliche Abbildung, die den Prozess aus ISO 31000 veranschaulicht, bestärkt.

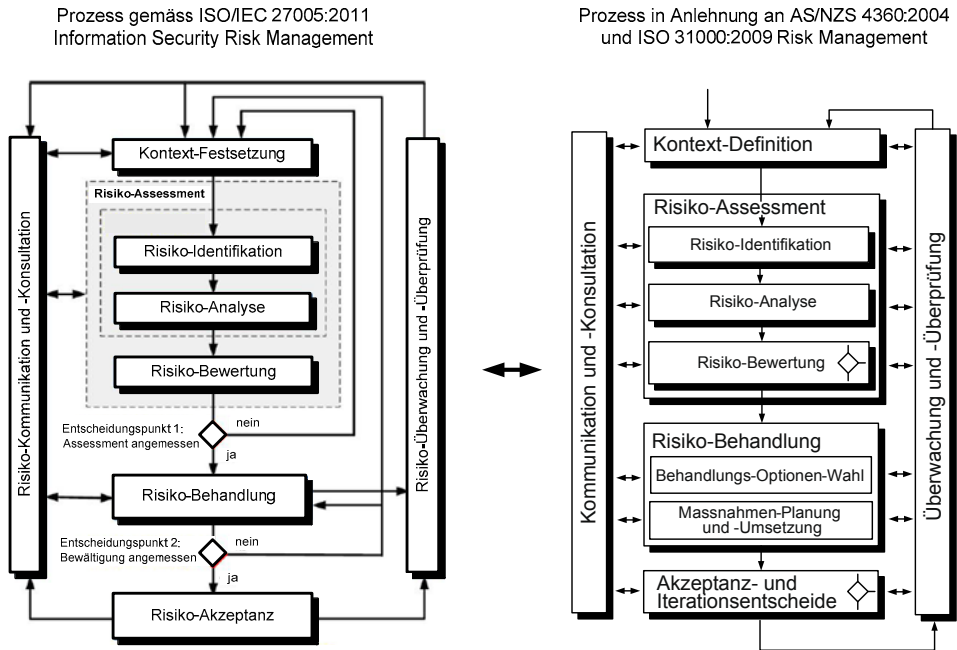


Abbildung 9.8: Risikomanagement-Prozess nach ISO/IEC 27005:2011

Interessant an diesem Standard sind vor allem die detaillierten Beschreibungen der Prozessschritte. Insgesamt können dem Standard 16 Prozessschritte der Struktur,

- Input
- Action
- Umsetzungs-Anleitung und
- Output

entnommen werden.

Ebenfalls sind die grundlegenden Kriterien für das Risikomanagement erläutert. Die Kriterien sind

- Risiko-Bewertungskriterien

- Impact-Kriterien
- Risikoakzeptanz-Kriterien und
- Notwendige Ressourcen

Anhang A

Hilfreich für die Durchführung des Informationssicherheits-Risikomanagement-Prozesses sind auch die informativen Ausführungen im Anhang des Standards. So erläutert Anhang A diejenigen Punkte, die zur Kontext-Definition (Scope and Boundaries) untersucht und definiert werden müssen.

*Anbänge B bis F
in ISO/IEC 27005*

Im Anhang B werden Erläuterungen über die „Identifikation“ und „Bewertung“ sowie über das „Impact Assessment“ gegeben. Der Anhang C beinhaltet eine Liste typischer Bedrohungen der Informationssicherheit. Der Anhang D zeigt Beispiele von Verletzlichkeiten im Hinblick auf die möglichen Bedrohungen sowie Methoden zur Analyse technischer Schwachstellen. Im Anhang E werden Ansätze gezeigt, wie das Risiko-Assessment mittels einer groben (high-level) Analyse und/oder mit einer detaillierten Analyse durchgeführt werden kann. Die grobe Analyse könnte in der Terminologie dieses Buches als Top-down-Analyse und die detaillierte Analyse als Bottom-up Analyse bezeichnet werden. Schliesslich werden im Anhang F die zu beachtenden Randbedingungen für den Massnahmeneinsatz angeführt. Solche Randbedingungen sind beispielsweise:

- Zeit
- Finanzen
- Technische Probleme
- Betriebliche Zwänge
- Kultur
- Ethische Zwänge
- Umwelt
- Gesetze
- Benutzerfreundlichkeit
- Personelle Voraussetzungen für Massnahmen
- Integration von neuen Massnahmen in ein bestehendes Umfeld

Insgesamt ist der Standard in seiner generische Form und seinen detaillierten Ausführungen bei der Gestaltung und Umsetzung eines Informations-Risikomanagement-Prozesses nützlich.

Wesentliche Ergänzung von ISO/IEC 27001

Damit ergänzt er in wesentlichen Aspekten des Risikomanagements den Standard ISO/IEC 27001. Eine punktgenaue Umsetzung des Standards, wie sie beispielsweise beim Standard ISO/IEC 27001 für die Erlangung einer Zertifizierung gefordert wird, ist jedoch beim Standard ISO/IEC 27005 weder beabsichtigt noch sinnvoll. Als Beispiel einer pragmatischen Anwendung des Standards sei auf den Abschnitt 10.1 verwiesen, in welchem die Anwendung im Rahmen eines IT-Sicherheitskonzepts gezeigt wird.

9.4

Framework zur Steuerung und Kontrolle der IT-Prozesse

CobiT® Framework

CobiT beansprucht, das Framework zur Steuerung und Überwachung der IT-Prozesse im Sinne der IT-Governance zu sein. Mit den auf die Version 3.0 folgenden Versionen 4.0 und 4.1 wurde inzwischen die Ausrichtung der Kontrollprozesse hinsichtlich einer wirksamen IT Governance im Rahmen der Corporate Governance vollzogen. Das Framework fokussiert die Prozesse auf die fünf IT-Governance-Kernbereiche:

- Strategic Alignment (strategische Ausrichtung der IT im Unternehmen)
- Value Delivery (Nutzensgenerierung durch die IT)
- Risk Management (Management von IT Risiken)
- Resource Management (IT Ressourcen Management)
- Performance Management (IT-Performance-Messungen)

In dem seit 12. April 2012 freigegebenen „CobiT 5“ soll insbesondere mit dem Governance Ziel, „Wertschöpfung“ die „Stakeholder“-Bedürfnisse an ein Unternehmen erfüllt werden. Dies soll durch „Nutzenrealisierung“, „Ressourcen-Optimierung“ und „Risiko-Optimierung“ bewerkstelligt werden [Isco2011]. Dazu wird das übergeordnete Ziel der Wertschöpfung auf entsprechende Unternehmens- und IT-Ziele heruntergebrochen.

Die für die Governance und das Management der IT massgeblichen Einzel-Frameworks der ISACA, CobiT 4.1, Val IT 2.0 und Risk IT sollen in ein gesamtes ganzheitliches Framework integriert und konsolidiert werden. Die Grundzüge von VAL IT und Risk IT sind in den Abschnitten 11.4.1 und 11.4.2 dieses Buches aufgezeigt. Ebenfalls sollen Bestandteile des „Information Technology Assurance Framework (ITAF)“ für die Prüfung von IT-

* CobiT = Control Objectives for Information and Related Technology

Prozessen und das „Business Model for Information Security (BMIS)“ der ISACA in das Framework CobiT 5 einbezogen werden. Das „Business Model for Information Security“ zeigt einen „systemischen“ Ansatz der wichtigen Zusammenhänge für die Informationssicherheit des Unternehmens mit seinen Prozessen und Technologien sowie der im Unternehmen agierenden Personen [Isbm2010]. Das „Governance-Modell“ von CobiT 5 verwendet die Mehrzahl der IT-Prozesse von CobiT 4.1. Auch wurden einige Prozesse aus CobiT 4.1 zusammengelegt, einige umbenannt und einige Prozesse, vor allem die Governance betreffend, zugefügt. Bemerkenswert ist die Empfehlung des „IT Governance Institut“, eine laufende Einführung von CobiT 4.1 vor einer Migration zu CobiT 5 erst abzuschliessen*.

9.4.1

CobiT 4.1

Nach dem kurzen Ausblick auf das zukünftige Framework CobiT 5 zurück zu CobiT 4.1, das als Framework für das Management der IT gilt und als solches die Anforderungen der IT-Governance bedient. In Abschnitt 5.4.3 wurde bereits gezeigt, wie die IT-Prozesse in den vier Prozessbereichen (CobiT-Domänen),

- PO:** Plan and Organize (Planung und Organisation)
- AI:** Acquire and Implement (Beschaffung und Implementierung)
- DS:** Deliver and Support (Lieferung und Unterstützung)
- ME:** Monitor and Evaluate (Überwachung und Beurteilung)

die Umsetzung der Geschäftsstrategie und der IT-Strategie steuern können.

Ebenfalls wurde gezeigt, wie mit Hilfe der Balanced Scorecard, sowie den Informationskriterien und den Kennzahlen die Erfüllung von Anforderungen und die Erreichung von strategischen Zielen messbar gemacht werden können.

Die Kontrolle[†] innerhalb der vier CobiT-Prozessbereiche erfolgt mittels 34 wichtiger IT-Prozesse, die sich in einem oder auch in

* www.itgovernance.com/changes_in_cobit5.pdf

† Die im Framework verwendete Formulierung „control over...“ deckt sowohl die managementmässige Steuerung als auch die Überprüfung und Überwachung mit entsprechenden Massnahmen ab.

mehreren der fünf IT-Governance Kernbereiche auswirken können. Pro IT-Prozess sind sodann jeweils mehrere detaillierte Kontrollziele (Control objectives) definiert. Das Zusammenspiel der IT-Prozesse, IT-Ressourcen und Informationskriterien in den vier Prozessbereichen ist anhand der Abbildung 9.9 nochmals veranschaulicht (vgl. [Gaul10], S. 19-20).

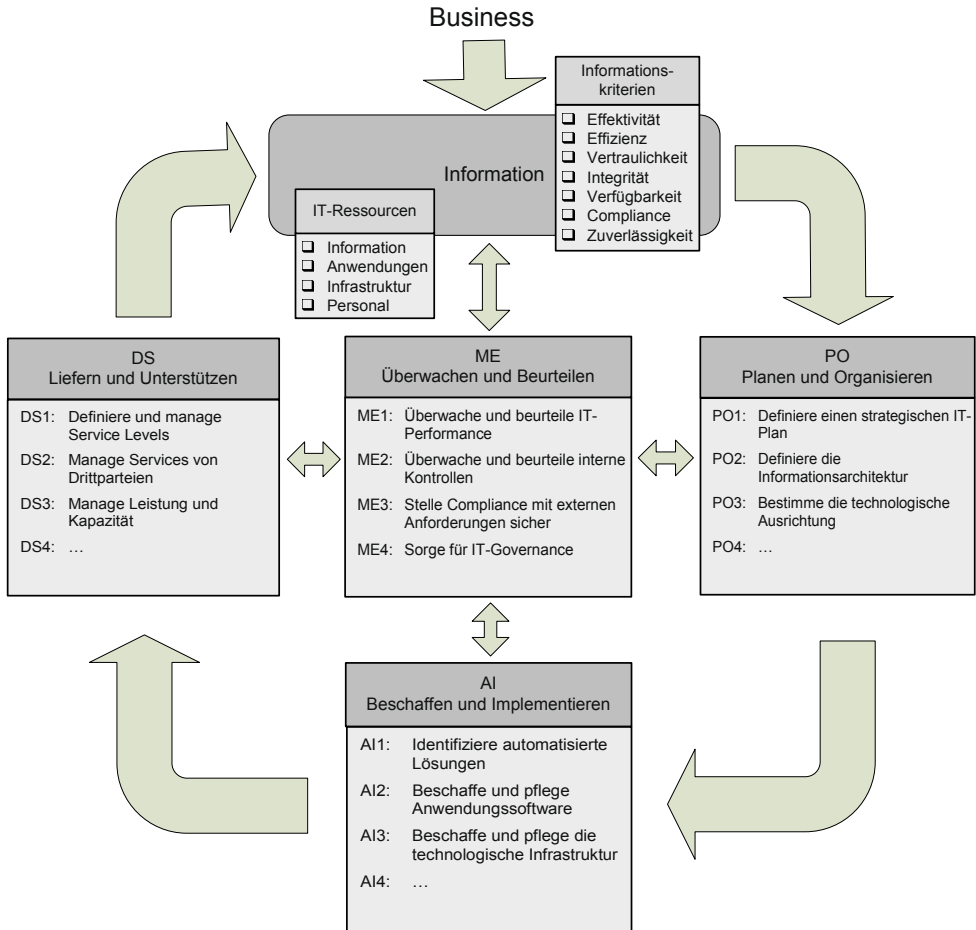


Abbildung 9.9: Zusammenspiel der IT-Prozessdomänen, IT-Ressourcen und Informationskriterien (vgl. [Gaul10], S. 19-20)

Tabelle 9.15: Übersicht über CobiT®

Regelwerk	CobiT® 4.1
Herkunft	Information Systems Audit and Control Foundation IT Governance Institute® USA. CobiT 3rd Edition in 2000, dann CobiT 4.0 in 2005 und CobiT 4.1 in 2007.
Einsatz-zweck	Geschäftsorientiertes "Framework" mit Kontrollzielen, das vor allem ein Leitfaden und eine Ausbildungs-Ressource für Chief Information Officers (CIOs), Senior Management, IT Management und Audit- und Revisionsfachpersonal darstellt.
Wichtige Merkmale	CobiT zeigt 34 IT-End-to-end-Prozesse in 4 Bereichen, die auf die IT-Governance fokussiert sind und mit denen die IT-Ressourcen verwaltet werden. Die IT-Prozesse werden anhand von Kontrollzielen gesteuert.

Anhand des CobiT -Würfels (s. Abbildung 9.10) ist das Framework nochmals anschaulich zusammengefasst, mit dem die IT-Ressourcen durch die IT-Prozesse gesteuert werden, um die IT-Ziele hinsichtlich der Geschäftsanforderungen zu erfüllen.

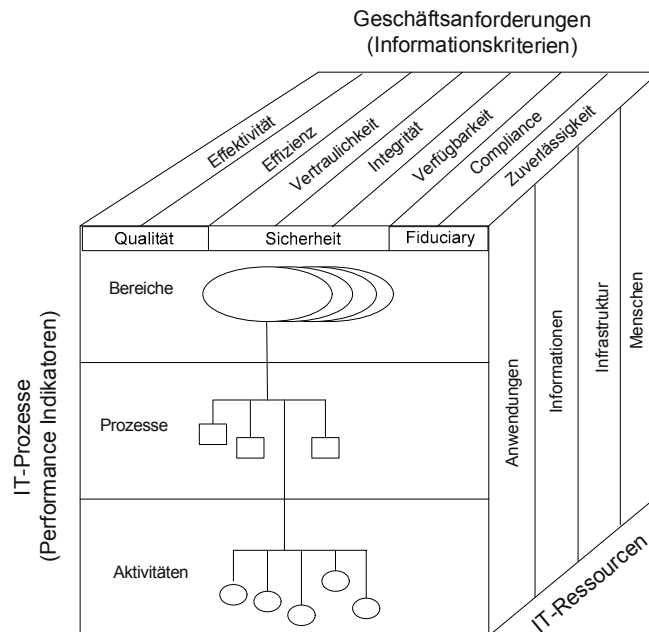


Abbildung 9.10: CobiT - Würfel (vgl. [Itgf07], S. 25)

Jeder Prozess in Abbildung 9.9 ist mit folgenden Informationen beschrieben:

- ☐ Prozessbeschreibung in einem Wasserfall-Modell (s. Abbildung 9.11)
- ☐ Detaillierte Kontroll-Ziele
- ☐ Informationskriterien, die durch den Prozess beeinträchtigt werden
- ☐ Durch Prozess adressierte Governance-Aspekte
- ☐ Betroffene Ressourcen-Kategorien
- ☐ Typische Charakteristiken, die den „Reifegrad“ des Unternehmens (Maturity Level) zum Ausdruck bringen
- ☐ Management Richtlinien

In den Management Richtlinien werden Input und Output der Prozesse sowie die Aktivitäten und Ziele mit ihren Metriken aufgezeigt.

Kontrolle über IT-Prozess

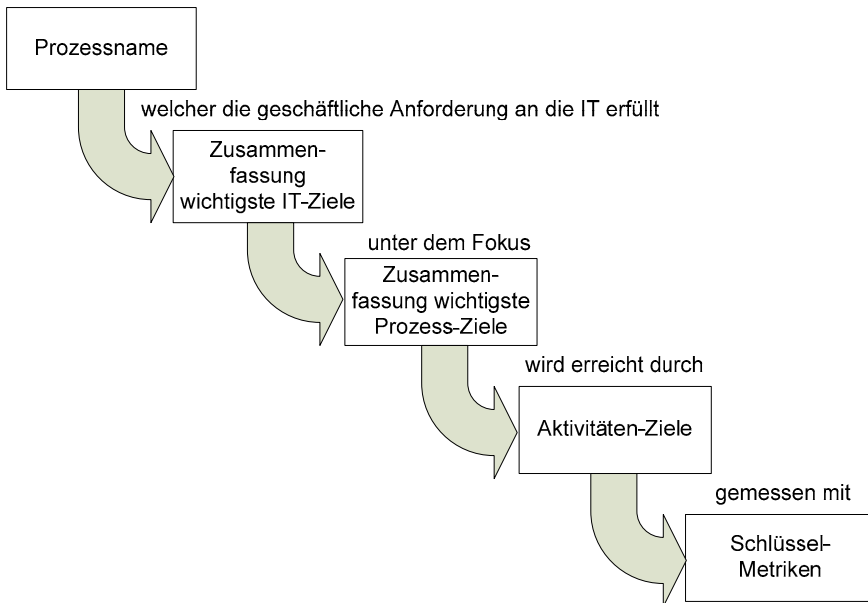


Abbildung 9.11: „Wasserfall“-Aufbau der Beschreibung eines CobiT-Prozesses

Das Prinzip ist nachfolgend an den beiden Prozessen PO 1 und PO 9 beispielhaft veranschaulicht.

*CobiT- Prozess
PO 1*

PO 1: Definition eines strategischen IT-Plans

- ❑ *Kontrolle über den IT-Prozess:*
Definition eines strategischen IT-Planes;
- ❑ *welcher die geschäftlichen Anforderungen an die IT erfüllt:*
Erhalt und Erweiterung der Geschäftsstrategie und der Governance-Anforderungen unter der Voraussetzung von Transparenz über Nutzen, Kosten und Risiken;
- ❑ *unter dem Fokus:*
Einbezug der Führungspersonen von IT und Geschäft in die Übersetzung von Geschäftsanforderungen in Dienstleistungsangebote und in die Entwicklung von Strategien zur Lieferung dieser Dienstleistungen in einer transparenten und effektiven Weise;
- ❑ *wird erreicht durch:*
 - Beanspruchung der verantwortlichen Führungspersonen bei der Ausrichtung der strategischen IT-Planung an den heutigen und zukünftigen Geschäftsanforderungen;
 - Verständnis des aktuellen IT-Leistungsvermögens
 - Bereitstellung eines Priorisierungsschemas, mit dem die Geschäftsanforderungen an die Geschäftsziele quantifiziert werden können;
- ❑ *gemessen mit:*
 - Prozentsatz der IT-Ziele im Strategieplan, die auf den strategischen Geschäftsplan zurückgeführt werden können;
 - Prozentsatz von IT-Projekten im IT-Projekt-Portfolio, die direkt auf die taktischen IT-Pläne zurückgeführt werden können;
 - Verzögerung zwischen der Überarbeitung des strategischen IT-Plans und den Überarbeitungen der taktischen IT-Pläne.

Anschliessend folgen die spezifischen und detaillierten Kontrollziele. So sind für jeden der 34 IT-Prozesse zwischen 3 und 30 detaillierte Kontrollziele aufgeführt. Die ersten beiden detaillierten Kontrollziele zu dem oben angeführten Prozess PO 1 sind beispielsweise:

*Detailliertes
CobiT-Kontroll-
ziel PO 1.1*

PO 1.1: IT Werte-Management

Zusammenarbeit mit den Geschäftsverantwortlichen, um sicherzustellen, dass das Unternehmens-Portfolio der IT-befähigenden Investitionen Programme mit soliden „Business Cases“ (Geschäftsnutzen) enthalten.

Erkennung, dass obligatorische, nachhaltige und beliebige Investitionen existieren, die sich in Komplexität, Freiheitsgrad und Zuordnung der Finanzmittel unterscheiden.

Die IT-Prozesse sollen die effektive und effiziente Lieferung der IT-Komponenten der Investitions-Programme bereitstellen und eine Frühwarnung über jegliche Plan-Abweichungen (einschliesslich Abweichungen von Kosten, Termin und Funktionalität) abgeben, welche die erwarteten Ergebnisse der Investitions-Programme beeinflussen könnten.

Die IT-Dienstleistungen sollen anhand gerechter und durchsetzbarer Service Level Agreements (SLAs) ausgeführt werden.

Die Zuständigkeiten zur Erreichung des Nutzens und der Einhaltung der Kosten sollen klar zugeordnet und überwacht werden.

Einrichtung von gerechten, transparenten wiederholbaren und vergleichbaren Bewertungen der „Business Cases“ einschliesslich der finanziellen Werte, sowie der Risiken hinsichtlich der Nichtlieferung von Leistungen oder der Nichterfüllung von Nutzererwartungen.

*Detailliertes
CobiT-Kontroll-
ziel PO 1.2*

PO 1.2: Ausrichtung der IT an dem Geschäft

Erstellung eines bi-direktionalen Prozesses für die Ausbildung und den wechselseitigen Einbezug in die strategische Planung, um die Ausrichtung und Integration von IT und Geschäft zu erlangen. Durch die Vermittlung zwischen Geschäft und IT-Zwängen können beispielsweise die Prioritäten gegenseitig vereinbart werden.

9.4.2

IT-Risikomanagement mit CobiT 4.1

Aus der Sicht des IT-Risikomanagements ist nachfolgend der CobiT-Prozess PO 9 aufgeführt:

*CobiT- Prozess
PO 9*

PO 9: Beurteilung und Steuerung der IT-Risiken

- ☐ *Kontrolle über den IT-Prozess:*
Beurteilung und Steuerung der IT-Risiken;
- ☐ *welcher die geschäftlichen Anforderungen an die IT erfüllt:*
Analyse und Kommunikation der IT-Risiken mit ihrem potentiellen Impact auf die Geschäftsprozesse und –ziele;
- ☐ *unter dem Fokus:*
Entwicklung eines Risikomanagement-Frameworks, welches in das Framework des Geschäfts- und des operationellen Risikomanagements, in die Risiko-Beurteilung, die Risiko-Milderung und die Kommunikation des Restrisikos integriert ist;
- ☐ *wird erreicht durch:*
 - Sicherstellung, dass das Risikomanagement gänzlich in die Managementprozesse, intern und extern, eingebettet ist und konsistent angewendet wird;
 - Durchführung von Risiko-Beurteilungen;
 - Empfehlung und Kommunikation der Risikobewältigungs-Aktionspläne;
- ☐ *gemessen mit:*
 - Prozentsatz von kritischen IT-Zielen, die mit einer Risikobeurteilung abgedeckt sind;
 - Prozentsatz identifizierter kritischer IT-Risiken mit einem entwickelten Aktionsplan;
 - Prozentsatz von zur Umsetzung genehmigten Risikomanagementplänen.

Wie am Beispiel des Prozesses PO 9 ersichtlich ist, wird beim Risikomanagement starkes Gewicht auf die Integration des IT-Risikomanagements in das Geschäfts-Risikomanagement gelegt. Dies kommt auch in den detaillierten Kontrollzielen zum Ausdruck, von denen nachfolgend vier der sechs Ziele des Prozesses PO 9 aufgezeigt sind:

*Detailliertes
CobiT-Kontroll-
ziel PO 9.1*

PO 9.1: IT-Risikomanagement Framework

Einrichtung eines IT-Risikomanagement-Frameworks, das auf das Unternehmens-Risikomanagement Framework ausgerichtet ist.

*Detailliertes
CobiT-Kontroll-
ziel PO 9.2*

PO 9.2: Erstellung des Risiko-Kontextes

Erstellung des Kontextes, innerhalb dessen das Risikobeurteilungs-Framework zur Sicherstellung angemessener Ergebnisse verwendet wird. Dieser soll die Bestimmung des internen wie auch des externen Kontextes beinhalten sowie das Ziel der Risikobeurteilung und die Kriterien, gegenüber derer die Risiken bewertet werden.

*Detailliertes
CobiT-Kontroll-
ziel PO 9.3*

PO 9.3: Ereignis-Identifikation

Identifikation von Ereignissen (wichtige und realistische Bedrohungen, welche eine signifikante, zutreffende Schwachstelle ausnützen), die einen potenziellen Impact auf die Ziele und den Betrieb des Unternehmens haben, einschliesslich der Aspekte des Geschäfts, der Regulative, der Gesetze, der Technologie, der Geschäftspartner, des Personals und des Betriebs.

Bestimmung der Eigenschaften des Impacts und der Verwaltung dieser Informationen.

Aufzeichnung und Verwaltung der relevanten Risiken in einem Risiko-Register.

*Detailliertes
CobiT-Kontroll-
ziel PO 9.4*

PO 9.4: Risiko-Beurteilung

Beurteilung der Wahrscheinlichkeit und des Impacts aller identifizierten Risiken auf wiederkehrender Basis unter Anwendung von sowohl qualitativen als auch quantitativen Methoden.

Die Wahrscheinlichkeit und der Impact der inhärenten Restrisiken sollen individuell, in der entsprechenden Kategorie, auf der Basis eines Portfolios bestimmt werden.

*Risiko-
Beurteilung*

Das Kontrollziel PO 9.4 schreibt sowohl qualitative als auch quantitative Methoden zur Risiko-Beurteilung vor, wobei CobiT für die Durchführung von qualitativen Risiko-Beurteilungs-

*Ganzheitliche
Betrachtung IT-
Leistungen*

Ansätzen ein reichhaltiges Instrumentarium ermöglicht, z.B. mittels Informationskriterien oder Kennzahlen. Hingegen stellt das CobiT-Framework bis anhin keine Anleitungen und Hilfsmittel zur Durchführung einer quantitativen Risiko-Analyse zur Verfügung.

CobiT bietet also in seiner Version 4.1 in erster Linie Prozesse, Leitlinien und Hilfsmittel zu einer ganzheitlichen Betrachtung der IT-Leistungen zur Erhaltung und Steigerung des Unternehmenswertes. Dabei spielt natürlich auch die Erfüllung von Informationssicherheits-Anforderungen eine grosse Rolle. Aus dieser Optik ist das durch CobiT empfohlene IT-Risikomanagement-Framework zur Erfüllung einer „good IT Governance“ zu verstehen.

9.5

BSI-Standards und Grundschatzkataloge

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat aus dem ursprünglichen IT-Grundschatzhandbuch durch laufende Erweiterungen und Ergänzungen, neben dem Katalog für Grundschatzmassnahmen, inzwischen Standards für ein „Information Security Management System“ (ISMS) und für die Risiko-Analyse entwickelt. Das IT-Grundschatzhandbuch ist 2005 in verschiedenen Bereichen umstrukturiert worden. Dabei sind die Beschreibung der Vorgehensweise nach IT-Grundschatz sowie die Informationen zum ISMS und zur Risiko-Analyse von den „IT-Grundschatz-Katalogen“ separiert worden. Die neue Dokumentenreihe ist wie folgt in Einzeldokumente aufgeteilt:

- ❑ **Standards zur Informationssicherheit**
 - **100-1:** Managementsysteme für Informationssicherheit (ISMS)
 - **100-2:** IT-Grundschatz-Vorgehensweise
 - **100-3:** Risikoanalyse auf der Basis von IT-Grundschatz
 - **100-4** Notfallmanagement
- ❑ **IT-Grundschatzkataloge** unterteilt in:
 - Vorspann
 - Schichtenmodell
 - Bausteinkataloge
 - Gefährdungskataloge und
 - Massnahmenkataloge

*Standard 100-1
für ISMS*

Der Standard 100-1 für das ISMS ist an den Standard ISO/IEC 27001 angelehnt. Seit Anfang 2006 können beim BSI Zertifizierung von „ISO-27001-Zertifikaten auf der Basis Grundschutz“ beantragt werden.

Zu einem ISMS gehören gemäss BSI folgende grundlegenden Komponenten [Bsim08], [Bsig08]:

- ☐ Management-Prinzipien
- ☐ Ressourcen
- ☐ Mitarbeiter
- ☐ IT-Sicherheitsprozess, welcher vor allem geprägt ist durch:
 - IT-Sicherheitsleitlinie,
 - IT-Sicherheitskonzept und
 - IT-Sicherheitsorganisation.

*IT-Sicherheits-
leitlinie*

In der „IT-Sicherheitsleitlinie“ (IT-Sicherheits-Politik) sind die IT-Sicherheitsziele und die Strategie zu ihrer Umsetzung dokumentiert; das „IT-Sicherheitskonzept“ und die „IT-Sicherheitsorganisation“ sind dabei die Werkzeuge der „Leitungsebene“ zur Umsetzung der IT-Sicherheitsstrategie.

*IT-Sicherheits-
konzept*

Das IT-Sicherheitskonzept bezieht sich in seinen Bewertungen und Massnahmendefinitionen auf die IT-Grundschutz-Kataloge des BSI. Bei den in den Grundschutzkatalogen enthaltenen Massnahmen handelt es sich sowohl um konkrete Implementierungshilfen zu den generischen Anforderungen aus ISO/IEC 27002 bzw. ISO/IEC 27001 als auch um zahlreiche technische Massnahmen für den sicheren Betrieb von typischen IT-Systemen und IT-Anwendungen. Eine genaue Anleitung zur Auswahl der Bausteine hilft dabei, alle sicherheitsrelevanten Aspekte zu berücksichtigen.

*IT-
Sicherheitsprozess*

Der **IT-Sicherheitsprozess** beinhaltet im Wesentlichen den folgenden Ablauf [Bsir08]:

*IT-
Strukturanalyse*

Nachdem der IT-Sicherheitsprozess initiiert worden ist, erfolgt eine IT-Strukturanalyse, die vor allem der Identifikation von Schutzobjekten und deren Abhängigkeiten untereinander dient. Der Sicherheitsprozess wird auf Zielobjekten (z.B. Systemen, Komponenten) durchgeführt. Im Rahmen der IT-Strukturanalyse werden somit die für den betrachteten IT-Verbund relevanten Schutzobjekte wie Informationen, IT-Anwendungen, IT-Systeme, Netze, Räume und Gebäude, aber auch die zuständigen Mitarbeiter ermittelt und dokumentiert. Zusätzlich müssen die Beziehungen und Abhängigkeiten zwischen den Schutzobjekten dargestellt werden.

*Schutzbe-
darf-
Feststellung*

*Modellierung
mit Baustei-
nen*

Die Erfassung von Abhängigkeiten dient dazu, die Auswirkungen von IT-Sicherheitsvorfällen auf die Geschäftstätigkeit zu erkennen, um dann angemessen reagieren zu können.

Nach der Strukturanalyse wird der Schutzbedarf (Impact) in drei ordinalen Stufen ermittelt; dieser orientiert sich an den möglichen Schäden hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität für die jeweiligen Geschäftsprozesse.

Mittels der IT-Grundschutzkataloge wird nun der analysierte IT-Verbund anhand der vorgegebenen Bausteine nachgebildet. Für die einzelnen Bausteine sind in den Grundschutzkatalogen typische Gefährdungslagen und Massnahmen-Empfehlungen vorgegeben.

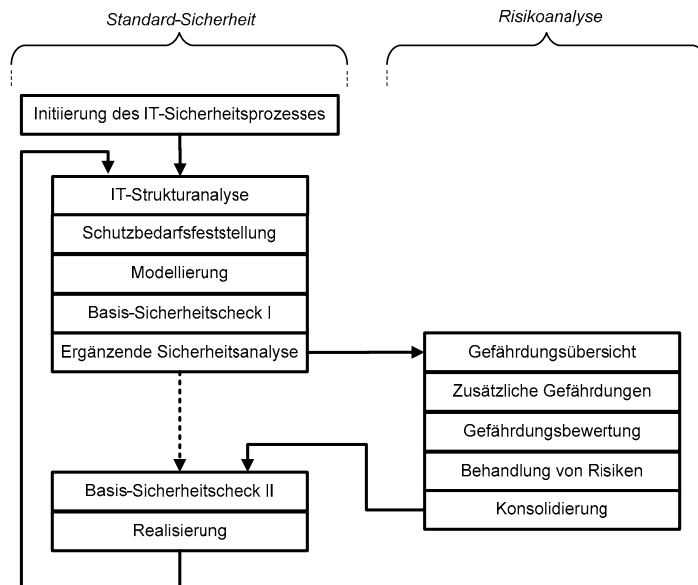


Abbildung 9.12 IT-Sicherheitsprozess der BSI [Bsir08]

*Basis-
Sicherheitschecks*

Wie die Abbildung 9.12 zeigt, werden im Verlaufe des IT-Sicherheitsprozesses sogenannte Basis-Sicherheitschecks* gemäss der IT-Grundschutz-Vorgehensweise durchgeführt. Dadurch wird mit Hilfe von Interviews jeweils festgestellt

* Der Basis-Sicherheitscheck dient einem schnellen Überblick über das Sicherheitsniveau in Bezug auf die Umsetzung des Grundschatzes in einem IT-Verbund.

*Handlungsbedarf
über IT-
Grundschutz
hinaus*

und aufgezeigt, welche Standard-Sicherheitsmassnahmen für den vorliegenden IT-Verbund bereits umgesetzt sind und wo noch Defizite bestehen.

Zeigt die Schutzbedarfs-Feststellung einen hohen oder sehr hohen Schutzbedarf hinsichtlich „Vertraulichkeit“, „Verfügbarkeit“ oder „Integrität“ oder können einzelne Zielobjekte (Schutzobjekte) mit den vorhandenen Bausteinen und Szenarien in den Katalogen nicht abgedeckt werden, dann wird das IT-Grundschutz-Sicherheitskonzept mit entsprechenden Gefährdungen (Bedrohungen) und Massnahmen ergänzt. Gefährdungen und Massnahmen, die in den Grundschutzkatalogen nicht aufgeführt sind, müssen somit noch analysiert und definiert werden.

*Eintrittswahr-
scheinlichkeiten
implizit berück-
sichtigt*

Die im BSI-Standard 100-3 beschriebene Risiko-Analysen-Methodik berücksichtigt die Eintrittswahrscheinlichkeiten nicht explizit, sondern lediglich implizit im Rahmen der Ermittlung und Bewertung von Gefährdungen.

9.6

Zusammenfassung

Zunehmend kommen für den Aufbau und den Erhalt der Informationssicherheit „Standard Regelwerke“, vor allem Grundschutz-Kataloge, zum Einsatz. Die Regelwerke existieren oft als nationale oder internationale Standards und erfahren so eine breite Abstützung, sowohl was ihre Erstellung als auch was ihre Anwendung betrifft. Viele der heute verfügbaren Standards entstanden aus weit verbreiteten Praktiken, den sogenannten „best Practices“. Bei dem mittels Grundschutz-Kataloge erreichbaren Basis-Schutz sind die spezifischen Sicherheitsbedürfnisse aufgrund erhöhter Risiken nicht abgedeckt. Es empfiehlt sich deshalb, einen kombinierten Ansatz von Grundschutz und risikobasierten Massnahmen zu wählen. Die Regelwerke berücksichtigen verschiedene Schwerpunkte. Anhand von Vergleichstabellen, können die Regelwerke miteinander verglichen werden. Die Vergleiche zeigen die Positionierungen und Überschneidungen der Regelwerke untereinander auf. Das CobiT-Regelwerk, in der im April 2012 freigegebenen 5.0 mit dem Governance-Ziel, „Wertschöpfung“, zeigt beispielsweise eine sehr hohe Anwendungsbreite, insbesondere was die Unternehmensprozesse betrifft. Die Standardreihe ISO/ICE 2700x liegt in der Anwendungsbreite unterhalb von CobiT, da sie vorwiegend auf die Informationssicherheit konzentriert ist. In der Version 4.1 von CobiT sind die IT-Prozesse und die Kontrollziele auf die IT-

Governance fokussiert. Hingegen ist das Regelwerk ISO/IEC 2700x tiefergehend auf die Informationssicherheit ausgelegt als CobiT und stellt einen zusätzlichen Standard (ISO/IEC 27005) zur Verfügung, der den Informations-Risikomanagement-Prozess im Einzelnen behandelt und wertvolle Hilfsmittel zur Risiko-Beurteilung aufzeigt.

Die neue Dokumentenreihe des deutschen BSI (Bundesamt für Sicherheit in der Informationstechnik) ist wie folgt in Einzeldokumente aufgeteilt:

Die Standards zur Informationssicherheit

- **100-1:** Managementsysteme für Informationssicherheit (ISMS)
- **100-2:** IT-Grundschutz-Vorgehensweise
- **100-3:** Risikoanalyse auf der Basis von IT-Grundschutz
- **100-4** Notfallmanagement

Die IT-Grundschutzkataloge unterteilt in:

- Vorspann
- Schichtenmodell
- Bausteinkataloge
- Gefährdungskataloge und
- Massnahmenkataloge

Der Standard 100-1 für das ISMS ist an den Standard ISO/IEC 27001 angelehnt. Seit Anfang 2006 können beim BSI Zertifizierung von „ISO-27001-Zertifikaten auf der Basis Grundschutz“ beantragt werden.

9.7

Kontrollfragen und Aufgaben

1. Nennen Sie Gründe, Grundschutzmassnahmen im Unternehmen einzusetzen.
2. Erklären Sie mit Worten ein Vorgehen, wie Sie feststellen können, dass bei bestehenden Grundschutzmassnahmen eine umfassende Risiko-Analyse notwendig ist.
3. Nennen Sie Informationskriterien bei CobiT.
4. Auf welche IT-Governance-Bereiche sind die CobiT-Prozesse und Kontroll-Ziele fokussiert?
5. Erläutern Sie die wesentlichen Merkmale der Risikobeurteilung anhand der BSI-Standards.

10

Methoden und Werkzeuge zum IT-Risikomanagement

Das Buch soll in erster Linie die Risiken und speziell die Informationssicherheits- und IT-Risiken aus der Perspektive des Unternehmens und der Governance behandeln. Deshalb sind in diesem Kapitel lediglich einige ausgesuchte Methoden und Werkzeuge behandelt, die im Rahmen des Informations-Risikomanagements eingesetzt werden; sie stehen somit für eine ganze Anzahl heute praktizierter Methoden und erhältlicher Werkzeuge. Bei der Behandlung in diesem Kapitel werden die Methoden und Werkzeuge jeweils an den Grundprinzipien eines Risikomanagement-Prozesses, wie er im Kapitel 3 zur allgemeinen Anwendung sukzessive aufgebaut wurde, reflektiert. Die Integration dieser Sub-Prozesse in die Unternehmensprozesse erfolgt im Teil D dieses Buches.

10.1

IT-Risikomanagement mit Sicherheitskonzepten

Die Erstellung eines IT-Sicherheitskonzepts ist immer dann angezeigt, wenn es bei Prozessen mit IT-Unterstützung oder bei IT-Systemen* darum geht, mit geeigneten Massnahmen die Risiken auf tragbare Restrisiken zu reduzieren und dabei sowohl die Bewertung als auch die Art und Weise der Bewältigung aufgezeigt und dokumentiert werden muss.

Funktion eines Risikomanagement-Prozesses

Mit definierten Abgrenzungen der Konzept-Gegenstände (z.B. IT-Systeme, Prozesse) und mit einem einbezogenen Risiko-Assessment erhält ein Sicherheitskonzept die Funktion eines Risikomanagement-Prozesses. Der Risikomanagement-Prozess wird dabei lediglich auf das Assessment und die Behandlung der Risiken im betreffenden Kontext (z.B. eines IT-Systems) zugeschnitten. Deshalb sieht der strukturelle Aufbau eines IT-Sicherheitskonzepts die konzeptionelle Einbindung der Sicher-

* Vgl. NIST Special Publication 800-18 [NIST 800-18]: Darin besteht ein IT-System aus einer definiert abgegrenzten Anzahl von Prozessen, Kommunikationen, Speicherungen und damit zusammenhängenden Ressourcen (einer Architektur).

	heits-Massnahmen in die verschiedenen IT-Prozesse, insbesondere in den System-Entwicklungsprozess, vor.
<i>Sicherheitsaspekte des Lebenszyklus eines Systems</i>	Das Sicherheitskonzept kann sich auf die Sicherheitsaspekte des gesamten Lebenszyklus eines Systems (z.B. Beschaffung, Entwicklung, Einführung, Betrieb und Entsorgung) oder auch nur auf einzelne Phasen (z.B. Entwicklung oder Betrieb) beziehen. Solche phasenspezifischen Sicherheitskonzepte sind dann sinnvoll, wenn einzelne Lebenszyklusphasen (z.B. Entwicklung, Migration und Einführung) in sich stark risikobehaftet sind.
<i>Neben Risiko-Bewältigung zusätzliche Anforderungen</i>	Die im Sicherheitskonzept neben der eigentlichen Risiko-Behandlung respektive -Bewältigung zusätzlich zu berücksichtigenden Anforderungen an die Sicherheitsmassnahmen sind: • Leistungsvorgaben (z.B. definiert mittels SLA) • Qualitätsanforderungen • Architektur-Vorgaben • Innerbetriebliche Weisungen • Innerbetriebliche Standards • Gesetzliche und regulative Vorgaben (Informationenschutz, Bankgeheimnis, Urheberrecht, Basel II usw.) • Kostenvorgaben
<i>Abwägung von Kosten, Nutzen und Wirksamkeit</i>	Wird das Sicherheitskonzept als Risikomanagement-Prozess verstanden, darf die Darstellung und Abwägung von Kosten, Nutzen und Wirksamkeit nicht fehlen. Gibt es doch, wie es Abbildung 10.1 zeigt, mehr oder weniger optimale Risiko-/Massnahmen-Kombinationen. Dies kann zur Folge haben, dass die Risiko-Analyse und -Bewertung mit unterschiedlichen Massnahmen-Konstellationen in mehreren Iterationen durchgeführt werden muss.

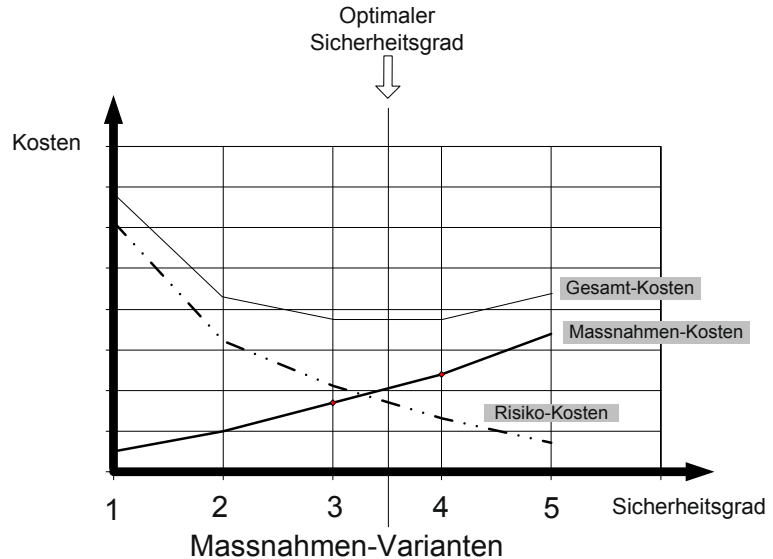


Abbildung 10.1 Kostenabwägung Risiko gegen Massnahmen

Organisatorische Umsetzungs- Aspekte

Letztlich kann die Sicherheit nur so gut sein, wie die konzipierten Massnahmen umgesetzt und kontrolliert werden. Das Sicherheitskonzept muss also die organisatorischen Aspekte für die Umsetzung der Sicherheitsmassnahmen enthalten (z.B. Verantwortlichkeiten, Termine und Kontrollen).

Insgesamt muss der Prozess der Erstellung und der Umsetzung eines Sicherheitskonzepts in die Risikopolitik, Sicherheits-Politik und in die Sicherheitsorganisation des Unternehmens eingebettet sein. So sollten sich die IT-Sicherheitskonzepte und die Prozesse ihrer Erstellung, Umsetzung und Überwachung vorzugsweise in den Risikomanagement-Prozess der IT und in den Risikomanagement-Prozess des Gesamtunternehmens integrieren.

Nützlichkeit

Ein derartiges Sicherheitskonzept erweist sich in folgenden Situationen als nützlich:

1. Bei der Entwicklung und Neueinführung eines IT-Systems;
2. Bei Änderungen an einem bestehenden IT-System;
3. In Situationen, wo bestehende Systeme auf ihre Sicherheit überprüft und die Restrisiken auf ein tolerables Mass reduziert werden müssen;
4. Für ganze Geschäfts- oder IT-Prozesse bei Outsourcing- oder Cloud-Computing-Vorhaben (s. Kapitel 14 und 16).

Orientierung an aktuellen Risiken

Der grosse Vorteil eines solchen Sicherheitskonzepts gegenüber einem „Baseline-Verfahren“ ist, dass die Risiko-Ermittlung und die Massnahmen-Bestimmung am realen Objekt konkret vorgenommen werden kann und sich damit die Massnahmen an den aktuell vorhandenen Risiken orientieren.

In Anlehnung an den elementaren Aufbau eines Risikomanagement-Prozesses kann der folgende Aufbau eines Sicherheitskonzepts die oben skizzierten Anforderungen erfüllen (s. Abbildung 10.2).

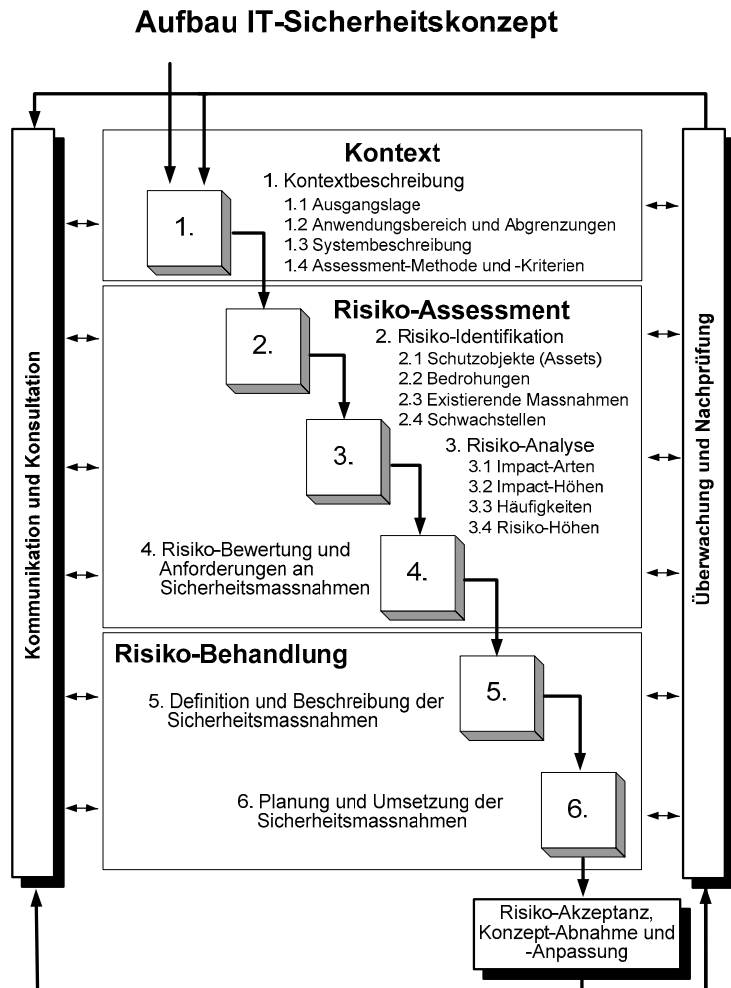


Abbildung 10.2: Aufbau IT-Sicherheitskonzept als RM-Prozess

Zudem wird mit dem Sicherheitskonzept das aufgrund von Compliance- oder Zertifizierungs-Anforderungen nachzuweisende Risikomanagement am betreffenden Objekt direkt durchgeführt und die konzipierten Massnahmen mit einem überprüfbaren Umsetzungsplan umgesetzt. Insbesondere die Kapitel 3 bis 6 eines solchen Sicherheitskonzepts werden vorzugsweise in mehreren Iterationen erstellt, da die Bestimmung der „tragbaren“ Restrisiken von den Anforderungen an die Sicherheitsmassnahmen sowie den bereits ein- und umgesetzten Massnahmen abhängig ist.

*Sechs Kapitel
eines IT-
Sicherheits-
konzepts*

Kapitel eines IT-Sicherheitskonzepts

Kapitel 1: Kontextbeschreibung

Kapitel 2: Risiko-Identifikation

Kapitel 3: Risiko-Analyse

Kapitel 4: Risiko-Bewertung und Anforderungen an Sicherheitsmassnahmen

Kapitel 5: Definition und Beschreibung der Sicherheitsmassnahmen

Kapitel 6: Planung und Umsetzung der Sicherheitsmassnahmen

Abbildung 10.3: Aufbau eines IT-Sicherheitskonzepts

In den folgenden Abschnitten 10.1.1 bis 10.1.7 werden diese sechs Kapitel eines Sicherheitskonzepts mit ihren Inhalten und ihren Erstellungsprozessen behandelt.

10.1.1

Kapitel „Kontextbeschreibung“

Um die Risikosituation im Kontext des Unternehmens treffend beurteilen zu können und um vergleichbare Voraussetzungen sowohl für das Vorgehen als auch für die Resultate von Risiken und Massnahmen zu schaffen, sind in der Kontextbeschreibung eine Vielzahl von Informationen zu eruieren und festzuhalten (s. Abbildung 10.4). Selbstverständlich können bei Sicherheitskonzepten mit ähnlichen Kontext-Hintergründen auf andere oder allgemeine Beschreibungen und Konzepte verwiesen werden, um nicht unnötigen Ballast in diesem Kapitel wiederholt zu dokumentieren.

Ausgangslage

Für das Verständnis sowohl des geschäftlichen als auch des organisatorischen Umfelds für das im Sicherheitskonzept behandelte System, wird am Anfang der Kontextbeschreibung die

Ausgangslage mit allen dazu notwendigen Informationen beschrieben.

Kontext

Kapitel 1: Kontextbeschreibung

1.1 Ausgangslage

- Allgemeines, Absichten, Zweck, Zielsetzungen
- Einflüsse und Abhängigkeiten intern und extern (z.B. organisatorische Zusammenhänge, vertragliche Bedingungen, zu beachtende Regulative)
- Wichtige Anforderungen (z.B. durch Geschäfts- und Support-Prozesse, terminliche Anforderungen)
- Bezeichnung der Auftraggeber und sonstige Verantwortlichkeiten (z.B. nominierter System-Owner)

1.2 Anwendungsbereich, Abgrenzungen und Einschränkungen

- Anwendungsbereich
- Abgrenzungen
- Restriktionen
- Randbedingungen

1.3 Systembeschreibung

- Verwendete Plattformen und Infrastruktur
- Systemlokalitäten und grobe Systemanordnung
- Systemanforderungen
- Systemfunktionen
- Abläufe, Prozesse
- Komponenten, Teilsysteme
- Standard-Produkte
- Konfigurationen
- Netzeinbindung und Kommunikations-Matrix (s. Abbildung 10.5)
- Schnittstellen (technisch, organisatorisch, extern, intern, etc.)
- Graphische Darstellungen

1.4 Assessment-Methoden und -Kriterien

- Assessment-Methode
- Risikoarten und Sicherheitsziele (z.B. Prozessrisiken, Verfügbarkeits- und Integritäts-Ziele)
- Impact-Kriterien und Schadensmetrik
- Bewertungskriterien und -masstäbe (z.B. Risikomatrix, Dringlichkeitsstufe)
- Akzeptanzkriterien (z.B. Akzeptanzlinie)

Abbildung 10.4: Wichtige Inhalte im Kapitel 1 eines IT-Sicherheitskonzepts

Für dieses Verständnis fragen wir, was der Zweck und die Ziele des zu behandelnden Systems sind. In welchem grösseren Kontext (z.B. Geschäftsfunktionen, Eigentums- und Vertragsverhältnisse) das System steht, wer für was verantwortlich ist. Auch werden die ganz besonderen Anforderungen aus Geschäfts- und Anwendersicht sowie die Einschränkungen und Rahmenbedingungen bereits am Anfang dokumentiert und die wichtigen Termine (Milestones) festgehalten.

Anwendungsbereich, Abgrenzungen und Einschränkungen

Mit der Festlegung des **Anwendungsbereichs, der Abgrenzungen und Einschränkungen** wird möglichst genau spezifiziert, für was das Sicherheitskonzept Gültigkeit haben soll. Dazu gehören beispielsweise die Benennung des Systems oder des Prozesses, die organisatorischen Abgrenzungen und Schnittstellen sowie die „Lifecycle“-Phase, für die das Sicherheitskonzept angefertigt werden soll.

Systembeschreibung

Zur wirklichkeitsnahen Darstellung der Zusammenhänge in einem IT-Sicherheitskonzept, aus der u.a. die Assets und Risiken abgeleitet werden können, gehört eine **Systembeschreibung**. Die Systembeschreibung muss in übersichtlicher Weise die für ein Risiko-Assessment und eine Massnahmen-Gestaltung massgeblichen Informationen und Zusammenhänge aufzeigen.

Sicherheitsrelevante Aspekte des Systems

Mit anderen Worten erläutern die Beschreibungen und Darstellungen die sicherheitsrelevanten Aspekte des Systems. Eine solche Darstellung ist beispielsweise die Kommunikations-Matrix, welche die notwendigen Kommunikations-Verbindungen des Systems mit anderen Systemen aufzeigt (s. Abbildung 10.5).

Für tiefergehende Beschreibungen und Darstellungen ist es sinnvoll, auf die entsprechenden Systemunterlagen zu verweisen (Grobkonzepte, Detailkonzepte, Betriebskonzepte und Handbücher.)

Zugriff von	Zugriff auf	Protokoll	Port	Zugriffsart / Client
Zugriff aus dem Internet in die „Demilitarisierte Zone“				
Internet	E-Gateway	HTTPS	443	Web-Browser
Administrationszugriffe aus der „Internen Zone“ in die „Demilitarisierte Zone“				
Applikations-Betreuer	E-Gateway	APICS	6390	Administrations-Client
		SSH	22	Applikations-Betreuer
Datei-Transfer zwischen I-Prozess und E-Gateway				
I-Prozess	E-Gateway	FTP	6370	I-Prozess
E-Gateway	I-Prozess	FTP	1366	E-Gateway
Zugriff von E-Gateway auf die Authentifikations-Mittel				
E-Gateway	Authentifikations-Server	UDP	5500	Authentifikations-Client des E-Gateway
		TCP	5510	

Abbildung 10.5: Beispiel einer Kommunikations-Matrix zur Firewall-Freischaltung

Da es bei einem Sicherheitskonzept mit eingeschlossenem Risiko-Assessment auch darum geht, den Zusatzaufwand für die Sicherheit und das Mass der Risiko-Reduktion zu veranschaulichen, empfiehlt es sich, das System mit den bereits vorhandenen Massnahmen (z.B. Grundschutzmassnahmen) darzustellen.

Assessment-Methoden und -Kriterien

Für die Durchführung des Risiko-Assessments werden im Abschnitt **Assessment-Methoden und -Kriterien** die anzuwendenden Methoden sowie die wesentlichen Kriterien zur Einschätzung, Bewertung und allfälligen Akzeptanz der Risiken angeführt oder auf die entsprechenden Festlegungen in Policy-Dokumenten verwiesen.

Solche Festlegungen, die vor allem bei der Risiko-Analyse und bei der Risiko-Bewertung gebraucht werden, sind beispielsweise die Risiko-Matrix mit eingezeichneter Akzeptanzlinie und die Schadenseinstufungstabelle, wie sie in Abschnitt 2.6 dieses Buches eingehend behandelt wurden.

10.1.2

Kapitel „Risiko-Assessment“

Risiko- Identifikation

Die **Risiko-Identifikation** als erster Schritt des Risiko-Assessments beginnt meist mit einem Aufsuchen und Einordnen der Schutzobjekte (Assets) in einer Asset-Liste.

Die Abgrenzung, die bereits in der Kontextbeschreibung definiert wurde, wird nochmals überdacht und festgehalten. So werden in diesem Schritt diejenigen Schutzobjekte, die anderweitig bereits analysiert wurden (z.B. eine bereits vorhandene Rechenzentrums-Infrastruktur), für ein erneutes Risiko-Assessment entsprechend markiert oder ausgeklammert. Selbstverständlich sind die bereits identifizierten und analysierten Risiken entsprechend ihres Einflusses auf die neu zu analysierende Risikosituation entsprechend zu berücksichtigen. Auch sollten an den Schnittstellen des Assessment-Bereichs geeignet zusammengefasste Schutzobjekte für den Aussenbereich definiert werden, da ein zu beurteilendes IT-System auch andere, ausserhalb des Assessment-Bereichs befindliche Systeme bedrohen kann.

Bei der Erstellung der Asset-Liste (auch unter dem Begriff Asset-Register bekannt) kann bereits eine wesentliche Vorarbeit für die spätere Risiko-Identifikation und Risiko-Analyse geleistet werden, indem die Assets aufgrund ihrer Abhängigkeiten in Asset-Typen eingeteilt und aufgelistet werden. Die Abbildung 10.6 veranschaulicht die Erstellung einer Asset-Liste anhand der Verschachtelung der Assets in einer typischen IT-Umgebung. Zu den technisch verschachtelten Assets kommen noch die auf alle Assets einwirkenden Asset-Typen „Personal“ und „Organisation“.

Bei der Risiko-Identifikation der meist sehr abstrakten Assets der Informations-Sicherheit geht es, neben der Erfassung der Assets und der darauf einwirkenden Gefahrenquellen auch darum, die relevanten Kausalketten, ausgehend von den Ursachen über die Auswirkungen bis hin zu den Konsequenzen für die Betroffenen (z.B. Unternehmen) darzustellen. So sind die „Unterstützenden Assets“ (z.B. Hardware) für die Analyse der Bedrohungsauswirkung auf die „Primären Assets“ (z.B. Endbenutzer-Services) wichtig, auch wenn der an ihnen anfallende Schaden (z.B. Ersatzkosten) vernachlässigbar sein sollte.

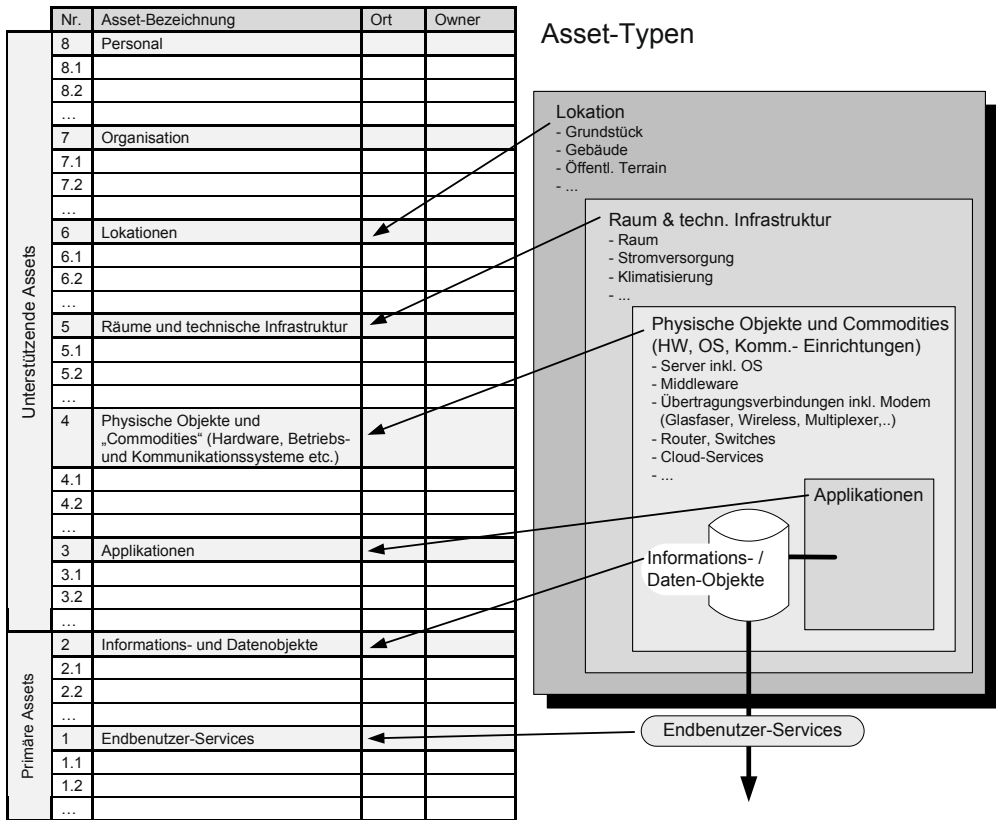


Abbildung 10.6 Einordnung der Assets in das Asset-Register

Ein weiterer wichtiger Aspekt bei der Erstellung der Asset-Liste ist die Wahl der richtigen „Granularität“ bei der Bestimmung der Assets. Dabei gilt der Grundsatz:

Grundsatz für Granularität der Assets

Praxistipp:

Im Hinblick auf die Analyse von Bedrohungen, Schwachstellen, Schadensauswirkungen und Massnavigengestaltungen soll die Festlegung der Assets „so grob wie möglich“ und „so fein wie nötig“ vorgenommen werden.

Die Abbildung 10.7 zeigt, welche Inhalte in das Kapitel 2, „Risikoidentifikation“, gehören. Bevor im nächsten Kapitel die Risiken in ihrer Höhe bestimmt werden können, sind im Kapitel 2 noch die für die Assets relevanten Bedrohungen sowie die bereits existierenden Massnahmen und die für eine Risiko-Exponierung der Assets vorhandenen Schwachstellen zu beschreiben.

Kapitel 2: Risiko-Identifikation

2.1 Schutzobjekte (Assets)

- ☐ Lokationen, d.h. Ort des IT-Einsatzes mit Relevanz für entsprechende Bedrohungen (z.B. Wasser, Erdbeben, gesetzgeberische Eigenheiten)
- ☐ Räume und umgebende Infrastruktur
- ☐ Physische Objekte und Commodities (z.B. Hardware, hardwarenahe Software wie Betriebs- oder Kommunikationssoftware)
- ☐ Applikationen (z.B. Legacy-Software)
- ☐ Informationen und Daten-Objekte (z.B. Personal-, Kreditkarten- oder Bankinformationen als Transaktionsdaten, Dateien oder Dokumente)
- ☐ Endbenutzer-Services (Lieferergebnis der Applikation für Endbenutzer (z.B. ausgeführte Transaktionen))

2.2 Bedrohungen

Für Assets und zu beurteilende Risikoarten relevante Bedrohungen

- Anhaltspunkte für typische Informationssicherheits- und IT-Bedrohungen sind in den Anhängen A.1 und A.2 dieses Buches sowie im Standard ISO/IEC 27005, Annex C zu finden.

2.3 Existieren Massnahmen

Für Assets und Bedrohungen bereits vorhandene Massnahmen.

2.4 Schwachstellen

Schwachstellen, die bei den vorhandenen Asset aufgrund der Bedrohungen Risiken zulassen.

- Beispiele für typische Informationssicherheits- und IT-Schwachstellen sind im Standard ISO/IEC 27005, Annex D zu finden und können unter Bezug des Standards ISO/IEC 27002, der „CobiT Security Baselines“, der „BSI Grundschutzkataloge“ oder des Datenschutzgesetzes eruiert werden.
- Die Schwachstellen können auch mittels analytischer Suchverfahren (s. Abschnitte 10.3 bis 10.5) oder durch Tests ermittelt werden.

Abbildung 10.7: Wichtige Inhalte im Kapitel 2 eines Sicherheitskonzepts

10.1.3

Kapitel „Risiko-Analyse“

Im Kapitel 3 eines IT-Sicherheitskonzepts wird die „Risiko-Analyse“ bezogen auf die identifizierten Schutzobjekte beschrieben. Die Risiko-Analyse liefert als Ergebnis die Höhe des Risikos entweder in qualitativen, quantitativen oder semi-quantitativen Werten. Die für die Risiko-Analyse relevanten vorgegebenen Kriterien wurden bereits im Kapitel der Kontextbeschreibung dokumentiert. Die Inhalte die im Kapitel 3 zum Thema „Risiko-Analyse“ dokumentiert werden sollen, sind in Abbildung 10.8 grob zusammengefasst.

Kapitel 3: Risiko-Analyse

3.1 Impact-Arten

Auswahl der für das Risiko relevanten Impact-Arten

- Direkter finanzieller Verlust
- Schädigung der geschäftlichen und wirtschaftlichen Interessen
- Beeinträchtigung personelle Sicherheit
- Nichteinhaltung gesetzlicher und regulativer Verpflichtungen
- etc.

3.2 Impact-Höhen

Einschätzung anhand der vorgegebenen Schadens-Einstufungskriterien (z.B. Schadenseinstufungstabelle)

3.3 Häufigkeiten

Einschätzung anhand der vorgegebenen Häufigkeits-Einstufungsmetrik (z.B. Risikomatrix mit Häufigkeits-Metrik)

3.4 Risiko-Höhen

Risiko-Bestimmung gemäss vorgegebenem Risikobestimmungsverfahren (z.B. Risikomatrix mit ordinalen Werten)

Abbildung 10.8: Inhalte im Kapitel 3 eines Sicherheitskonzepts

Die Abbildung 10.9 zeigt das Beispiel der in einem sogenannten „Risiko-Register“ festgehaltenen Identifikation und Analyse von Informationssicherheitsrisiken. Zur Spalte der Bedrohungen im Risiko-Register gilt zu erwähnen, dass für die Analyse der Häufigkeit eines Schadens die Schwachstellen bezogen auf das „Asset“ ermittelt werden müssen, um den tatsächlichen Einfluss der Bedrohung einschätzen zu können. Die für die „Primären Assets“ relevanten „Unterstützenden Assets“ sowie die bereits vorhandenen Massnahmen, Bedrohungen und Schwachstellen können in einer separaten Tabelle aufgeführt und bei der Risiko-Analyse entsprechend berücksichtigt werden. Die an jedem einzelnen

Risiko beteiligten „Unterstützenden Assets“ können aber auch in einer zusätzlichen Spalte des Risiko-Registers registriert werden, was der nachfolgenden Gestaltung der Massnahmen dienlich ist.

Identifikation						Analyse							
Nr.	Asset	Risikobezeichnung	Spezifische Bedrohung *)	Schwachstellen	Schadensszenario	Schaden		Informations-Kriterium			Häufigkeit	Risiko **) (Risiko-Rating gemäss Risiko-Matrix)	
						s. klein (0) klein (1) mittel (2) gross (3) s. gross(4)	Wiederherstellungskosten						
								Imageverlust	Direkter finanzieller Schaden	Verfügbarkeitsverlust			Vertraulichkeitsverlust
1.1	Zahlungsverkehr E-Banking	Betrug an Kundenvermögen	Maskerade einer Benutzer-Identität	Unachtsamkeit Benutzer	Diebstahl Kunden-Credentials mittels Phishing-Attacke		4	3		x	x	3	a
1.2		Ausspähen Bankdaten		Schwaches Authentisierungsverfahren			4	3		x		2	a
1.3		Lahmlegen E-Banking	Denial-of-Service-Attacke	keine technischen und vorsorglichen Massnahmen	gezielte Blockade des Internet - Zugangs mittels Distributed Denial-of-Service-Attacke	2	3	3	x		2	b	
1.4		Falschüberweisungen	Softwarefehler	Verfahren für Erstellung und Testen der Software nicht anforderungsgerecht.	Sporadische Verfälschungen von Überweisungsdaten infolge schlecht ausgetesteter Software-Release	2	4	4		x		2	a
*) Zur Bestimmung der Häufigkeit ist die Analyse der auf das Asset bezogenen Schwachstellen notwendig, welche der Bedrohung eine Schadensauswirkung erlauben.													
**) a: hohes Risiko; b: mittleres Risiko; c: geringes Risiko.													

Abbildung 10.9: Beispiel „Identifikation“ und „Analyse“ im Risiko-Register

Es stellt sich nun noch die Frage, wie die Werte für ein solches Risiko-Register in pragmatischer Weise ermittelt werden können?

Szenario-Analyse

Dafür bietet sich unter den vielfältig möglichen Methoden vor allem die „Szenario-Analyse“ mit „Experten-Befragung“ an (s. Abschnitt 3.7.2). Diese Methode in einem „Bottom-up-Verfahren“,

d.h. von den Ursachen zu den Auswirkungen hin, durchzuführen, bringt meist unmittelbar auch die Erkenntnis für die zur Risikomilderung geeigneten präventiven Massnahmen.

Natürlich können zusätzliche Methoden und anspruchsvollere analytische Methoden (z.B. „Failure Effekt und Ausfall-Analyse“, „Fehlerbaum-Analyse“, s. Abschnitte 10.3 bis 10.5) zusätzlich wichtige Risiko-Zusammenhänge und Schwachstellen in den Systemen und Prozessen aufzeigen.

Einstufungstabelle

Für einen pragmatischen Ansatz zur Einschätzung der Risiken, die meist mit einem knappen Zeitbudget durchgeführt werden muss, sind im Anhang 3 dieses Buches einige hilfreiche Einstufungstabellen zusammengestellt (Tabellen A.3.2, A.3.3, A.3.4 und A.3.5). Die Vorschriften und Kriterien zur Verwendung eines Verfahrens werden vorzugsweise in einem entsprechenden Politikpapier vorgegeben.

Praxistipp:

Gerade bei einer vollständigen Risiko-Analyse mit ausgefeilten Analyse-Verfahren ist es wichtig, dass keine Pseudo-Genauigkeiten bei den Risiko-Einschätzungen vorgetäuscht werden.

Nachdem mit den weiteren Kapiteln 4 bis 6 des Sicherheitskonzepts die Definition, Konzeption und Umsetzung der Massnahmen ausgearbeitet wurden, empfiehlt es sich, sowohl die Risiken vor als auch nach der Massnahmenumsetzung in einem Risiko-Register am Ende des Kapitels 3 aufzuzeigen.

Aufgrund der Anforderungen kann es auch angezeigt sein, anstelle einer kompletten Risiko-Analyse, lediglich eine Impact-Analyse oder eine Schwachstellen-Analyse durchzuführen. Impact-Analysen werden beispielsweise bei sehr seltenen Ereignissen mit hohem Schadensausmass, z.B. im Rahmen des Kontinuitätsmanagements, durchgeführt.

10.1.4

Schwachstellen-Analyse anstelle einer Risiko-Analyse

Oft ist es schwierig, die Impact-Analyse (Schadensausmass-Analyse) durchzuführen, da die Schutzobjekte nicht in einer bewertbaren Form bekannt sind. So ist es bei IT-Infrastruktur-Einrichtungen manchmal gar nicht möglich, die Werte der Schutzobjekte abzuschätzen (z.B. bei zu übertragender Information in Übertragungsnetzen).

In solchen Fällen kann oft eine Schwachstellen-Analyse den Zweck erfüllen. Die Schwachstellen-Analyse wird meist auf der Basis bestehender Grundschutzmassnahmen (Baseline Security Standards) durchgeführt. Als Schwachstelle kann dann eine ungenügend realisierte Grundschutzmassnahme gelten. Natürlich muss die Grundschutzmassnahme für eine Bedrohung des Schutzobjekts relevant sein.

Anhand unseres Risiko-Modells (s. Abbildung 10.10) lässt sich eine Schwachstelle wie folgt definieren:

*Definition
Schwachstelle*

Eine Schwachstelle ist eine fehlende oder ungenügend vorhandene, für das Schutzobjekt (Asset) relevante Massnahme.

Eine der wesentlichen Zweckbestimmungen, eine Risiko-Analyse durchzuführen, insbesondere im Zusammenhang mit einem Sicherheitskonzept, ist die Bestimmung von Sicherheitsmassnahmen. Eine Massnahmenbestimmung aufgrund einer Schwachstellenanalyse vorzunehmen, ist eine nützliche Alternative, insbesondere wenn aus den (ggf. aggregierten) Risiken nicht ohne weiteres auf die Platzierung der Massnahmen geschlossen werden kann.

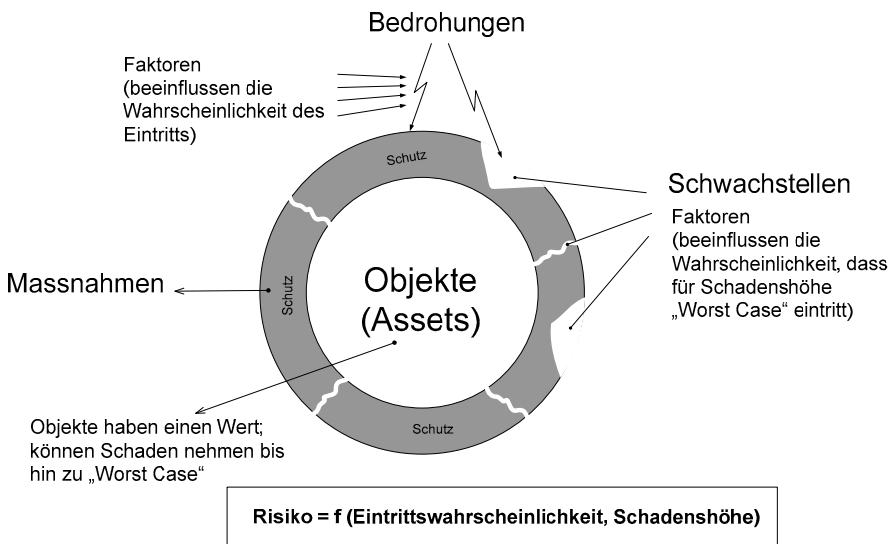


Abbildung 10.10: Risiko-Modell

*Einschätzung der
Schwachstelle*

Als Anhaltspunkte für die erforderliche Stärke einer Massnahme empfiehlt es sich, die Schwachstellen einer Einschätzung zu unterziehen. Um zusätzlich die Relevanz der Schwachstellen bezüglich der vorhandenen Bedrohungen zu berücksichtigen, kann auch der Einfluss der Bedrohungen auf das Schutzobjekt eingeschätzt werden. Die Gesamt-Einschätzung einer Schwachstelle erfolgt sodann aus der Kombination der beiden Einschätzungen.

Praxistipp:

Eine nach dem gezeigten Verfahren „sklavisch“ durchgeführte Risiko-Analyse oder Schwachstellen-Analyse kann sehr bald umfangreich und unübersichtlich werden. Deshalb sollte zu jedem Zeitpunkt hinterfragt werden, ob signifikante Impacts oder Bedrohungen an einem Schutzobjekt überhaupt möglich sind. Wenn nicht, dann sollte das betreffende Risiko oder die Schwachstelle als „unbedeutend“ nicht weiter betrachtet werden.

10.1.5**Kapitel „Bewertung und Anforderungen an Massnahmen“**

Zur Konzeption der Sicherheitsmassnahmen müssen die Risiken, wie sie aus der Risiko-Analyse hervor gegangen sind, für die nun folgende Massnahmenbestimmung zunächst bewertet werden. Primär ist in diesem Schritt zu prüfen inwiefern die Risiken im Rahmen der Akzeptanz-Kriterien liegen oder mit welcher „Wichtigkeit“ und „Dringlichkeit“ Massnahmen ergriffen werden müssen.

Die Risiko-Bewertung der bereits analysierten Risiken wird sowohl im Rückblick auf den „Kontext“ des Systems als auch im Vorausblick auf die in den folgenden Kapiteln des Sicherheitskonzeptes zu konzipierenden Massnahmen durchgeführt. So können hohe Massnahmen-Kosten, oder Chancen-Behinderungen Einfluss auf das Resultat der Risiko-Bewertung haben. Rückblickend auf die Kontext-Festlegungen könnten sich auch Sicherheitseigenschaften wie Vertraulichkeit oder Integrität oder auch die Anforderungen an die Geschäftsprozesse nach durchgeführter Risiko-Analyse in einem neuen Licht darstellen.

Iterative Erstellung

Wie das Risikomanagement in iterativen Zyklen abgewickelt wird (s. Kapitel 3 dieses Buches), werden auch die Kapitel und Abschnitte eines Sicherheitskonzeptes weitgehend iterativ erstellt. Gerade beim Kapitel der Risiko-Bewertung wird die Angemes-

senheit der Verfahren, Methoden und Ergebnisse nochmals hinterfragt, um allenfalls notwendige Nachbesserungen vorzunehmen. Vorausblickend auf die Behandlung der Risiken und Wahl der Massnahmen ist beispielsweise zu entscheiden, ob mit den zu treffenden Massnahmen vorwiegend die Häufigkeit oder das Schadensausmass reduziert werden soll. Auch sind der Vorrang von Massnahmen, wenn sie beispielsweise zu sekundären Risiken führen, oder auch die Zeitprioritäten der Realisierung bei Budget- und Kapazitätsbeschränkungen zu bestimmen.

In Abbildung 10.11 ist ein Beispiel gezeigt, wie das „Risiko-Register“ auf einige wichtige Risiko-Bewertungs-Aspekte im Rahmen des Sicherheitskonzepts erweitert werden kann.

Nr.	Asset	Risikobezeichnung	Identifikation			Analyse							Bewertung		
			Spezifische Bedrohung *)	Schwachstellen	Schadensszenario	Schaden		Informations-Kriterium	Häufigkeit	Akzeptanz-Vorgaben: a = vermeiden oder reduzieren; b = bewältigen nach wirtschaftl. Aspekten c = tragen unter Beobachtung. Zeitprioritäten für Umsetzung: 1 = hoch: sofort; 2 = mittel: im Rahmen Budget; 3 = tief: in nächster Strategie- / Budget-Periode einplanen.					
						Wiederherstellungskosten	Imageverlust		Direkter finanzieller Schaden		Verfügbarkeitsverlust	Vertraulichkeitsverlust		Integritätsverlust	mehre Male pro Jahr (4) 1-3 Jahre (3) 3-10 Jahre (2) 10-30 Jahre (1) > 30 Jahre (0)
Risiko (Risiko-Rating gemäss Risiko-Matrix)															
1.1	Zahlungsverkehr E-Banking	Betrug an Kundenvermögen	Maskerade einer Benutzer-Identität	Unachtsamkeit Benutzer	Diebstahl Kunden-Credentials mittels Phishing-Attacke	4	3		x	x	3	a	a1		
1.2		Ausspähen Bankdaten		Schwaches Authentisierungsverfahren		4	3		x		2	a	a2		
1.3		Lahmlegen E-Banking	Denial-of-Service-Attacke	keine technischen und vorsorglichen Massnahmen	gezielte Blockade des Internet - Zugangs mittels Distributed Denial-of-Service-Attacke	2	3	3	x		2	b	b3		
1.4		Falschüberweisungen	Softwarefehler	Verfahren für Erstellung und Testen der Software nicht anforderungsgerecht.	Sporadische Verfälschungen von Überweisungsdaten infolge schlecht ausgetesteter Software-Release	2	4	4		x	2	a	a1		

*) Zur Bestimmung der Häufigkeit ist die Analyse der auf das Asset bezogenen Schwachstellen notwendig, welche der Bedrohung eine Schadensauswirkung erlauben.

*) Zur Bestimmung der Häufigkeit ist die Analyse der auf das Asset bezogenen Schwachstellen notwendig, welche der Bedrohung eine Schadensauswirkung erlauben.

Abbildung 10.11: Beispiel mit Risiko-Bewertung erweitertes „Risiko-Register“

Zusätzliche Anforderungen an die Sicherheitsmassnahmen

Im Weiteren sind für die im Kapitel 5 des Sicherheitskonzepts detailliert auszuarbeitenden Massnahmen nicht alleine die Risiken, sondern eine Reihe zusätzlicher Anforderungen zu berücksichtigen.

Solche Anforderungen können beispielsweise zu erfüllende Leistungsanforderungen (SLAs) an das System sein. Auch unternehmensinterne Vorgaben für den Einsatz bestimmter Standards oder einer vorgegebenen System- und Sicherheitsarchitektur können für die konkrete Auslegung der Massnahmen wichtige Randbedingungen darstellen. Alle diese Anforderungen gehören im Kapitel 4 des Sicherheitskonzepts beschrieben. Folgende Abbildung 10.12 zeigt eine Zusammenfassung von Bewertungen und Anforderungen, die in das Kapitel 4 des Sicherheitskonzepts gehören.

Kapitel 4: Risiko-Bewertung und Anforderungen an Sicherheitsmassnahmen

- Ergebnisse und Methoden-Verifikation
- Vergleich mit Akzeptanzkriterien
- Grundlagen für Bewältigungsstrategie (Chancenbeeinflussung, Reduktion Auftretens-Häufigkeit oder Schadensausmass)
- Massnahmen-Vorrang und Zeitprioritäten für Realisierung
- Bewertete Risiken mit zeitlichen „Bewältigungs-Prioritäten“ oder „Akzeptanz-Aussagen“ des zuständigen Managements
- Leistungsanforderungen (SLAs)
- Gesetze, Policies, Richtlinien, Architekturvorgaben und Standards, technische und organisatorische Bedingungen und Anforderungen (z.B. aus dem Grobkonzept).

Abbildung 10.12: Anforderungen an die Sicherheitsmassnahmen

10.1.6

Kapitel „Definition und Beschreibung Massnahmen“

Nachdem die zu behandelnden Risiken und die Anforderungen an die Sicherheitsmassnahmen bekannt sind, werden im Kapitel 5 des Sicherheitskonzepts die einzelnen Sicherheitsmassnahmen ausgearbeitet und beschrieben (Abbildung 10.13).

Kapitel 5: Beschreibung der Sicherheitsmassnahmen

- Zuordnung Massnahmen
- Technische Massnahmenbeschreibung (Realisierungsvorschrift) innerhalb der vorliegenden Systemanordnung
- Graphische Darstellung der Massnahmen und deren Integration in das System (Ergänzung des in Kapitel 1 beschriebenen Systems)
- Organisatorische Massnahmenbeschreibung
 - Aufbauorganisatorische Massnahmen
 - Ablauforganisatorische Massnahmen
- Zugriffskonzept

Abbildung 10.13 Inhalte des Kapitels „Beschreibung der Sicherheitsmassnahmen“

Die Beschreibung der Massnahmen soll sich auf die wesentlichen Merkmale beschränken, so dass sie in der erforderlichen Wirksamkeit realisiert, eingeführt und betrieben werden können.

Anpassungen der Systembeschreibung

In diesem Kapitel werden auch die durch die zusätzlichen Sicherheitsmassnahmen notwendig gewordenen Anpassungen der Systembeschreibung (aus Kapitel 1 des Sicherheitskonzepts) aufgeführt.

In Abbildung 10.14 ist ein Beispiel gezeigt, wie das „Risiko-Register“ mit den Definitionen der Massnahmen im Rahmen des Sicherheitskonzepts erweitert werden kann.

Nr.	Asset	Identifikation				Analyse						Bewertung		Massnahmen
		Risiko- bezeichnung	Spezifische Bedrohung *)	Schwachstellen	Schadensszenario	Schaden		Informations- Kriterium	Häufigkeit	Risiko (Risiko-Rating gemäss Risiko-Matrix)	Akzeptanz- Vorgaben: a = vermeiden oder reduzieren; b = bewältigen nach wirtschaftl. Aspekten c = tragen unter Beobachtung. Zeitprioritäten für Umsetzung: 1 = hoch: sofort; 2 = mittel: im Rahmen Budget; 3 = tief: in nächster Strategie- / Budget- Periode einplanen.			
						Wiederherstellungskosten	Imageverlust							
												Direkter finanzieller Schaden	Verfügbarkeitsverlust	
					s. klein (0) klein (1) mittel (2) gross (3) s. gross(4)				mehre Male pro Jahr (4) 1-3 Jahre (3) 3-10 Jahre (2) 10-30 Jahre (1) > 30 Jahre (0)					
1.1	Zahlungsverkehr E-Banking	Betrug an Kundenvermögen	Maskerade einer Benutzer-Identität	Unachtsamkeit Benutzer	Diebstahl Kunden-Credentials mittels Phishing-Attacke	4	3	x	x	3	a	a1	Brief an Kunden über Vorsichtmassnahmen E-Banking;	
1.2		Ausspähen Bankdaten	Schwaches Authentifizierungsverfahren			4	3	x		2	a	a2	Starkes Authentifizierungs-Verfahren (3-Faktoren).	
1.3		Lahmlegen E-Banking	Denial-of-Service-Attacke	keine technischen und vorsorglichen Massnahmen	gezielte Blockade des Internet - Zugangs mittels Distributed Denial-of-Service-Attacke	2	3	3	x	2	b	b3	Abwehrsystem Telekom einrichten; Vorgehen im Rahmen BCM planen.	
1.4		Fälschüberweisungen	Softwarefehler	Verfahren für Erstellung und Testen der Software nicht anforderungsgerecht.	Sporadische Verfälschungen von Überweisungsdaten infolge schlecht ausgestelltem Software-Release	2	4	4	x	2	a	a1	Überarbeitung Standards und Vorgehen zur Software-Qualitätssicherung.	

*) Zur Bestimmung der Häufigkeit ist die Analyse der auf das Asset bezogenen Schwachstellen notwendig, welche der Bedrohung eine Schadensauswirkung erlauben.

Abbildung 10.14 Beispiel mit Massnahmen erweitertes „Risiko-Register“

10.1.7 Kapitel „Umsetzung Massnahmen“

Umsetzung durch entsprechende Aktionen

Ein Sicherheitskonzept ist schliesslich nur so gut, wie es in der Praxis umgesetzt wird. Die einzelnen Massnahmen müssen durch entsprechende Aktionen (ggf. in einem Projekt) umsetzbar sein. Dafür müssen die Aktionen und erwarteten Ergebnisse mit den dafür verantwortlichen Personen abgesprochen und die Termine oder allenfalls auch die Periodizitäten für Aktionen und Massnahmen festgelegt werden. Dokumentiert werden in diesem Kapitel des Sicherheitskonzepts insbesondere die Festlegungen **wie, bis wann und durch wen** die Massnahmen umgesetzt werden (s. Abbildung 10.15).

Kapitel 6: Umsetzung der Sicherheitsmassnahmen

Festlegungen:

- Verantwortlichkeiten und Termine für die Realisierung der Massnahmen
- Verantwortlichkeiten für den Betrieb der Massnahmen
- Nutzen (Wirksamkeit) und Kosten der Massnahmen
- Kontrollen, Reviews und Auditing
- Einverständnis durch Unterschriften

Abbildung 10.15 Festlegungen für die Umsetzung

*Kosten-/Nutzen-
Abwägung*

Bei den Untersuchungen zur Umsetzbarkeit muss der Aspekt der Kosten-/Nutzen-Abwägung einbezogen werden. Die Massnahmenkosten beim Aufbau und Betrieb sollten in einem vernünftigen, wenn nicht sogar optimalen Verhältnis zum Risiko stehen (s. Abbildung 10.1).

Bei zu teuren oder schlecht umsetzbaren Massnahmen wird der Prozess der Sicherheitskonzept-Erstellung von Kapitel 3 bis Kapitel 6 iteriert und das Restrisiko, die Kosten und die Machbarkeit optimiert.

Umsetzungsplan

Stehen die Massnahmen einmal fest, dann wird in diesem letzten Kapitel des Sicherheitskonzepts der Umsetzungsplan in klarer und eindeutiger Weise dokumentiert. Abbildung 10.16 zeigt, wie ein solcher Umsetzungsplan aussehen kann.

Massnahmen		Nutzen	Aufwand / Kosten	Verantwortung	Termin / Periodizität
M1	Brief an Kunden über Vorsichtsmassnahmen	gross	klein	CISO	sofort
M2	Starkes Authentifizierungsverfahren (3-Faktoren mit Smartcard) einführen	gross	gross	Projekt-Owner	Mai 20xy
M3	Starkes Authentifizierungsverfahren (3-Faktoren mit Smartcard) betreiben	gross	mittel	Betriebs-Owner	laufend
M4	Access Control anpassen	gross	klein	Betriebs-Owner	Feb 20xy
M5	DDOS-Abwehrsystem mit Carrier einrichten	mittel	mittel	Netz-Owner	Feb 20xy
M6	DDOS-Massnahmen im Rahmen von BCM planen	gross	klein	CISO	laufend
M7	Überarbeitung Standards und Vorgehen zur Software Qualitätssicherung	gross	mittel	Entwicklungs-Owner	Jan 20xy
•					
•					
•					

Abbildung 10.16: Beispiel Umsetzungsplan eines IT-Sicherheitskonzepts

Unterschriften

Im Rahmen einer guten IT-Governance verpflichten sich die Verantwortlichen, ihre mit Unterschrift bestätigten Aufgaben zum angegebenen Termin auszuführen (Abbildung 10.17). Die Unterschriften bestätigen auch das Einverständnis mit den dokumentierten Aussagen im jeweiligen Zuständigkeitsbereich wie beispielsweise die Akzeptanz von Restrisiken.

Stelle / Rolle	Name	genehmigt	Datum	Unterschrift
Chief Information Security Officer (CISO)	F. Helfer			
Projekt-Owner	M. Beutler			
Betriebs-Owner	A. Holzer			
Entwicklungs-Owner	E. Waldmann			
Netz-Owner	P. Niedermeier			

Abbildung 10.17: Beispiel Unterschriften-Tabelle eines IT-Sicherheitskonzepts

10.1.8

Kommunikation und kooperative Ausarbeitung der Kapitel

Prozess- Rückkopplungen

Für den gesamten Prozess der Erstellung eines IT-Sicherheits-Konzepts gelten die im Abschnitt 3.1 bereits für den allgemeinen Risikomanagement-Prozess beschriebenen Hinweise zur „Kommunikation und Konsultation“.

Bei der Risiko-Analyse sollten die „Impacts“ durch Verantwortliche der Geschäftsprozesse eingestuft werden (z.B. durch Geschäftsprozess-Owner). Für die Festlegung der Wahrscheinlichkeiten muss Fachwissen über den Aufbau des Systems und sein Umfeld vorhanden sein. Für die Bedrohungs- und Schwachstellen-Analyse werden entsprechende IT-Fachexperten zugezogen.

Fachinformatio- nen aus Geschäfts- und IT- Perspektive

Schliesslich werden die Fachinformationen sowohl aus der Geschäfts-Perspektive als auch der IT-Perspektive in einem gemeinsamen Dialog zur Einschätzung des tatsächlichen Risikos zusammen gebracht.

Der Dialog ist auch dann wichtig, wenn sich die Massnahmenkosten als zu hoch erweisen und mit einer geänderten Behandlungsstrategie die Restrisiken neu eingeschätzt und bewertet werden müssen.

Bereits die Ausarbeitung des Sicherheitskonzepts ist Teil des Risikomanagements für das betreffende System, deshalb soll die Ausarbeitung auch durch diejenigen Stellen vorgenommen werden, die über das Wissen und die Verantwortung über das System (Prozess) verfügen.

Moderation oder Coaching

Eine Moderation oder ein Coaching des Erstellungsprozesses von zentraler Stelle (z.B. durch CISO) kann die Effizienz des Erstellungsprozesses wesentlich steigern.

10.1.9

Risiko-Akzeptanz, Konzept-Abnahme und -Anpassung

Vorlage, Abnah- me und Akzep- tanz

Ausserhalb des Prozesses der Konzepterstellung bedarf es eines weiteren wichtigen Prozesses, nämlich des Prozesses der Vorlage, der Abnahme und Akzeptanz sowie der Umsetzungskontrolle der durch eine entsprechende „Policy“ gesteuert ist. Mit einem solchen zusätzlichen Prozess erfüllt ein Sicherheitskonzept die an einen Risikomanagement-Prozess gestellte wichtige Anforderung der stetigen Kontrolle und Anpassung an die Risikolage.

Festlegungen in Policy

In der Policy wird beispielsweise festgelegt, für was und zu welchem Anlass (z.B. Einführung eines IT-Systems) ein Sicherheitskonzept zu erstellen ist und wer die Verantwortung für die Ablieferung eines Sicherheitskonzepts trägt.

Akzeptanz Konzept und Restrisiken

Das aus dem Sicherheitskonzept ersichtliche Vorgehen, wie die Risiken ermittelt und die Massnahmen definiert und umgesetzt werden, sind für die Akzeptanz des Konzepts und der daraus ersichtlichen „Restrisiken“ wichtig. Es empfiehlt sich deshalb, das Sicherheitskonzept zum Zeichen der Akzeptanz von den verantwortlichen Führungspersonen „abnehmen“ und unterzeichnen zu lassen.

Verpflichtung zur Aktualisierung

Sind die für die Erstellung und Aktualität eines Sicherheitskonzepts verantwortlichen Personen (z.B. Owner) per Policy definiert, dann können diese Personen periodisch und zu geeigneten Anlässen zur Aktualisierung verpflichtet werden.

10.1.10

Überwachung und Überprüfung

Überprüfungen im Rückblick

Der Prozess der Erstellung eines IT-Sicherheitskonzepts weist die für einen Risikomanagement-Prozess üblichen Rückkopplungen zu früheren Prozess-Schritten auf. Bei der schrittweisen Bearbeitung ist immer wieder zu prüfen, ob die Aussagen (z.B. das Assessment) auch dem realen übergeordneten Kontext entsprechen und auch die Wirksamkeit der Massnahmen hinsichtlich ihrer Umsetzung und der eingeschlagenen Behandlungs-Optionen gewährleistet ist.

Überprüfung Einhaltung und Richtigkeit

Die Einhaltung der Vorlage- und Aktualisierungsvorschriften, wie auch die Richtigkeit der Akzeptanz-Entscheide, sind in entsprechende Überprüfungen einzubeziehen.

Für die gesamten Prozesse der Erstellung, Vorlage, Abnahme und Akzeptanz der Sicherheitskonzepte gelten die im Abschnitt 3.10 bereits für den allgemeinen Risikomanagement-Prozess beschriebenen Hinweise zur „Überwachung und Überprüfung“.

10.2

Die CRAMM-Methode

Risiko-Analyse und Massnahmen-Zuordnung

Die CRAMM*-Methode ist ursprünglich für den Einsatz in Regierungsstellen des United Kingdom entwickelt worden. Die Methode sollte mit einer entsprechenden Software sowohl das Risiko-Assessment unterstützen als auch geeignete Massnahmen zuordnen können. CRAMM wurde 1986 erstmalig publiziert und 1988 in der ersten Software-Version (Version 1.0) für den öffent-

* CRAMM (= Centre for Information Systems Risk Analysis und Management Method); CRAMM has been produced in consultation with the Security Service and CESG, who are UK Government national security authorities.

lichen Sektor und kurz darauf auch für den privaten Sektor freigegeben. Zum Zeitpunkt dieser Buchauflage ist die Version 5.2.5 sowie die durch die NATO angewandte Version NATO (CRAMM) V5.6 erhältlich. Seit einiger Zeit werden die Methode und das Software-Tool durch „Siemens Enterprise Communication Ltd.“ weiterentwickelt, vertrieben und gewartet. Damit wird das Tool auch jeweils für die aktuellen MS-Windows-Plattformen lauffähig gemacht. Hervorzuheben ist die volle Kompatibilität zum Standard ISO/IEC 27001 und die mögliche Unterstützung zur Erlangung einer ISO-27001-Zertifizierung. Anhand von unterschiedlichen Modulen kann das Tool auch wahlweise in einem „Expert“-Modus oder in einem „Express“-Modus betrieben werden.

Profile

Das System kann mit verschiedenen, auf das Anwendungsgebiet zugeschnittenen „Profilen“ arbeiten: Prinzipiell wurden die Profile für die NATO, das UK Government, die EU, und für andere Institutionen (z.B. Militär der Niederlande) oder private Firmen unterschieden.

Profil-Festlegungen

Die Profile enthalten Festlegungen für:

- Schutzobjekt-Typen (Asset Types)
- Bedrohungs-Arten
- Fragebögen sowie Eingabe-Masken für die Erhebung und Eingabe der Bedrohungen und Schwachstellen
- Risiko-Matrix, mit welcher die Risiken aus den eingegebenen Werten für die Schutzobjekte, Bedrohungen und Schwachstellen berechnet werden können (s. Abbildung 10.18).
- Massnahmenkataloge zur Bewältigung der Risiken
- Report-Format zur Präsentation der Ergebnisse
- Unterstützung anwendungsspezifischer „Policy Frameworks“ (z.B. für NATO-Benutzer)

	Bedrohung	sehr klein			klein			mittel			gross			sehr gross		
		klein	mittel	gross	klein	mittel	gross	klein	mittel	gross	klein	mittel	gross	klein	mittel	gross
Schutzobjekt-Wert	1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
	2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
	3	1	2	2	2	2	2	2	3	3	3	3	4	3	4	4
	4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
	5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
	6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
	7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
	8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
	9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
	10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Beispiel: Bedrohung = sehr gross, Schwachstelle = klein, Schutzobjekt-Wert = 8 ergibt Risiko-Wert aus der Tabelle = 6.

Abbildung 10.18: Beispiel einer CRAMM-Risiko-Matrix*

Das Software-Tool führt systematisch durch einen „Risk Management Review“ und gibt die folgenden Schritte vor:

Review-Schritte

1. Festlegen der Rahmenbedingungen und System-Abgrenzungen für den Review
2. Identifikation der Schutzobjekte (Assets) und Konstruktion des Schutzobjekte-Modells (Asset Model)
3. Bewertung der Schutzobjekte (Asset Valuation)
4. Erhebung und Einstufung der Bedrohungen (Threats) und der bei diesen Bedrohungen massgeblichen Schwachstellen (Vulnerabilities)
5. Risiko-Bestimmung
6. Massnahmenzuordnung
7. Abschliessende Berichterstattung

* Insight Consulting: Broschüre „CRAMM 3 Overview“

**Rahmen-
bedingungen und
Kontext****Zu Schritt 1:**

Bei der Festlegung der Rahmenbedingungen des Reviews in Schritt 1 verlangt das Programm die Eingabe der Funktionsbeschreibung für das zu untersuchende System und die mit dem zuständigen Management abgestimmten Systemabgrenzungen, die organisatorischen Rahmenbedingungen und andere Kontext-Informationen für den durchzuführenden Review.

Asset Modell**Zu Schritt 2:**

Nachdem im Schritt 2 die relevanten Schutzobjekte aufgesucht und identifiziert wurden, werden diese aufgrund ihrer Schadensabhängigkeiten in einem Schutzobjekt-Modell (Asset Model) logisch verknüpft.

Die logischen Verknüpfungen erfolgen in der folgenden Hierarchie:

- Informationen-/Informationsobjekt und für die Informations-Lieferung zuständiger „Endbenutzer-Service“.
- Software-Objekt
- Physische Objekte, welche die Informationsobjekte jeweils unterstützen (z.B. Hardware, Netzwerkkomponenten und Betriebssysteme. Anm.: die Betriebssysteme und ihre Komponenten werden zu den physischen Objekten gezählt)
- Räume

Die Methode bedient sich eines sogenannten „Enduser Service“. „Enduser Services“ können beispielsweise Interaktive Sessions, File Transfer, Application-to-Application-Messaging, E-Mail, Sprache oder Video sein.* Das Schutzobjekt-Modell (Asset Model) spiegelt die Logik wider, wie die einzelnen Schutzobjekte voneinander abhängen, d.h. bezüglich der Bedrohungsauswirkung ineinander verschachtelt sind.

* Der „Enduser Service“ bestimmt die Art, wie die anderen Schutzobjekte die Informations-Schutzobjekte unterstützen resp. „liefern“. Der Grund sind die unterschiedlichen Risiken bei unterschiedlichen „Liefer-Arten“. (Greift beispielsweise eine Person „interaktiv“ auf die Informationen in einer Informationsbank zu, dann sind die Risiken anders als bei Informationsaustausch zwischen unterschiedlichen Applikationen.)

Die freie Eingabe von praktisch beliebigen Schutzobjekt-Modellen erlaubt die flexible Anpassung eines Reviews an die Gegebenheiten einer realen Systemkonfiguration. Damit können die Bedrohungsauswirkungen über beliebig ineinander verschachtelte Schutzobjekte modelliert werden.

Beispiel:

Auf ein „Pensions-Versicherungs-System“ für die interaktive Verarbeitung der Versicherungs-Informationen mit anschließendem Ausdruck des Versicherungsausweises kann über 5 Workstations zugegriffen werden. Zum Review der Risiken und der Sicherheitsmassnahmen mittels CRAMM und dem allenfalls notwendigen Zuordnen von zusätzlichen Sicherheitsmassnahmen wird vorgängig ein Schutzobjekte-Modell (Asset-Modell) erstellt (s. Abbildung 10.19).

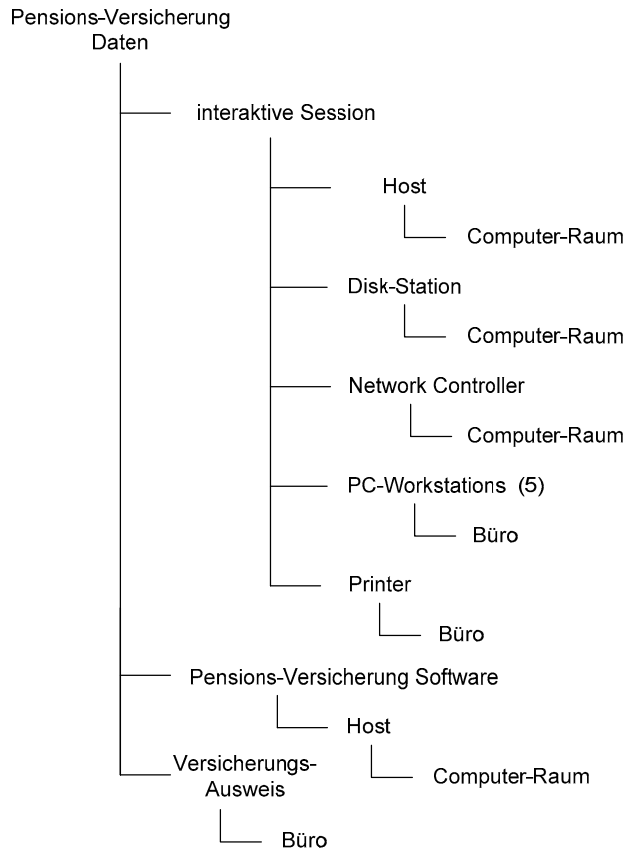


Abbildung 10.19: Beispiel eines CRAMM „Asset Modells“

*Wert-
Einschätzung
Schutzobjekte*

Zu Schritt 3:

Zur Einschätzung der Schutzobjekte steht eine Werteskala von 10 Stufen zu Verfügung. Die Einschätzung wird für das „Worst case“-Szenario (z.B. Totalverlust) durchgeführt. Nach Abschluss der Schutzobjekt-Bewertung in Schritt 3 werden nur noch diejenigen Schutzobjekte weiter analysiert, deren Schutzbedarf nicht durch „Baseline Security“-Massnahmen abgedeckt werden können. Der Massnahmen-Katalog gemäss Standard ISO/IEC 27002 ist im Tool enthalten.

*Einstufung
Bedrohungen und
Verletzlichkeiten*

Zu Schritt 4:

Im Schritt 4 werden die Bedrohungen und die Verletzlichkeiten aufgrund ihrer Einflussstärke auf das Schutzobjekt mit entsprechenden Faktoren eingestuft.

Die Schutzobjekte, welche von der gleichen Bedrohung direkt betroffen sind, werden vor der Einstufung der Bedrohung und der Verletzlichkeit zu Schutzobjekte-Gruppen zusammengefasst. Im oben aufgeführten Beispiel werden demzufolge bezüglich der Bedrohung „Brand“ die Schutzobjekte „Computer-Raum“ und „Büro-Raum“ zu einer Gruppe und bezüglich der Bedrohung „Stromausfall“ alle Hardware-Einrichtungen zu je einer Gruppe zusammengefasst.

Zur Einstufung einer Bedrohung auf ein Schutzobjekt (oder eine Schutzobjekt-Gruppe) stehen fünf Stufen von Häufigkeiten zur Verfügung, mit denen die Bedrohung je nach Stärke zum Ereigniseintritt führen kann (jeden Monat, alle 4 Monate, jedes Jahr, alle 10 Jahre).

Zur Einstufung der Verletzlichkeit eines Schutzobjekts (oder einer Schutzobjekt-Gruppe) stehen drei Bereiche von Wahrscheinlichkeiten zur Verfügung, mit welchem der Worst Case (z.B. Totalverlust) eintritt.

*Berechnung
Risiko-Werte*

Zu Schritt 5:

Mit den Einschätzungen des Schutzobjekt-Wertes, der Bedrohung und der Verletzlichkeit wird mittels der Risiko-Matrix (s. Abbildung 10.18) ein Risiko-Wert berechnet.

Bezogen auf jede Bedrohung wird ein solcher Risiko-Wert berechnet,

- für jedes Schutzobjekt in einer Schutzobjekt-Gruppe,
- für jedes Schutzobjekt, welches von einer Schutzobjekt-Gruppe abhängig ist oder von welchem eine Schutzobjekt-Gruppe abhängt und

- für jede Art von Schadensauswirkung (Impact Type), die von einer Bedrohung herrührt.

„Backtracking“-Funktion

Mittels einer „Backtracking“-Funktion können sämtliche Bewertungen und Eingaben, die zu den Risikowerten geführt haben, zurückverfolgt werden.

Sowohl beim Backtracking als auch bei den jeweiligen Schritten der Risiko-Berechnung können entsprechend Reports ausgedruckt werden.

Massnahmen-Zuordnungen

Zu Schritt 6:

Die Teilschritte bei der Massnahmenzuordnung werden in der Terminologie des Tools als „Risikomanagement“ bezeichnet. Bei dieser Massnahmenzuordnung können Massnahmenvorschläge des Tools eingesetzt werden. Die Massnahmenbibliothek beinhaltet zurzeit 7000 detaillierte Massnahmen, die in 70 logische Gruppen unterteilt sind. Es können aber auch alternative Massnahmen aus einem eigens angelegten Massnahmenkatalog zugeordnet werden. Für den gesamten Review-Prozess besteht eine „Backtracking“- und eine „What-if“-Funktion.

„What-if“-Funktion

Die „What-if“-Funktion erlaubt das Durchspielen des Reviews mit anderen Variablen und Werten, ohne dass die zuvor eingegeben Variablen und Werte verloren gehen.

Risikomanagement-Report

Zu Schritt 7:

Der abschliessende Risikomanagement Report gibt die wesentlichen Informationen für die Umsetzung der definierten Massnahmen wieder (Abbildung 10.20).

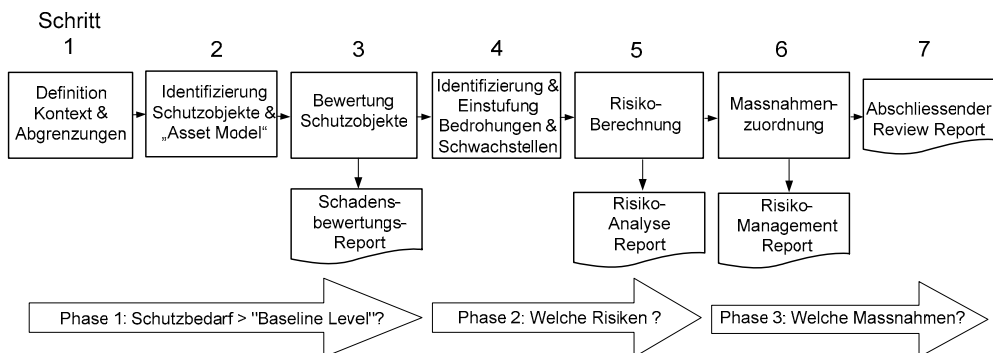


Abbildung 10.20: Ablauf eines Reviews mittels CRAMM-Software

10.3

Fehlermöglichkeits- und Einfluss-Analyse

FMEA

Die Fehlermöglichkeits- und Einfluss-Analyse (FMEA: Failure Mode and Effects Analysis) war ursprünglich (1940) als Standard MIL-STD-1629 des US Departments of Defence (DoD) zur Ermittlung von Schwachstellen in technischen Systemen, vor allem in der Raketen-Entwicklung, vorgesehen. In der Luft- und Raumfahrt und der Rüstungsindustrie sind die Nachfolgestandards MIL-STD-129A FMCEA (Failure Mode Effect and Criticality Analysis) und SAE ARP5580 FMEA entstanden. 1970 wurde der Standard durch die Ford Motor Company aufgegriffen, um das Design und die Produktion von Autos zu verbessern. Auch hier sind Nachfolgestandards entstanden (z.B. SAE J1739 FMEA und AIAG FMEA).

Bottom-up-Methode

Grundsätzlich ist FMEA eine „Bottom-up-Methode“ (s. Abschnitt 3.7) und zeigt, wo Einzelkomponenten zu Ausfällen und Auswirkungen auf den höheren Ebenen eines ganzen Systems oder Teilsystems führen können.

Schwachstellen-Analyse-Methode

Sie ist unter anderem auch eine Schwachstellen-Analyse-Methode, die dem Aufzeigen von „Single Point of Failures“ dienen kann. Falls mit korrektiven Massnahmen die „Single Point of Failures“ nicht eliminierbar sind, können zumindest nach dem „What-if“-Prinzip (Was ist, wenn...?) Massnahmen herausgefunden werden, welche den Störungs-Einfluss einer kritischen Komponente auf das Gesamtsystem mildern.

Zuverlässigkeits-Analyse

Das Verfahren wird hauptsächlich in der Zuverlässigkeits-Analyse eingesetzt. Einschränkungen in der Anwendung bestehen darin, dass die gegenseitige Beeinflussung der Komponenten nicht berücksichtigt wird und die Methode lediglich Aussagen über Schwachstellen und die daraus resultierenden Ausfallszenarien macht, hingegen keine echte Risiko-Analyse aufgrund von Bedrohungen und Verlustpotentialen vornimmt.

Die Methode wird heute hauptsächlich im Bereich des präventiven Qualitätsmanagements für die Produkte-Herstellung insbesondere in der Automobil- und Medizinaltechnik verwendet. Dabei geht es darum, in den planerischen Phasen einer Produktentwicklung potentielle Fehler während der Entwicklung oder der Herstellung aufzudecken und geeignete Vorkehrungen (Massnahmen) zu treffen.

Qualitäts-Management

Mit der FMEA-Methode können im Lebenslauf eines Produktes (in unserem Falle eines IT-Systems) die Fehlerquellen von der

Entwicklung bis hin zur Nutzung analysiert und bewältigt werden. Im klassischen Qualitätsmanagement erfolgt die Fehlerquellen-Analyse mit FMEA in den drei Betrachtungsgebieten [SEGH96]:

Betrachtungsgebiete

- **Konstruktions-FMEA:** Ermittelt die Risiken der Produkte (Systeme) während der Entwicklung (Eignungs-Validierung und Funktionen-Verifizierung). Die in dieser Phase zu treffenden Massnahmen können sowohl in der Entwicklung als auch im Herstellungsprozess einsetzen
- **Prozess-FMEA:** Ermittelt die Risiken vor der Herstellung, während des Produktplanungsprozesses und baut auf den Ergebnissen der Konstruktions-FMEA auf.
- **System-FMEA:** Ermittlung der gesamtheitlichen Risiken mehrerer Untersysteme und deren Konstruktions-FMEA. Dabei gehen die FMEAs der Konstruktions-FMEAs der einzelnen Untersysteme in die Betrachtung des Gesamtsystems ein.

Risikoprioritäten-zahl

Es ist eine Spezialität der Methode, aufgrund von potentiellen Fehlern eine Risikoprioritätenzahl zu liefern, mit welcher die Reihenfolge der Verbesserungsmassnahmen gesteuert werden können.

$$\text{Rpz} = A \times B \times E$$

Rpz: Risikoprioritätenzahl mit

A: Auftretenswahrscheinlichkeit

(1= sehr gering; 10= sehr hoch)

B: Bedeutung

(1=geringfügige Folgen; 10=äusserst schwerwiegende Folgen)

E: Entdeckungswahrscheinlichkeit

(1= sehr hoch; 10 = sehr gering)

Einsatz im Qualitätsmanagement

Das Verfahren wird heute hauptsächlich im Automobilbau benutzt. Der Verband der (deutschen) Automobilindustrie hat ein genormtes Formblatt (VDA-Formular) mit einer Schrift „Qualitätsmanagement in der Automobilindustrie VDA 4.2“ herausgegeben ([Eber03], S.83-116). Für jedes System respektive Merkmal werden im Wesentlichen die potenziellen Fehler, die potenziellen Folgen der Fehler, die potenziellen Fehlerursachen sowie die empfohlenen Massnahmen mit Verantwortlichkeitszuordnung

registriert. Der derzeitige sowie der mit Massnahmen verbesserte Zustand werden mit den oben angegebenen Risiko-Parametern bewertet.

Einsatz in der Informations-Technologie

Die FMEA kann in abgewandelter Form auch in der Informations-Technologie eingesetzt werden, wo es um die Gesamtverfügbarkeit von Systemen oder ganzen IT-Dienstleistungen aufgrund der Zuverlässigkeit einzelner Komponenten und einer bestimmten Anordnung der Komponenten im System geht.

Soll beispielsweise ein System auf möglichst hohe Gesamtverfügbarkeit an der Schnittstelle zum Kunden ausgelegt werden, dann können für das Gesamtsystem sowie für einzelne Untersysteme die FMEAs unter Einsatz verschiedener Komponenten und Konfigurationen durchgespielt werden. Die Zuordnung der Risikoprioritätenzahl zu einzelnen Komponenten oder Konfigurationen ermöglicht die quantitative Bewertung der Gesamtzuverlässigkeit einer gewählten Systemvariante. Zu bedenken ist, dass die Komponenten nicht zu weit heruntergebrochen werden dürfen, da andernfalls die FMEA aufgrund der Komplexität unübersichtlich wird.

10.4

Fehlerbaum-Analyse

„Top-Ereignis“

Entgegen der FMEA-Analyse ist die Fehlerbaum-Analyse (FTA: Fault Tree Analysis) eine Top-Down-Methode (s. Abschnitt 3.7). Bei dieser Methode werden von einem bestimmten Fehlerereignis dem sog. Top-Ereignis (Top Event) „deduktiv“ die ursächlichen Ereignisse gesucht, die für das Top-Ereignis verantwortlich sind.

Logische Verknüpfungen als Baum

Die möglichen Ereignisse werden dabei logisch zu einer Baumstruktur verknüpft. Der Baum zeigt auf, welche untergeordneten Ereignisse in welcher logischen Verknüpfung ein jeweils übergeordnetes Fehler-Ereignis verursachen.

Wahrscheinlichkeit des Top-Ereignisses

Das Verfahren kann sowohl qualitative als auch quantitative Aussagen liefern. Als quantitative Aussage ist insbesondere die Eintrittswahrscheinlichkeit des Top-Ereignisses von Interesse. Diese Wahrscheinlichkeit ergibt sich rechnerisch aus den logischen Verknüpfungen des Baumes und den Wahrscheinlichkeiten der ursächlichen (Basis)-Ereignissen.

Systemdefinition

Im ersten Schritt der Fehlerbaum-Analyse, der „Systemdefinition“, ist es wichtig, im abgegrenzten Analysebereich alle Top-Ereignisse sowie die Situationen für das Eintreten der Top-Ereignisse zu bestimmen [Leve95].

UND- / ODER- Verknüpfungen

Vom resultierenden Ereignis werden die dafür verantwortlichen „ursächlichen“ Ereignisse gesucht. Müssen für den Eintritt eines Ereignisses die dafür ursächlichen Bedingungen gemeinsam auftreten, dann werden sie algebraisch (Boolesche Algebra) mittels eines logischen UND verknüpft. Genügt bereits eine der ursächlichen Fehler-Bedingungen, um das Fehlerereignis zu bewirken, dann wird diese Eigenschaft durch eine logische ODER-Verknüpfung abgebildet. Die Eingangs-Bedingungen für jede logische Verknüpfung sind die Resultate der direkt untergeordneten Verknüpfungen. Der Baum wird solange von oben nach unten konstruiert, bis die Bedingungen für solche Verknüpfungen „grundlegend“ sind und deshalb nicht mehr weiter hergeleitet werden können.

„Blätter“ = „Basis- Ereignisse“

Die grundlegenden Bedingungen können anschaulich als die Blätter des Baumes verstanden werden. Diese Blätter werden auch „**Basis-Ereignisse**“ genannt. Bei der Definition der Basis-Ereignisse ist darauf zu achten, dass diese nicht voneinander abhängig oder aufgrund gemeinsamer Ursachen eintreten. Wird der Baum gezeichnet, dann werden die im Standard IEC 1025 normierten Symbole verwendet (Abbildung 10.21). Die jeweiligen „Resultats-Ereignisse“ werden in einem Rechteck dargestellt. Hingegen werden die Basis-Ereignisse als Kreis und die Ereignisse mit ungeklärten Ursachen als Raute gezeichnet.

Cut Set

Bei der Auswertung eines solchermassen konstruierten Baumes sind vorab die sogenannten „Cut Sets“ von Interesse:

Ein **Cut Set** ist eine Gruppe von gleichzeitig auftretenden Basis-Ereignissen, die den Eintritt des Top-Ereignisses bewirkt.

Single Point of Failure

Ein Fehler-Baum weist in der Regel mehrere Cut Sets auf (s. Beispiel in Abbildung 10.21). Enthält beispielsweise ein Cut Set lediglich ein einziges Basis-Ereignis, dann liegt ein „Single Point of Failure“ vor.

Minimal Cut Set

Die Cut Sets können auch zur Berechnung der Wahrscheinlichkeit des Top-Ereignisses herangezogen werden. Dazu müssen aber vorab die „Minimal Cut Sets“ bestimmt werden:

Ein **Minimal Cut Set** ist eine minimale Gruppe von gleichzeitig auftretenden Basis-Ereignissen, die den Eintritt des Top-Ereignisses bewirkt.

Berechnung der Wahrscheinlichkeit aus „Minimal Cut Sets“

Mit den „Minimal Cut Sets“ kann die Wahrscheinlichkeit (oder Häufigkeit) des Top-Ereignisses berechnet werden, indem die Wahrscheinlichkeiten der in einem „Minimal Cut Set“ vertretenen Basis-Ereignisse multipliziert und anschliessend die Ergebnisse aus den einzelnen „Minimal Cut Sets“ aufsummiert* werden. Die Ermittlung der „Cut Sets“ aus dem Fehlerbaum und deren Reduktion auf „Minimal Cut Sets“ erfolgt mittels Boolescher Algebra ([Vese81], S. VII-1 bis VII-19). Zur Berechnung der Wahrscheinlichkeiten aus den „Minimal Cut Set“ dient die Wahrscheinlichkeits-Algebra ([Vese81], S. VI-3 bis VI-8).

Beispiel:

Für den Fehlerbaum in Abbildung 10.21 soll die Wahrscheinlichkeit für das Top-Ereignis für die beiden Fälle Stromausfall E-Werk ≤ 20 Min. und Stromausfall > 20 Min. berechnet werden.

Stromausfall E-Werk $t \leq 20$ Min.		Stromausfall E-Werk $t > 20$ Min.	
Minimal Cut Sets [†]	Häufigkeit pro Jahr	Minimal Cut Sets	Häufigkeit pro Jahr
{b e d}	$0.1 * 0.05 * 0.5 = 0.0025$	{ e d}	$0.05 * 0.2 = 0.01$
{b f d}	$0.1 * 0.2 * 0.5 = 0.01$	{ f d}	$0.2 * 0.2 = 0.04$
	0.0125		0.05

Die obige Tabelle gibt die quantitative Auswertung des Fehlerbaums über seine Minimal Cut Sets wieder. Die Häufigkeit, dass der Computer infolge Ausbleibens der Stromversorgung ausfällt, beträgt 1.25 Mal in 100 Jahren im Zeitintervall von ≤ 20 Min. und 1 Mal in 20 Jahren im Zeitintervall von > 20 Min.

* Die Addition führt zu einem annähernd guten Ergebnis, wenn die Cut Sets kleine Wahrscheinlichkeiten liefern. Andernfalls ist die Wahrscheinlichkeit des Top-Ereignisses mit folgender Formel aus den Wahrscheinlichkeiten p_i der Minimal Cut Sets zu berechnen:

$$P_t = 1 - \prod_{i=1}^n (1 - p_i)$$

† Mit Boolescher Algebra aus Fehlerbaum hergeleitet:
 $a = bcd = b(e+f)d = bed + bfd$

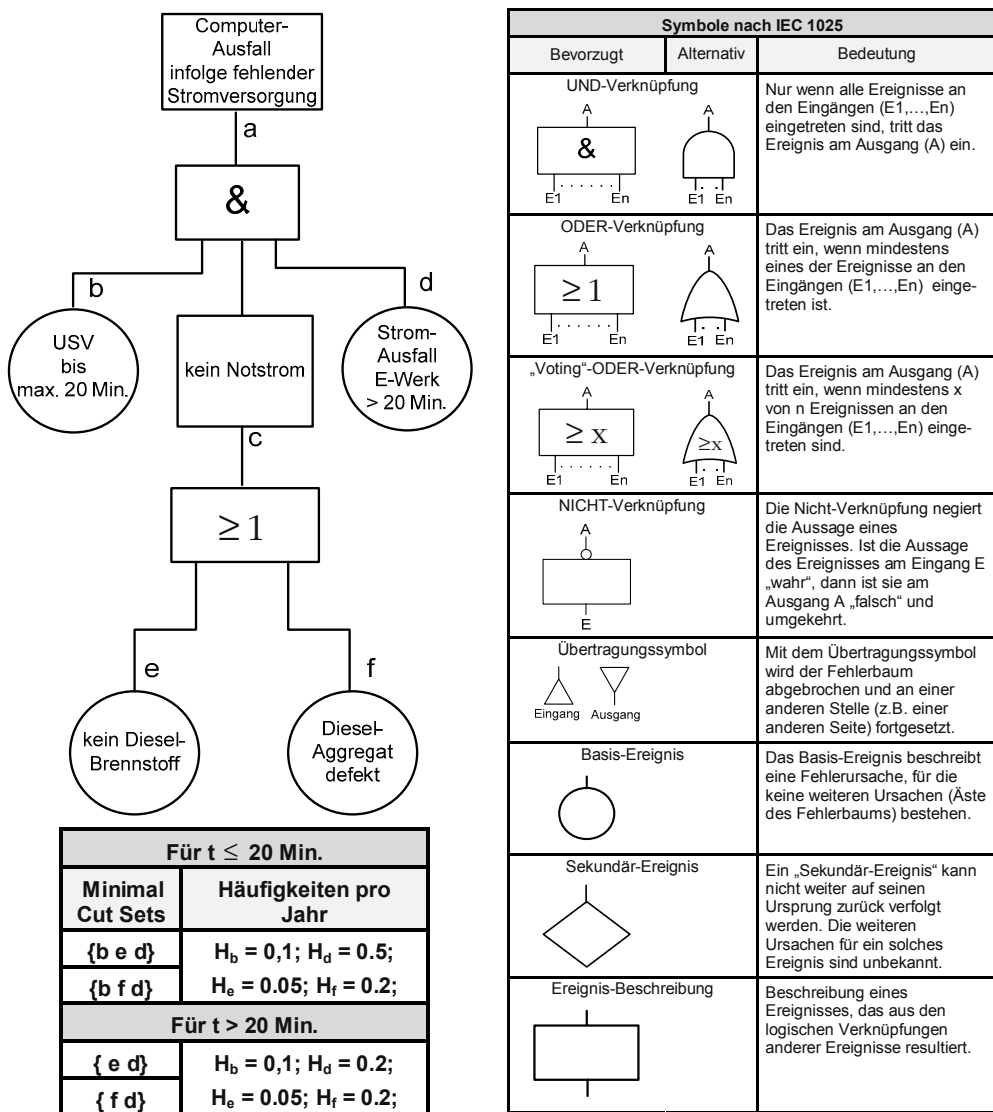


Abbildung 10.21: Beispiel eines einfachen Fehlerbaums

Grössere Fehlerbäume

Zur Konstruktion und Auswertung von grösseren Fehlerbäumen helfen Softwareprogramme, mit welchen die Bäume erfasst und die Wahrscheinlichkeiten von den Basis-Ereignissen auf das resultierende Top-Ereignis hochgerechnet werden können.

	Die Bäume zu konstruieren und die Wahrscheinlichkeiten für die Primäreignisse zu schätzen, ist bei Informationen und IT-Komponenten nicht trivial und bedarf einiger Erfahrung.
<i>Angriffsbaum-Analyse</i>	Eine modifizierte Form der Fehlerbaum-Analyse ist die Angriffsbaum-Analyse. Bei dieser Analyse wird untersucht, welche Angriffsstrategien für einen Angreifer hinsichtlich seines Angriffsziels, bei vorliegenden Schwachstellen, hinreichend lukrativ sind [Witb06].
<i>Fehlerbaum für komplexes IT-System</i>	Eine Fehlerbaum-Analyse für ein komplexes IT-System erfolgt in der Regel in einem Team von in verschiedenen Disziplinen erfahrenen Fachkräften. Ein auf hohe Verfügbarkeitsanforderungen ausgelegtes Systemkonzept kann anhand dieses Verfahrens verifiziert werden. Das Verfahren eignet sich auch vorzüglich für „Sensitivitäts-Analysen“, indem durch Variationen in den Konfigurationen und dem Zuordnen von Massnahmen, z.B. bei Sichtbarwerden von „Single Point of Failures“, die resultierenden Auswirkungen auf das Top-Ereignis studiert werden können.
<i>Geschicktes Einfügen von Redundanzen</i>	Durch geschicktes Einfügen von Redundanzen in ein System können diese „Single Point of Failures“ eliminiert und damit die Wahrscheinlichkeit für das Eintreten des Top-Ereignisses verringert werden. Anhand der Variationen kann unter anderem das Kosten-/Wirksamkeits-Verhältnis der Massnahmen optimiert werden.
<i>Anwendungen</i>	Die Fehlerbaum-Analyse kann bei unterschiedlichen Fragestellungen Anwendung finden: ☐ Präventive Qualitätssicherung auf Entwicklerbasis; ☐ System-Analyse / Bestätigung des Systemkonzepts; ☐ Problemlösung bei neu eingetretenen Fehlern.
<i>Ausfallkategorien</i>	Es werden drei Ausfallkategorien unterschieden ([Stor96], S. 45): ☐ Primärer Ausfall: Ausfall bei zulässigen Einsatzbedingungen; ☐ Sekundärer Ausfall: Ausfall bei unzulässigen Einsatzbedingungen; ☐ Kommandierter Ausfall: Ausfall aufgrund einer falschen oder fehlenden Ansteuerung.

10.5

Ereignisbaum-Analyse

Analyse der Folgen eines Ereignisses

Bottom-up-Methode

Wahrscheinlichkeiten an Gabelungspunkten

Bei der Ereignisbaum-Analyse (ETA: Event Tree Analysis) gehen wir von einem Ereignis aus und untersuchen, welche Folgen dieses Ereignis im System haben kann. Das auslösende Ereignis kann der Ausfall einer Systemkomponente oder ein anderes Ereignis im System sein. Die Ereignisbaum-Analyse ist somit eine Bottom-up-Methode (s. Abschnitt 3.7).

Ausgehend vom auslösenden Ereignis wird ein Baum von links nach rechts gezeichnet, der sich nach jedem Suchschritt in zwei Äste aufteilt. Der Ast nach oben gibt ein positives Folgeereignis und der Ast nach unten jeweils ein negatives (schädliches) Folgeereignis an.

Die Ereignisse an jedem Gabelungspunkt des Baumes sind mit Eintritts-Wahrscheinlichkeiten verbunden. Der Baum endet dort, wo das Schadensausmass am höchsten ist oder wo sich ein Unfall oder Schadensereignis in vollem Ausmass oder in einem zu untersuchenden Folgeereignis präsentiert. Die nachfolgende Abbildung 10.22 zeigt das Beispiel eines Ereignisbaumes.

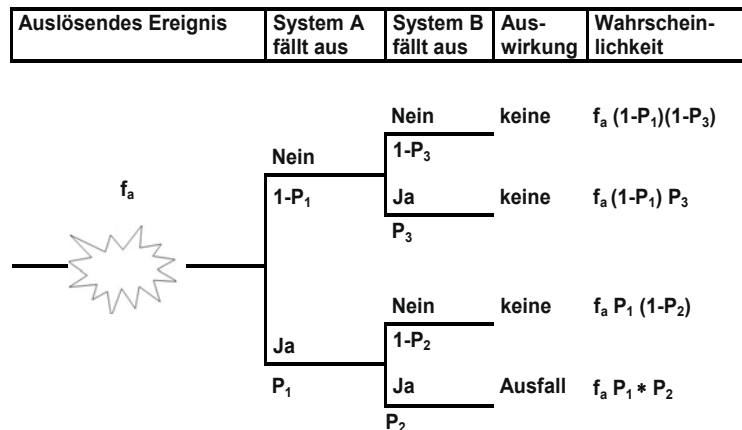


Abbildung 10.22: Beispiel eines Ereignisbaums

Wahrscheinlichkeit für Eintritt Folgeereignis

Die Multiplikation der Wahrscheinlichkeiten auf dem Pfad des Baumes bis zum Folgeereignis ergibt die Wahrscheinlichkeit dafür, dass das Folgeereignis eintritt. In dem in Abbildung 10.22 gezeigten einfachen Beispiel tritt der Ausfall dann ein, wenn System A und System B ausfallen. Die Wahrscheinlichkeit dafür ist P_1 multipliziert mit P_2 .

In grossen (asymmetrischen) Ereignisbäumen wird das zu untersuchende Folgeereignis möglicherweise über mehrere Pfade des Baumes erreicht. In diesem Falle ergibt sich die Wahrscheinlichkeit für den Eintritt des Folgeereignisses aus der Kombination der Wahrscheinlichkeiten aller Pfade, die zum Folgeereignis führen.

Für komplexe Systeme ergeben sich sehr grosse Ereignisbäume, die zwar mit Computer-Unterstützung gut verwaltet werden können, jedoch bei der numerischen Auswertung der geschätzten Wahrscheinlichkeiten zu grossen Ungenauigkeiten führen.

*Anwendung in
der Informationssicherheit*

Um einen Ereignisbaum erstellen zu können, muss das System in seinen Eigenschaften gut analysierbar sein. Die Anwendung in der Informationssicherheit ist deshalb nur in Teilbereichen und für gut analysierbare Konstellationen und Aspekte (z.B. Brandschutz, Rechenzentrums-Standortbestimmung) sinnvoll. Eine Ereignisbaum-Analyse für die umfassende Gefahren- und Schwachstellen-Situation eines IT-Systems scheidet nach den oben angeführten Schwierigkeiten aus.

10.6

Zusammenfassung

Als eine Methode zur Durchführung eines IT-Risikomanagements ist an erster Stelle ein als Risikomanagement-Prozess ausgelegtes **Sicherheitskonzept** zu nennen. Die Erstellung eines solchen Sicherheitskonzepts ist immer dann angezeigt, wenn es bei Prozessen oder IT-Systemen darum geht, mit geeigneten Massnahmen die Risiken auf tragbare Restrisiken zu reduzieren. Und wenn sowohl die Beurteilung als auch die Art und Weise der Bewältigung der Risiken aufgezeigt und dokumentiert werden muss. Das Sicherheitskonzept kann sich auf die Sicherheitsaspekte des ganzen Lebenszyklus eines Systems (z.B. Beschaffung, Entwicklung, Einführung, Betrieb und Entsorgung) oder auch nur auf einzelne Phasen (z.B. Entwicklung oder Betrieb) beziehen. Wird das Sicherheitskonzept als Risikomanagement-Prozess verstanden, darf die Darstellung und Abwägung von Kosten, Nutzen und Wirksamkeit nicht fehlen. Der grosse Vorteil eines solchen Sicherheitskonzepts gegenüber einem „Baseline Verfahren“ ist, dass die Risiko-Ermittlung und die Massnahmenbestimmung abgestimmt auf das reale Objekt (resp. System) vorgenommen werden und sich die Massnahmen an den aktuell vorhandenen Risiken orientieren. Bei der schrittweisen Bearbeitung, insbesondere der drei letzten Kapitel, wird immer wieder die Wirksamkeit der Massnahmen hinsichtlich der eingeschlage-

nen Behandlungs-Strategien überprüft werden müssen. Das Sicherheitskonzept eignet sich auch zur Dokumentation der Risiken und Massnahmen und zur „Besiegelung“ von Einverständnissen der zuständigen Führungspersonen.

Die **CRAMM-Methode** ist ursprünglich für den Einsatz in Regierungsstellen des United Kingdom entwickelt worden. Die Methode sollte mit einer entsprechenden Software sowohl die Risiko-Analyse unterstützen als auch den analysierten Risiken angemessene Massnahmen zuordnen können. Das Software-Tool gibt die Schritte für einen durchzuführenden „Risk Management Review“ vor.

Grob sind dies die folgenden Schritte:

1. Festlegen der Rahmenbedingungen und System-Abgrenzungen für den Review;
2. Identifikation der Schutzobjekte (Assets) und Konstruktion des für das zu untersuchende system-spezifische Schutzobjekt-Modell (Asset Model);
3. Bewertung der Schutzobjekte (Asset valuation);
4. Erhebung und Einstufung der Bedrohungen (Threat assessment) und der bei diesen Bedrohungen massgeblichen Schwachstellen (Vulnerability assessment);
5. Risiko-Bestimmung;
6. Massnahmenzuordnung;
7. Abschliessende Berichterstattung.

Die **Fehlermöglichkeits- und Einfluss-Analyse (FMEA)** ist eine „Bottom-up-Suche“ und zeigt, wo Einzelkomponenten zu Ausfällen und Auswirkungen auf den höheren Ebenen eines ganzen Systems oder Teilsystems führen können. Damit dient sie als „Schwachstellen-Analyse“, die insbesondere dem Aufzeigen von „Single point of Failures“ dienen kann. Falls mit korrektiven Massnahmen die „Single point of Failures“ nicht eliminierbar sind, können aufgrund des Analyse-Prinzips zumindest nach dem „What-if“-Prinzip (Was ist, wenn...?) Massnahmen herausgefunden werden, die den Störungs-Einfluss einer kritischen Komponente auf das Gesamtsystem mildern. Die FMEA kann in abgewandelter Form auch in der Informationstechnologie eingesetzt werden, wo es um die Gesamtverfügbarkeit von Systemen oder ganzen IT-Dienstleistungen aufgrund der Zuverlässigkeit einzelner Komponenten und einer bestimmten Anordnung der Komponenten im System geht.

Die **Fehlerbaum-Analyse** ist eine Top-Down-Analyse. Das heisst, bei dem Vorgehen werden deduktiv, ausgehend von einer bestimmten Fehlersituation respektive einem bestimmten Fehlerereignis, die ursächlichen Ereignisse gesucht, die eintreten müssen, um das übergeordnete unerwünschte Fehlerereignis auszulösen. Die solchermassen verknüpften möglichen Ereignisse führen zu einer Baumstruktur, die aufzeigt, welche untergeordneten Ereignisse wie eintreten müssen, damit das jeweilige übergeordnete Ereignis eintritt. Das Verfahren liefert das numerische Ergebnis einer Wahrscheinlichkeit, mit der das jeweils übergeordnete Ereignis eintritt. Müssen für den Eintritt eines Ereignisses die dafür ursächlichen Bedingungen gemeinsam auftreten, dann werden sie algebraisch (Boolesche Algebra) mittels eines logischen UND verknüpft. Genügt bereits eine der ursächlichen Fehler-Bedingungen (untergeordnetes Fehlerereignis), um das Fehlerereignis zu bewirken, dann wird diese Eigenschaft durch eine logische ODER-Verknüpfung abgebildet. Die ursächlichen Ereignisse sind wiederum Resultate weiterer ursächlicher Bedingungen, für welche auch wieder die logische Verknüpfung festgestellt werden muss. Die grundlegenden Fehlerereignisse werden als „Basisereignisse“ bezeichnet. Die Bäume zu konstruieren und die Wahrscheinlichkeiten für die Basisereignisse zu schätzen, ist bei Informationen und IT-Komponenten nicht trivial und bedarf einiger Erfahrung.

Bei der **Ereignisbaum-Analyse** gehen wir von einem Ereignis aus und untersuchen, welche Folgen dieses Ereignis im System haben kann. Das auslösende Ereignis kann der Ausfall einer Systemkomponente oder ein anderes Ereignis im System sein. Ausgehend vom auslösenden Ereignis wird ein Baum von links nach rechts gezeichnet, der sich nach jedem Suchschritt in zwei Äste aufteilt. Der Ast nach oben gibt ein positives Folgeereignis und der Ast nach unten jeweils ein negatives (schädliches) Folgeereignis an. Die Ereignisse an jedem Gabelungspunkt des Baumes sind mit Eintrittswahrscheinlichkeiten verbunden. Der Baum endet dort, wo das Schadensausmass am höchsten ist oder wo sich ein Unfall oder Schadensereignis in vollem Ausmass oder in einer für die Untersuchung sinnvollen Wahrscheinlichkeit präsentiert. Die Anwendung in der Informationssicherheit ist nur in Teilbereichen oder für gut zu definierende und bekannte Systemkonstellationen oder Teilaspekte (z.B. Brandschutz, Rechenzentrums-Standortbestimmung) sinnvoll.

10.7**Kontrollfragen und Aufgaben**

1. Nennen Sie fünf Beispiele von Anforderungen, die in einem Sicherheitskonzept neben den Risiken ebenfalls zu berücksichtigen sind.
2. In welchen Situationen erachten Sie die Erstellung eines IT-Sicherheitskonzepts als nützlich?
3. Nennen Sie die Überschriften der sechs Kapitel eines Sicherheitskonzepts.
4. Nennen und Beschreiben Sie einen wichtigen Prozess außerhalb dem Erstellungsprozess eines Sicherheitskonzepts.
5. In welchen Situationen führen Sie anstelle einer Risiko-Analyse eine Schwachstellen-Analyse durch?
6. Zeigen Sie die Hierarchie der Schutzobjekte-Kategorien bei CRAMM.
7. Was zeigt die FMEA-Methode?
8. Wie ist die Risikoprioritätenzahl bei FMEA definiert?
9. Welche Art von Ergebnis liefert die Fehlerbaum-Analyse?
10. Was liefert die Ereignisbaum-Analyse?
11. Fallstudie: Das Unternehmen „Interpay“ bietet ein Zahlungsportal im Internet für ca. 10' 000 Händler (Buchhändler, Computershops, Zeitschriftenhändler, Videotheken etc.) an. Als Zahlungsmittel für die Kunden der Händler können Kreditkarten, Einzahlungsscheine oder Zertifikate eingesetzt werden. Die den Internetkunden belasteten Geldbeträge werden monatlich mittels E-Banking der Hausbank des jeweiligen Händlers gutgeschrieben. Im Rahmen eines Projekts sollte nun folgende Zusatzdienstleistung für den Händler untersucht und mit entsprechenden Massnahmen realisiert werden:
 - Der Händler soll online 7 x 24 Std. „Umsatz“ und „Kassenbestand“ seiner Internet-Verkäufe über eine Internet-Verbindung ansehen können.
 - Für spontane Werbeaktionen soll der Händler weitere Informationen über die Käufer abfragen können: Name, Wohnort, Geschlecht, Alter, Familienstand, Beruf, Betragshöhe und Häufigkeit der Einkäufe.

Die Informationen über seinen „Umsatz“ und „Kassenbestand“ betrachtet der Händler aus Wettbewerbsgründen als sein Geschäftsgeheimnis.

Mit der Zusatzdienstleistung möchte Interpay die Wünsche der Händler erfüllen. Doch ist Interpay auch darauf bedacht, die Datenschutz-Vorschriften einzuhalten.

Sie sind Berater von Interpay und bearbeiten die Vorstellungen und Anforderungen von Interpay im Rahmen eines entsprechenden Sicherheitskonzepts.

Die folgenden Lösungsvorschläge von Interpay sind bei der Ausarbeitung des Sicherheitskonzepts zu beachten und mit weiteren allenfalls notwendigen Massnahmen zu ergänzen:

- Der Kunde des Händlers soll beim Kauf auf eine entsprechende Verwendung der eingegebenen Informationen und die Einhaltung des Datenschutzes hingewiesen werden (Informationsschutzklausel in den „Allgemeinen Geschäftsbedingungen“);
 - Der Zugriff des Händlers auf seine Verkaufsinformationen (u.a. Kassenstand) soll mittels SSL (Secure Socket Layer) und Übertragungs-Chiffrierung sowie Händler-Authentifizierung mittels Chipkarte erfolgen.
- a) In welche Kapitel des Sicherheitskonzepts nehmen Sie die bereits jetzt bekannten Informationen des Falles auf?
 - b) Nennen Sie die relevanten Informationssicherheits-Gefahren, die in das Risiko-Assessment einzubeziehen sind. Begründen Sie die Relevanz.
 - c) Für welche System-Ziele (Vertraulichkeit, Integrität“ und „Verfügbarkeit“) fallen bei der Dienstleistung allenfalls hohe Risiken an?
 - d) Bei der Durchführung des Risiko-Assessments mit einer „schwachen Authentisierung“ für den Internetzugriff der Händler wird ersichtlich, dass die Informationssicherheit ungenügend gewährleistet ist.

Welche Folge-Risiken gehen einerseits die Händler und andererseits die Firma „Interpay“ beim Einsatz einer schwachen Authentisierung für den Händler-Zugriff ein?

- e) Das Ergebnis der unter d) durchgeführten Risiko-Analyse wird in der Tabelle 1 sowie in der Risk Map (Abbildung 10.23) in der gezeigten Weise eingetragen.

Tabelle 10.1: Ergebnisse Risiko-Analyse für Authentisierung

R.- Nr.	Risiko-Bezeichnung	Schwache Authentisierung		Starke Authentisierung	
		Scha- den	Häu- figkeit	Scha- den	Häu- figkeit
R1	Risiko für Händler: „Abfluss von Geschäfts- Informationen an Konkurrenz“	gross	selten	?	?
R2	Reputationsrisiko für Händler: „Abfluss von Kunden-Informationen an Dritte“	mittel	selten	?	?
R3	Reputationsrisiko für Interpay: „Abfluss von Kunden- oder Geschäfts- Information an Dritte“	gross	oft	?	?

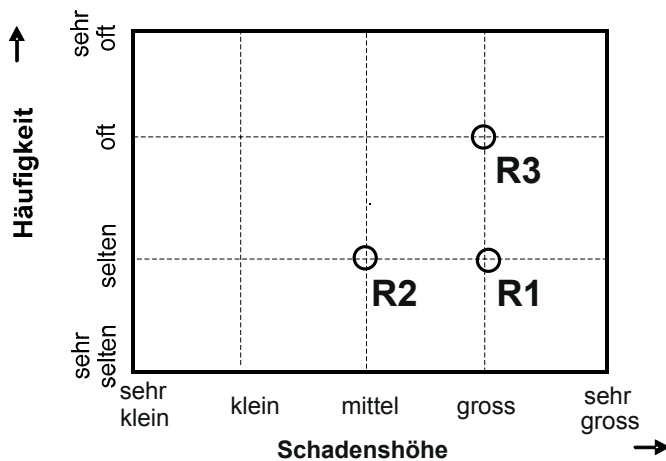


Abbildung 10.23: „Risk Map“ für Authentisierung

- f) Tragen Sie nun in die Tabelle 1 sowie in die Abbildung 10.23 ein, wie sich die Risiken 1, 2 und 3 nach Ihrer Einschätzung beim Einsatz einer starken Authentisierung verändern würden.
- g) Bei der Bearbeitung des Kapitels 5 im Sicherheitskonzept, „Definition und Beschreibung der Sicherheitsmassnahmen“ stellt sich heraus, dass der Einsatz der Chipkarte unverhältnismässig hohe Kosten verursacht. Welche alternative, kostengünstigere Händler-Authentisierung ist zu untersuchen?
- h) Schlagen Sie eine gangbare Lösung des Datenschutzproblems vor (Tipp: Werbeaktionen beziehen sich auf Kundensegmente und nicht auf einzelne Personen).
- i) Zeichnen Sie auch die „Restrisiken“ mit den unter g) und h) gewählten neuen Massnahmen in die obige „Risk Map“ ein.
- j) Welche Behandlungs-Strategie haben Sie gegen eine Kompromittierung der schutzwürdigen Daten gewählt, wenn Sie die Daten anonymisieren?

Die Risiko-Behandlungs-Optionen heissen:

- Risiken vermeiden
 - Risiken vermindern
 - Risiken überwälzen
 - Risiken bewusst tragen
- k) Erstellen Sie das IT-Sicherheitskonzept, das sowohl die neuen Leistungsanforderungen als auch den Datenschutz und das Geschäftsgeheimnis angemessen berücksichtigt.

Wie die IT-Risiken einerseits zu grossen, oder gar „existenzbedrohenden“ Verlusten in Unternehmen führen können, stellen andererseits oft auch die Kosten der Massnahmen für die Informationssicherheit verhältnismässig hohe Kostenblöcke dar.

Quantitative Aussagen

Deshalb werden im Rahmen der Strategie-, Investitions- und Budgetplanung oder zur Wertbestimmung bei Angeboten oder zu Kostenverrechnungen von Produkten und Dienstleistungen der IT vermehrt quantitative Aussagen über die Sicherheit verlangt.

Solche quantitativen Aussagen sollten nicht nur über die Risiken und Restrisiken sondern auch über die Kosten, die Wirksamkeit und die Angemessenheit der Massnahmen gemacht werden können.

Kosten/Nutzen-Nachweise

Wie für die IT-Prozesse im Allgemeinen sind auch für die Informationssicherheits-Prozesse im Besonderen Kosten-/Nutzen-Nachweise zu erbringen. Das Finden von betriebswirtschaftlich optimalen Sicherheitsmassnahmen, wie dies in Abbildung 10.1 veranschaulicht ist, setzt voraus, dass sowohl die Risiken wie auch die Massnahmen kostenmässig analysierbar sind. Für „faire“ Vergleiche gelten dabei als Massnahmenkosten sämtliche Kosten, die zur Behandlung der Risiken aufgewendet werden.

Kosten der Unternehmensrisiken

Eine solche quantitative Kostendarstellung ist meist schwer zu erfüllen. So können die **Kosten der Unternehmensrisiken** vor und nach der Massnahmen-Umsetzung meist nur aufgrund rudimentärer Annahmen bestimmt werden. Wie an verschiedenen Stellen des Buches gezeigt wird, liegen für die in der Zukunft zu „erwartenden“ Schadensereignisse oft komplexe Wirkungszusammenhänge aus Bedrohungen, Schwachstellen und Schadenshöhen vor. Für die mit geringer Wahrscheinlichkeit auftretenden „unerwarteten“ grossen Schadensereignisse ist in der Regel ungenügend statistisches Zahlenmaterial vorhanden, um zuverlässige statistische Aussagen treffen zu können.

Kosten der Risikobewältigung

Ähnlich schwierig stellt sich meist die Erhebung (Berechnung) der **Kosten, der für die Risikobewältigung eingesetzten Massnahmen** dar. Die Hauptschwierigkeit bei der Massnah-

menkostenbestimmung liegt darin, dass für eine effiziente Sicherheit die Massnahmen möglichst inhärent in den IT-Systemen und IT-Prozessen verankert sein sollten und daher die Sicherheitskosten von den IT-Kosten schwer zu extrahieren sind.

*Massnahmen
inhärent
verankert*

So stellt sich beispielsweise bei der Aufschaltung eines neuen Benutzers an ein IT-System die Frage, welcher Kostenanteil der „normalen“ Leistungserbringung und welcher Kostenanteil der „Risiko-Minderung“ aufgrund der Zugriffskontrolle zuzuordnen sind. Solche Kosten können allenfalls lediglich grob geschätzt werden. Um dennoch eine über ein ganzes Unternehmen konsistente „verursachergerechte“ Erhebung der IT-Sicherheitskosten zu ermöglichen, sind für die einzelnen Bereiche entsprechend klare „Erhebungs-Richtlinien“ notwendig.

*Kostenerhebung
bei komplexen IT-
Systemen*

Ein weiteres Problem für die Kostenerhebung bei komplexen IT-Systemen ist die Tatsache, dass ein bestimmtes Risiko oft durch mehrere Massnahmen gemildert wird und umgekehrt eine bestimmte Massnahme der Reduktion mehrerer Risiken dienen kann. Auch haben Massnahmen oft Nebeneffekte, indem sie andere Risiken hervorrufen oder verstärken können. So rufen beispielsweise die Massnahmen zur Gewährleistung der Geheimhaltung meist erhöhte Risiken hinsichtlich der Verfügbarkeit der Informationen hervor (z.B. Kopierverbot der geheimen Schlüssel und damit verbundenes Verlustrisiko der chiffrierten Daten im Falle eines Schlüsselverlusts).

Für ein kleines Unternehmen mit einfacher Informatik-Unterstützung, z.B. einem PC für die Abwicklung der Zahlungs- und Buchhaltungsvorgänge, mag die Wirtschaftlichkeit der Sicherheitsmassnahmen (z.B. Virenschutz und Datensicherstellung) an einfachen Szenarien plausibel dargestellt werden können. Für die Sicherheit der Informationen und IT-Systeme grosser Unternehmen mit sicherheitskritischen Anwendungen ist ein umfassender quantitativer Nachweis der Sicherheitskosten und der Angemessenheit der Massnahmen schwierig und wird in der Praxis wie in der Wissenschaft kontrovers diskutiert.

*Unternehmens-
und
Geschäftsziele*

Wie aus den im Teil B dieses Buches beschriebenen Anforderungen hervorgeht, muss ja der Nutzen der Risiko-Bewältigung, einschliesslich der dafür eingesetzten Managementprozesse, letztlich an der Erfüllung der Unternehmens- und Geschäftsziele gemessen werden.

Lösungsansätze

Basierend auf den praktischen Erfahrungen des Autors werden in den folgenden Abschnitten die zum heutigen Zeitpunkt häufig diskutierten Lösungsansätze mit den entsprechenden praktischen Hinweisen dargestellt.

11.1

Formel für "Return on Security Investments" (ROSI)

Risiko-Exposure

Zur numerischen Berechnung der sogenannten „Rendite von Sicherheits-Investitionen“ (ROSI) wird vorab das mit Massnahmen zu reduzierende „Risiko-Exposure“ als ein pro Jahr zu erwartender Verlust dargestellt:

$$R_a = H_a \times S_E$$

wobei

R_a : jährlich zu erwartender Verlust;

H_a : Häufigkeit mit der ein Schadensereignis in einem Jahr eintritt;

S_E : Voraussichtliche durchschnittliche Kosten eines einzelnen Schadenereignisses.

Netto-

Verlustreduktion

Von diesem „erwarteten“ Verlust kann durch geeignete Massnahmen ein Anteil in der Höhe von E_a bewältigt werden. Sind die mit den Massnahmen reduzierten „erwarteten“ Verluste höher als die Kosten der Massnahmen pro Jahr, dann können wir von einer „Netto-Verlustreduktion“ durch die Sicherheitsmassnahme sprechen:

$$\text{Netto-Verlustreduktion} = E_a - T_a$$

wobei

E_a das bewältigte Risiko pro Jahr darstellt mit

$$E_a = R_a \times \text{Risikoreduktion [\%]}$$

und

T_a : Massnahmenkosten pro Jahr

Der jährlich verbleibende Restverlust ALE^* aus verbleibenden Risiken und Massnahmenkosten beträgt somit:

$$ALE = R_a - (E_a - T_a)$$

wobei

ALE : jährlich zu erwartender Restverlust

ROSI

Oft wird bereits die Netto-Verlustreduktion als ROSI bezeichnet [Isae06]. In Analogie zum ROI (Return on Investment) als Finanz-Kennzahl[†] wird der ROSI (Return on Security Investment)-Wert auch als Verhältniszahl ausgedrückt [Sonn06]:

$$ROSI = \frac{E_a - T_a}{T_a}$$

Die Herausforderungen im Umgang mit dieser Formel liegen bei der Einschätzung des Risikos und dessen Reduktion durch die Massnahmen sowie in der Erhebung respektive Berechnung der Massnahmenkosten.

Erwartungswert als Risikomass

Bereits der Umstand, dass für ROSI als Risikomass der Erwartungswert eingesetzt wird, zeigt, dass die Berechnung lediglich für relativ häufig auftretende Schadensereignisse gültig ist, wo ein Erwartungswert eine sinnvolle Risikoaussage liefert. Für die relativ seltenen „unerwarteten“ Schadensereignisse greift die ROSI-Berechnung zu kurz, indem sie mit dem Erwartungswert das Risiko ungenügend quantifiziert (s. Abschnitte 2.3 und 2.4). In Anbetracht der Schwierigkeiten, quantitative Risikogrössen zu ermitteln, werden in der praktischen Anwendung auch semi-quantitative Werte (Scores) eingesetzt [Sonn06].

Für die Ermittlung der Massnahmenkosten in einem Unternehmen zur Bewältigung der Sicherheitsrisiken wird im nächsten

* In der anglo-amerikanischen Literatur ist dieser jährlich zu erwartende Verlust unter der Bezeichnung „Annual Loss Exposure“ oder kurz ALE zu finden (vgl. [Sonn06]).

† Vorsicht: Analogien zur Finanzkennzahl ROI sind nicht ohne weiteres zulässig, da die Finanzkennzahl ROI eine Ertrags-Kennzahl darstellt, hingegen in eine ROSI-Berechnung keine Erträge eingehen.

Abschnitt ein Lösungsansatz gezeigt, der in komplexen IT-Umgebungen zu sinnvollen Ergebnissen führen kann.

11.2

Ermittlung der Kosten für die Sicherheitsmassnahmen

Um die Massnahmenkosten den reduzierten Risiken gegenüberstellen zu können, müssen wir vorab klären, was Massnahmenkosten der Informationssicherheit sind und was diese Kosten enthalten müssen.

Jahreskosten

Da das bewältigte Risiko auf die Periode eines Jahres bezogen wird, müssen auch die Massnahmenkosten auf ein Jahr umgerechnet werden. So sind beispielsweise die Sicherheitsinvestitionen mit Abschreibungsdauern von mehreren Jahren auf Jahreskosten umzurechnen:

Kosten-Kategorien

Generell können die Massnahmenkosten in die folgenden drei hauptsächlich Kategorien eingeteilt werden:

1. Investitionskosten: Einmalige Aufwendungen, um neue Hardware, Software zu beschaffen (einschliesslich Entwurf, Entwicklung und Kauf).
2. Einführungs- und Inbetriebnahmekosten: Einmalige Aufwendungen, um die Massnahmen in Betrieb zu nehmen und nach einer Gebrauchszeit wieder zu entsorgen.
3. Betriebskosten: Laufende Aufwendungen, um die Massnahmen zu betreiben und zu unterhalten.

Kostengliederung

Die weitere Kostengliederung von Sicherheitsmassnahmen wird sinnvollerweise nach ähnlichen Gesichtspunkten wie für die gesamten IT-Kosten vorgenommen.

Grob ist eine Gliederung wie folgt üblich:

- Personal: einmalige, laufende und sporadische Kosten
- Hardware: einmalige und laufende Kosten
- Software: einmalige und laufende Kosten
- Kosten für Massnahmen-Auswahl, und -Planung
- Kosten für Installation und Inbetriebnahme
- Externe Kosten (Externe Berater und Mitarbeiter)
- Betriebskosten für Raum und Einrichtung
- Kosten für Gebrauchs- und Verbrauchsmaterial sowie Entsorgungskosten
- Kosten für Betreuung und Pflege

Diese Grob-Aufteilung unterscheidet sich noch nicht von den IT-üblichen Kostenartengruppen.

sicherheitsrelevante Kostenarten

Die Kunst liegt nun im Füllen dieser Kostengruppen mit sicherheitsrelevanten Kostenarten für die Einzelmassnahmen, Sicherheitssysteme und Sicherheitsprozesse. Solche Kostenarten erhalten wir aus den „Sicherheitsfunktionen“, die den IT-Risiken zur Risiko-Reduktion gegenübergestellt werden.

Eingliederung von Sicherheitsfunktionen

Die Abbildung 11.1 veranschaulicht beispielhaft die Eingliederung von Sicherheitsfunktionen in die verschiedenen IT-Systemebenen und die Aufteilung der Kosten in Kostenarten.

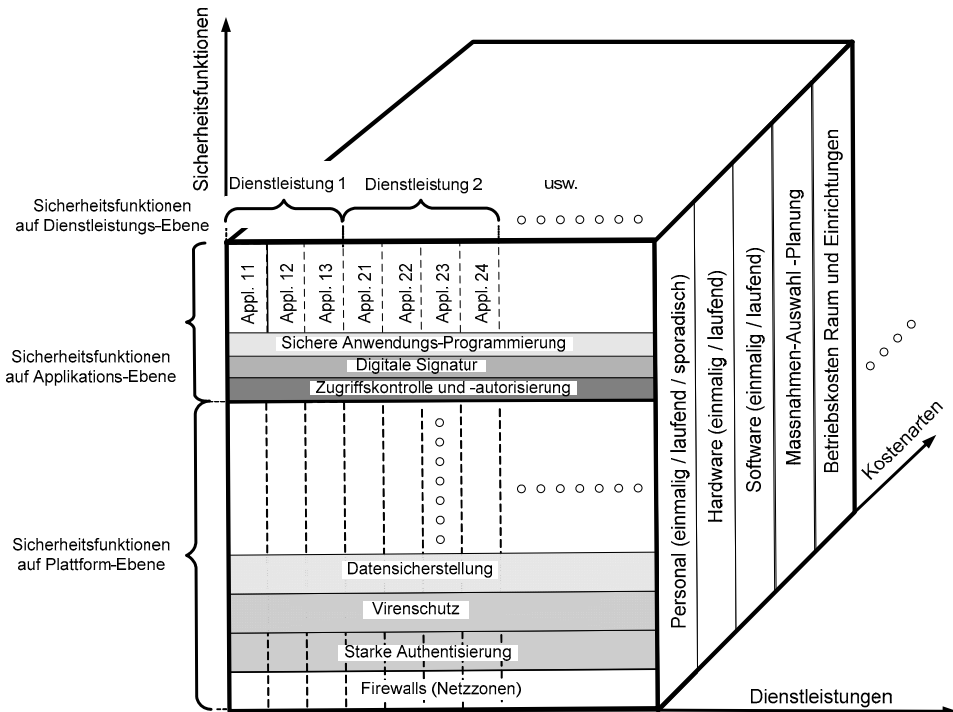


Abbildung 11.1 Prinzip der Massnahmen-Kostenrechnung

Wie für die Ermittlung der „normalen“ IT-Kosten können nun die Sicherheitskosten aus den Buchungs- und Inventarisierungssystemen der IT sowie mittels Zeitaufschreibungen für die Personalkosten erhoben werden.

Triage Sicherheitskosten / normale Kosten

Für die Triage in „IT-Sicherheitskosten“ und „normale IT-Kosten“ empfiehlt es sich, eine Policy mit Zuordnungs-Grundsätzen zu erstellen, mit der für die einzelnen Sicherheitsfunktionen im

Voraus klar festgelegt und kommuniziert wird, welche Aufwendungen als Sicherheitskosten zu erfassen sind.

Ein Policy-Grundsatz könnte beispielsweise heissen:

Alle für einen effizienten Normalbetrieb ohnehin notwendigen Tätigkeiten und Aufwendungen gelten nicht als Sicherheitskosten. (Der Grundsatz muss sicherlich mit einigen für das Unternehmen relevanten Beispielen untermauert werden.)

Indirekte Massnahmen-Kosten

In den Grundsätzen kann beispielsweise auch festgehalten werden, inwieweit „indirekte Massnahmen-Kosten“ einzubeziehen sind. Solche indirekten Massnahmen-Kosten sind beispielsweise:

- Systemleistungsverminderung durch Sicherheitsmassnahmen
- Betriebsbehinderungen durch überrestriktive Sicherheitsvorschriften
- Umständliche und unsichere Handhabung von Passwörtern
- Patching-Einflüsse
- Verfügbarkeitsrisiken durch Verschlüsselung

Divisions-Kalkulation

Werden die Sicherheitsfunktionen in grösseren „Stückzahlen“ eingesetzt (z.B. Smartcard zur starken Authentisierung), dann kann die Kostenerhebung auf Stückkostenbasis durchgeführt werden. Die Ermittlung der Stückkosten (respektive des Verrechnungspreises) erfolgt dann mittels einer „Divisions-Kalkulation“ (Kosten dividiert durch Anzahl) berechnet.

Vollkosten und Total Cost of Ownership

Werden die Kosten von Sicherheitsfunktionen in einer ROSI-Berechnung verwendet, dann sollten für eine faire Berechnung womöglich die „Vollkosten“^{*} sowie die in der IT-Kostenrechnung wichtige „Total Cost of Ownership“[†] angewendet werden.

^{*} Die Vollkostenrechnung berücksichtigt entgegen der Teilkostenrechnung auch die Kosten (Gemeinkosten), die nicht einem Kostenträger direkt zugerechnet werden können.

[†] Die „Total Cost of Ownership“ enthalten, zusätzlich zur Vollkostenrechnung, die alles umfassenden Gesamtkosten einer Investition über die gesamte Lebensdauer, einschliesslich der z.T. versteckten indirekten Kosten und der Folgekosten wie beispielsweise für die Entsorgung.

11.3**Ermittlung der Kosten der behandelten Risiken**

Im vorherigen Unterkapitel haben wir gesehen, welche Kosten für die einzelnen Massnahmen vorkommen können. In diesem Unterkapitel stellen wir uns die Frage, welche Kosten die Sicherheitsvorfälle zur Folge haben und mit welcher Häufigkeit solche Sicherheitsvorfälle auftreten. Von dem gesamten Risiko pro Jahr (R_a) wird durch die gewählte Massnahme in der Regel nur ein bestimmter Prozentsatz reduziert.

*Monetärer Wert
des Risikos*

Die Aufgabe besteht nun darin, zum einen den monetären Wert des Risikos vor dem Einsatz der Massnahme und zum anderen den Prozentsatz zu finden, mit dem eine gewählte Massnahme das Risiko (Impact und/oder Häufigkeit) reduziert.

*Quantitative
Analyse-Methoden*

Zur Analyse des Risikos und des „Restrisikos“ kommt gemäss den Ausführungen in Abschnitt 2.8 eine Reihe von „quantitativen“ Analyse-Methoden in Frage. Im konkreten Fall ist es nützlich, ein System-Modell* zu bilden und die Ereignis-Szenarien hinsichtlich der Gefahrenauswirkungen und zukünftiger Verluste zu untersuchen. So ist es beispielsweise sinnvoll, für Internet-Attacken (Würmer, Distributed Denial-of-Service-Attacken) die monetären Schadenswerte zu folgenden Schadenstypen (vgl. [Dübe05], S. 19-22) zu ermitteln:

- Ausfallzeit-Verlust (Einbussen an Produktivität und Umsatzerlösen während der Ausfallzeit)
- Wiederherstellungskosten (Personal- und Materialkosten)
- Haftungskosten (Kosten infolge Nichteinhaltung von Leistungen oder anderer Forderungen)
- Verluste durch Abfall von Kunden (Verlust aktueller und potentieller Kunden)

Die so berechenbaren Schäden beziehen sich jeweils auf ein einziges Schadensereignis. Für die Berechnung des Risikos ist nun noch die Abschätzung der Häufigkeit (pro Jahr) der voraussichtlichen Schadensereignisse notwendig.

* Interessant ist die in [Dübe04] anhand des Modells vorgenommene Schadenseinschätzung, die für den Fall einer „massiven“ DDOS-Attacke auf das Internet Schweiz (Totalausfall 1 Woche) einen wirtschaftlicher Schaden von CHF 6 Mia. ausweist.

*Anteil Risiko-
reduktion durch
Massnahmen*

Haben wir das Risiko vor dem Massnahmen-Einsatz ermittelt, dann stellt sich für die ROSI-Berechnung die Frage, welcher Anteil eines identifizierten Risikos durch die Massnahme(n) tatsächlich reduziert wird.

Dazu sind die beiden folgenden Fragen zu beantworten:

1. Inwieweit sind Modell und Szenario für das identifizierte Risiko zutreffend?
2. Inwieweit wird das identifizierte und analysierte Risiko durch die Massnahme tatsächlich gemildert?

Beide Fragen können bezüglich des durch eine Massnahme tatsächlich „ex ante“ zu bewältigenden Risikos weitreichende Konsequenzen haben und sind hinsichtlich einer fairen ROSI-Aussage sorgfältig zu klären. Dabei gilt es zu berücksichtigen, dass bei IT-Risiken für beide Fragen zum heutigen Zeitpunkt noch keine im mathematischen Sinne exakten Antworten verfügbar sind. Wie für die Einschätzung der Häufigkeiten wird stattdessen, unter Abwägung der verfügbaren Fakten, eine prozentuale Reduktion des vorab analysierten Risikos geschätzt werden müssen. Für die allenfalls notwendige spätere Verteidigung der Schätzung müssen die für die Schätzung berücksichtigten Fakten dokumentiert werden.

*Fehlende Abzin-
sung der Kapital-
beträge*

Eine weitere Schwäche des ROSI-Ansatzes für Sicherheits-Investitionsentscheide liegt auch in der fehlenden Abzinsung der Kapitalbeträge im Sinne einer Barwertberechnung. Eine solche Kapital-Abzinsung ist zwar bei den Massnahmen-Investitionen möglich. Hingegen fehlen bei der Risikobestimmung mit Erwartungswerten die Zeitparameter zur Berechnung eines Barwerts (Discounted Cash Flow).

Praxistipp:

Bei komplexen IT-System-Modellen oder für seltene Ereignis-Szenarien (unerwartete Verluste) liefert eine ROSI-Berechnung fragwürdige Resultate und sollte in solchen Fällen nicht für Realisierungsentscheide herangezogen werden.

11.4

Massnahmen-Nutzen ausgerichtet an Unternehmenszielen

Sowohl aufgrund der Mängel des ROSI-Ansatzes hinsichtlich seltener Ereignisse als auch der fehlenden Ausrichtung von Risiken und Massnahmen an Geschäftszielen muss der ROSI-Ansatz

zumindest als Basis für Realisierungsentscheide von Informationssicherheits-Massnahmen in Frage gestellt werden.

Nutzenfrage

In einem ganzheitlichen integrierten Risikomanagement-Ansatz lautet die Nutzenfrage nicht primär, was die Einsparungen an Risiko- und Massnahmenkosten sind, sondern inwieweit die Sicherheitsprozesse und -massnahmen die Strategieziele des Unternehmens unterstützen. Mit einer solchen Fragestellung sind die Investitionsentscheide über Sicherheitsmassnahmen in den Unternehmensstrategie- und -Risikomanagementprozess eingebunden, wie dies im Kapitel 5 dargestellt wurde.

Umsetzung Sicherheitsziele

Wie die definierten Sicherheitsziele im Einzelnen umgesetzt werden können, zeigt uns der Ansatz mit der Balanced Scorecard im Abschnitt 5.4.3. Die IT unterstützt in diesem Ansatz die Geschäftsziele. Die diesbezüglichen Anforderungen können anhand von Prozessen, Informationskriterien, Performance-Indikatoren und Risk-Indikatoren beschrieben und analysiert werden.

Ein solches integriertes Vorgehen liegt dem CobiT-Rahmenwerk des „IT Governance Instituts“ (ITGI) mit seinen Zusatz-Rahmenwerken „Val IT“ und „Risk IT“ zugrunde. Auch der Standard ISO/IEC 27001 fordert die Ausrichtung des Sicherheitsmanagements am strategischen Risikomanagement des Unternehmens.

Nutzengenerierung durch IT

Das „IT Governance Institut“ verknüpft die Nutzengenerierung durch die IT ganz allgemein mit der Unternehmens-Governance und dem Management von Risiken und Chancen. Die Relation von Aufwand und Nutzen von Sicherheitsmassnahmen wird damit auf die geschäftliche Ebene der Wertegenerierung des Unternehmens angehoben. Dabei dient das Rahmenwerk unter der Bezeichnung „Val IT“ vor allem dem Management der Unternehmenswerte durch die IT und ergänzt damit das im Abschnitt 9.4 behandelte CobiT-Rahmenwerk (s. Abbildungen 11.2 und 11.3).

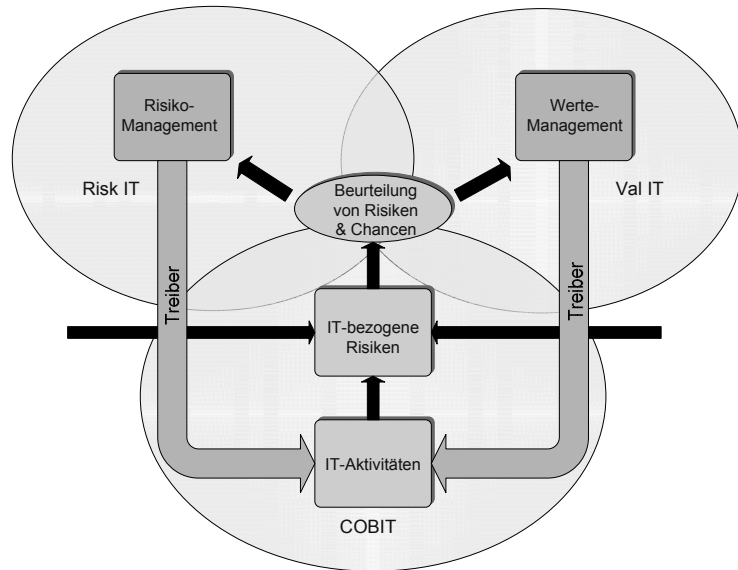


Abbildung 11.2: Risiken und Chancen in den ITGI Rahmenwerken [Itgr09]

Das neue in das CobiT 5 integrierte Rahmenwerk „Risk IT“ dient dem Management von IT-Risiken und zwar auch solchen, die nicht ausschliesslich der Informationssicherheit zuzuordnen sind, sondern die gesamte IT-Leistung im Unternehmen betreffen (z.B. Compliance-Risiken, Projektrisiken und Nutzenrisiken).

*Rahmenwerke
Risk IT, Val IT
und CobiT*

Die drei Rahmenwerke CobiT, Val IT und Risk IT ergänzen sich gegenseitig, wie dies in Abbildung 11.2 veranschaulicht wird. Die Frage nach einem Nutzen der Massnahmen (u.a. der Sicherheitsmassnahmen) wird durch alle drei sich gegenseitig unterstützenden und ergänzenden Rahmenwerke beantwortet. Um das ganzheitliche Konzept der Nutzengenerierung durch die IT zu veranschaulichen, werden die beiden Rahmenwerke Val IT und Risk IT nachfolgend in ihren Grundzügen dargestellt.

11.4.1

Grundzüge von Val IT

*Effektivität von IT-
Investitionen*

Die unter Val IT definierten Prozesse widmen sich zum einen der Effektivität von IT-Investitionen im Einklang mit der Unternehmensstrategie und unterstützen so die IT-Governance; zum anderen helfen sie bei der Realisierung des optimalen Nutzens aus den IT-Prozessen.

Unternehmens-Strategie:**Investition unter Beachtung**

- Vision
- Geschäfts-Grundsätze
- Strategische Ziele
- Optimale Werte zu erschwinglichen Kosten und akzeptablen Risiken

IT-Architektur:**Investition unter Beachtung**

- Architektur
- Architektur-Grundsätze
- Architektur-Population
- Andere Initiativen

Unternehmens-Werte:

- Klare und gemeinsames Verständnis über den erwarteten Nutzen
- Klare Verantwortlichkeiten zur Nutzen-Realisierung
- Relevante Metriken
- Effektiver Prozess zur Nutzen-Realisierung

IT-Lieferung:

- Effektive und disziplinierte Management-, Lieferungs- und Change-Management-Prozesse
- Kompetente technische und geschäftliche Ressourcen um
 - die verlangten Fähigkeiten und
 - den notwendigen organisatorischen Wandel zu liefern

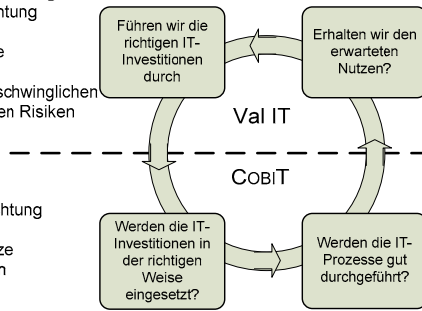


Abbildung 11.3 Zusammenspiel von CobiT und Val IT [Itgv08]

Prozesse in
Val IT

Die Prozesse von Val IT sind in folgende drei Hauptgruppen (Domänen) unterteilt [Itgv08]:

Domänen in
Val IT

Werte-Governance (VG): diese sorgt für eine klare Verbindung zwischen der Unternehmens-Strategie und einem Portfolio von Investitionsprogrammen und dem Portfolio bestehend aus IT-Services, Ressourcen etc.

Portfolio-Management (PM): Verwaltung des Portfolios von IT Investitionen zur Wertoptimierung im Unternehmen.

Investitions-Management (IM): damit werden die einzelnen Investitionen anhand der folgenden drei Instrumente verwaltet:

1. „Business Case“ zur Auswahl der Investitionsmassnahmen,
2. Programm-Management zur Umsetzung der in den Programmen definierten Projekte und
3. Nutzenrealisierung gemäss dem Business Case.

Ziele und
Metriken

In der für CobiT üblichen Weise sind die Domänen und Prozesse mit Zielen und Metriken hinterlegt.

Business Case
in Val IT

Ein zentrales Instrument von „Val IT“ ist der „Business Case“. Der Business Case behandelt Fakten und Analysen über alle Lebenszyklus-Phasen einer Investition oder eines Investitionsprogramms. Als Ergebnis soll er eine umfassende Begründung für den Investitionsentscheid liefern. In den einzelnen Entwicklungsschritten (s. Abbildung 11.4) spielen die Schritte „Risiko-Analyse“ sowie „Abschätzung und Optimierung von Risiko und Ertrag“

eine wichtige Rolle. In dieser ganzheitlichen Betrachtung ist der Ertrag für das Geschäft aus der IT-Lieferung zu berücksichtigen. Demzufolge hat die Risiko-Optimierung hinsichtlich der Ausrichtung auf die Unternehmensziele zu erfolgen.

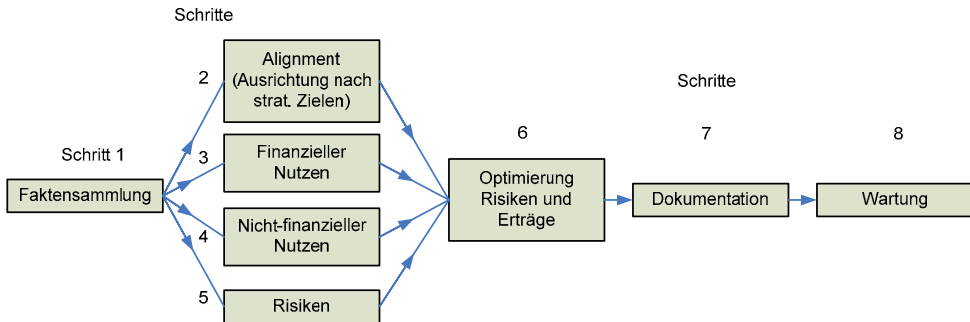


Abbildung 11.4: Entwicklungsschritte des Business Case bei Val IT [Itgv08]

Hinsichtlich der Verfahren zur Risiko-Einschätzung bleibt die Anleitung in VAL IT für den Business Case noch vage. Dem vorgeschlagenen Vorgehen entsprechend, erfüllen Risiko-Masszahlen in der Form von Kennzahlen (Key Risk Identifiers) und „Scores“ den Zweck. Das Risikomanagement selbst wird im dafür bestimmten Dokument „Risk IT“ ausführlich behandelt.

Die Grundzüge von Risk IT werden entsprechend der derzeit erhältlichen Entwurfsfassung [Itgr09] im folgenden Abschnitt behandelt.

11.4.2

Grundzüge von Risk IT

Wie bei den Rahmenwerken COBIT und VAL IT basiert das Risk-IT-Rahmenwerk auf einer Anzahl Prozesse, die in die folgenden drei Hauptgruppen (Domänen) unterteilt sind [Itgr09]:

*Domänen
in Risk IT*

Risiko-Governance (RG): diese sorgt für die Einbettung des IT-Risikomanagements in das Unternehmen und gewährleistet damit, dass die Erträge risikoadjustiert sind.

Risiko-Bewertung (RE): damit wird sichergestellt, dass die IT-bezogenen Risiken und Chancen identifiziert, analysiert und in Geschäftsbegriffen ausgewiesen werden. Die Analyse und Bewertung der Risiken erfolgt anhand von „Key Risk Indikatoren“. Die Key Risk Indikatoren sollten beispielsweise anhand der folgenden Kriterien definiert werden (vgl. [Itgr09], S. 29):

*Key Risk
Indikatoren*

- Sensitivität: Indikatoren müssen repräsentativ und zuverlässig hinsichtlich dem anzuzeigenden Risiko sein
- Impact: Indikatoren müssen vorwiegend Risiken mit hohen Geschäfts-Impact aufzeigen
- Messaufwand: Bevorzugung von einfach zu benutzenden Indikatoren
- Zuverlässigkeit: Indikatoren müssen möglichst genau das Risiko und möglichst gute Vorhersagen und Ergebnisse wiedergeben

Risiko-Reaktion (RR): damit wird gewährleistet, dass die IT-bezogenen Risiko-Fragen, Chancen und Ereignisse in einer kostenwirksamen Weise und in einer geschäftsrelevanten Prioritätenfolge behandelt werden.

*Prozesse in
Risk IT*

Die Prozesse in diesen drei Domänen sind die folgenden:

Risiko-Governance (RG):

Aufbau und Unterhalt einer gemeinsamen Risiko-Sicht (RG1)

Integration in das Unternehmens-Risikomanagement (RG2)

Risikobewusste Geschäftsentscheide (RG3)

Risiko-Bewertung (RE):

Erheben von Daten (RE1)

Analysieren der Risiken (RE2)

Unterhalt von Risiko-Profilen (RE3)

Risiko-Reaktion (RR):

Aufzeigen von Risiken und Findings (RR1)

Behandlung der Risiken (RR2)

Reaktionen auf Ereignisse (RR3)

Diese Prozesse besitzen jeweils eine Prozessbeschreibung und ein Prozessziel und sind zusätzlich in eine Anzahl von Schlüsselaktivitäten aufgeteilt. Diese Schlüsselaktivitäten besitzen Inputs und Outputs zu anderen Prozessen sowohl im Risk-IT-Rahmenwerk als auch in den beiden Rahmenwerken Val IT und CobiT. Sämtliche Domains, Prozesse und Aktivitäten sind mit Zielen und Metriken versehen. Die Vernetzungen der Prozessaktivitäten über Inputs und Outputs an andere Prozessaktivitäten sorgen für die Erfüllung der dem Unternehmenswert dienlichen effektiven Massnahmenentscheide.

Beispiel Vernetzung Prozessaktivitäten

Beispiel:

Die Vernetzung der Prozessaktivitäten von Risk IT soll am Beispiel der zum Prozess RR2 gehörenden Prozess-RR2.3 demonstriert werden (s. Tabellen 11.1 und 11.2):

Die Aktivität RR2.3 lautet: „Reaktion auf eine Risiko- und Chancen-Ermittlung“. Zusammengefasst beinhaltet die Aktivität das Abwägen und Priorisieren einer Risiko-Reduktionsmassnahme unter Berücksichtigung der strategischen Geschäftsentscheidungs-Prozesse unter Einhaltung der vorgegebenen Risiko-Toleranz.

Tabelle 11.1 Inputs zu Risk IT Aktivität RR 2.3 [Itgr09]

Von Prozess-Aktivität	Inputs
RG3.3	Kosten und Nutzen über ganzen wirtschaftlichen Lebenszyklus
RG3.4, RR3.4	Anforderungen an Risiko-Reaktion
RG 3.5	Nutzen aus Risikomanagement für IT-Portfolio
Val IT IM5	Investitionsprogramm-Plan
COBIT PO1	IT-Projekt-Portfolio
COBIT PO1	IT-Sourcing-Strategie
COBIT PO2	IT-Architektur
COBIT PO3	Technology-Infrastruktur-Plan
COBIT PO5	IT-Budgets

Tabelle 11.2 Outputs von Risk IT Aktivität RR 2.3 [Itgr09]

An Prozess-Aktivität	Outputs
RG2.3, RG3.3, RR2.4, Val IT PM4, COBIT PO9, PO10	Risiko-Programme
RG3.4, COBIT PO4, PO9, ME1, ME2	Risiko- und Massnahmen-Wirksamkeitsberichte
COBIT PO9, Val IT IM1	IT-Risiko-Reaktions-Definition

11.5**Fazit zu Ansätzen der Sicherheit-Nutzen-Bestimmung**

*Wertegenerierung
und Nutzenbe-
trachtung*

Die Rahmenwerke „Risk IT“, „Val IT“ und „COBIT“ des ITGI kommen den Anforderungen von zielgerechten Massnahmen in einem integrierten IT-Risikomanagements entgegen. Die auf einzelne Risiken und Massnahmen bezogene isolierte Nutzenbetrachtung des ROSI-Ansatzes wird mit dem ganzheitlichen ITGI-Ansatz vermieden. Auch begegnet der ITGI-Ansatz der Schwierigkeit von absoluten quantitativen Kostenberechnungen, indem die Bewertungsmetriken auf qualitativen Kennzahlen (z.B. Key-Risk-Indikatoren und Performance-Indikatoren) beruhen.

Das Finden geeigneter Kennzahlen, welche sowohl die an den Unternehmenszielen und Risiken zu messende Effektivität (Wirksamkeit) als auch die Effizienz (Wirtschaftlichkeit) wiedergeben, wird zukünftig eine gute Ergänzung oder gar eine Alternative zum ROSI-Ansatz darstellen.

11.6**Zusammenfassung**

Zur numerischen Berechnung der sog. „Rendite von Sicherheits-Investitionen“ (ROSI = Return on Security Investments) werden von dem durch geeignete Massnahmen reduzierten Verlustanteil E_a eines „erwarteten“ Verlusts R_a die Massnahmenkosten pro Jahr T_a subtrahiert: $ROSI = E_a - T_a$.

Die Herausforderungen im Umgang mit dieser Formel liegen bei der Einschätzung des Risikos und der Erhebung respektive Berechnung der Massnahmenkosten.

Bereits der Umstand, dass für ROSI als Risikomass der Erwartungswert eingesetzt wird, zeigt, dass die Berechnung lediglich für relativ häufig auftretende Schadensereignisse gültig ist, wo auch ein Erwartungswert sinnvoll erhoben werden kann. In der praktischen Anwendung können aber auch semi-quantitative Werte (Scores) eingesetzt werden.

Zur Ermittlung der Sicherheitsmassnahmen-Kosten in einem Unternehmen wird die Kostengliederung sinnvollerweise nach ähnlichen Gesichtspunkten wie für die gesamten IT-Kosten vorgenommen. Wie für die Ermittlung der „normalen“ IT-Kosten können die Sicherheitskosten aus den Buchungs- und Inventarisierungssystemen der IT sowie mittels Zeitaufschreibungen für die Personalkosten erhoben werden.

Für die Triage in „IT-Sicherheitskosten“ und „normale IT-Kosten“ empfiehlt es sich, eine Policy mit Zuordnungs-Grundsätzen zu erstellen, mit der für die einzelnen Sicherheitsfunktionen im Voraus klar festgelegt und kommuniziert wird, welche Aufwendungen als Sicherheitskosten zu erfassen sind.

Werden die Sicherheitsfunktionen in grösseren „Stückzahlen“ eingesetzt (z.B. Smartcard zur starken Authentisierung), dann kann die Kostenerhebung auf Stückkostenbasis durchgeführt werden. Werden die Kosten von Sicherheitsfunktionen in einer ROSI-Berechnung verwendet, dann sollten womöglich die „Vollkosten“ sowie die in der IT-Kostenrechnung wichtige „Total Cost of Ownership“ angewendet werden.

Zur Analyse des Risikos und des „Restrisikos“ kommen gemäss Abschnitt 2.8 verschiedene „quantitative“ Analyse-Methoden in Betracht. Ist das Risiko vor dem Massnahmen-Einsatz ermittelt, dann stellt sich für die ROSI-Berechnung die Frage, welcher Anteil des Risikos durch die Massnahme(n) tatsächlich reduziert wird. Dafür wird, unter Abwägung der verfügbaren Fakten, eine prozentuale Reduktion des vorab analysierten Risikos geschätzt werden müssen.

Aufgrund der Schwächen des ROSI-Ansatzes empfiehlt es sich, bei komplexen IT-System-Modellen oder für seltene Ereignis-Szenarien (unerwartete Verluste), die ROSI-Berechnung nicht für Realisierungsentscheide heranzuziehen.

In einem ganzheitlichen integrierten Risikomanagement-Ansatz wird der Nutzen nicht primär daran ermesen, was die Einsparungen an Risiko- und Massnahmenkosten sind, sondern inwieweit die Sicherheitsprozesse und -massnahmen die Strategieziele des Unternehmens unterstützen.

Ein solches integriertes Vorgehen liegt dem CobiT-Rahmenwerk des „IT Governance Instituts“ (ITGI) mit seinen Zusatz-Rahmenwerken „Val IT“ und „Risk IT“ zugrunde. Auch der Standard ISO/IEC 27001 fordert die Ausrichtung des Sicherheitsmanagements am strategischen Risikomanagement des Unternehmens.

Das „IT Governance Institut“ knüpft dabei die Nutzengenerierung durch die IT ganz allgemein an die Unternehmens-Governance und das Management von Risiken und Chancen.

Die drei Rahmenwerke des „CobiT“, „Val IT“ und „Risk IT“ ergänzen sich gegenseitig. Die Frage nach einem Nutzen der Massnahmen (u.a. der Sicherheitsmassnahmen) wird durch alle

drei sich gegenseitig unterstützenden und ergänzenden Rahmenwerke beantwortet.

Die unter Val IT definierten Prozesse sind in die folgenden drei Hauptgruppen (Domänen) unterteilt:

Werte-Governance (VG)

Portfolio-Management (PM)

Investitions-Management (IM)

Ein zentrales Instrument von Val IT ist der "Business Case"; dieser behandelt Fakten und Analysen über alle Lebenszyklus-Phasen einer Investition oder eines Investitionsprogramms. Als Ergebnis soll er eine umfassende Begründung für den Investitionsentscheid liefern.

Das Risikomanagement basiert auf Kennzahlen (Key Risk Identifiers) und „Scores“ und wird im dafür bestimmten Dokument „Risk IT“ ausführlich behandelt. Dieses Framework ist in die folgenden Hauptgruppen (Domänen) und Prozesse unterteilt:

Risiko-Governance (RG):

Aufbau und Unterhalt einer gemeinsamen Risiko-Sicht (RG1)

Integration in das Unternehmens-Risikomanagement (RG2)

Risikobewusste Geschäftsentscheide (RG3)

Risiko-Bewertung (RE):

Erheben von Daten (RE1)

Analysieren der Risiken (RE2)

Unterhalt von Risiko-Profilen (RE3)

Risiko-Reaktion (RR):

Aufzeigen von Risiken und Findings (RR1)

Behandlung der Risiken (RR2)

Reaktionen auf Ereignisse (RR3)

Sämtliche Domains, Prozesse und Aktivitäten sind mit Zielen und Metriken versehen. Die Vernetzungen der Prozessaktivitäten über Inputs und Outputs an andere Prozessaktivitäten (auch von CO-BIT und VAL IT) sorgen für effektive Massnahmenentscheide. Das Finden geeigneter Kennzahlen, welche sowohl die an den Unternehmenszielen und Risiken zu messende Effektivität (Wirksamkeit) als auch die Effizienz (Wirtschaftlichkeit) wiedergeben, wird zukünftig eine Ergänzung oder eine Alternative zum ROSI-Ansatz darstellen.

11.7**Kontrollfragen und Aufgaben**

1. Ein Unternehmen stellt seinen Mitarbeitern „Remote Access“ mittels PC über das Internet zum Zugriff auf eine Firmen-Datenbank und zum Zugriff auf das Firmen E-Mail zur Verfügung. Die Authentisierung des Benutzers erfolgt mit einem einfachen Passwort. Im vergangenen Jahr konnten 10 Hacking-Attacken auf die Datenbank und auf E-Mail-Accounts registriert werden. Der durch diese Attacken verursachte Schaden betrug insgesamt 100' 000 €. Mit dem geplanten Einsatz einer „starken Authentisier-Methode“ wird erwartet, dass die Anzahl von Attacken auf eine im Zeitraum von zwei Jahren reduziert werden können. Die Einführung und der Betrieb der Massnahme führt zu jährlichen Kosten von 50' 000 €.

Berechnen Sie mit der ROSI-Formel den ROSI-Wert.

2. Ein Unternehmen hat auf seinen Arbeitsplatz-PCs veraltete Viren-Scanner im Einsatz. Im letzten halben Jahr mussten 5 Viren-Verseuchungen bereinigt werden. Die Kosten für den Bereinigungsaufwand und den Produktionsausfall aufgrund der Nichtverfügbarkeiten betrug 50' 000 €. Der Anschaffungswert und die Betriebsmehrkosten eines neuen „Scanning Tools“ beträgt 40' 000 €. Es wird erwartet, dass mit dem neuen Tool statt der fünf lediglich noch eine Virus-Verseuchung pro Jahr eintritt.

Berechnen Sie den ROSI-Wert.

3. Diskutieren Sie die Nützlichkeit der ROSI-Berechnungen in den beiden oben angeführten Fällen (Aufgabe 1 und Aufgabe 2).
4. Zur Fällung von Investitionsentscheiden in den in Aufgaben 1 und 2 angeführten Problemen können die Rahmenwerke „VAL IT“ und „Risk IT“ beigezogen werden. Nennen Sie wichtige Aktivitäten, die zwangsläufig durchgeführt werden müssen, um die Entscheide zu fällen.
5. Schlagen Sie einige Kennzahlen vor, die der Analyse und Lösung der in den Aufgaben 1 und 2 angeführten Probleme dienlich sind.

Teil D

Unternehmens- Prozesse meistern

Im Teil B dieses Buches haben wir die Anforderungen an ein RM im Unternehmen aufgezeigt. Aus diesen Anforderungen ging hervor, dass das RM auf höchster Unternehmensebene zur Frühwarnung und Steuerung der Risiken im Gesamtunternehmen für eine gute Corporate Governance unerlässlich ist. Die Einblicke in das Führungssystem zeigten, dass das Risikomanagement Einfluss auf die Strategiefindung im Unternehmen haben muss. Um den Erfordernissen einer risikoabhängigen Strategiefindung bezüglich Strategien und Massnahmen gerecht zu werden, ist sogar die Integration des RM in den Führungs- und Strategieprozess des Unternehmens zu empfehlen.

Im Teil C wurden Modelle, Methoden und Verfahren für das Management der Informationssicherheits- und der IT-Risiken beleuchtet. Ausgehend von den Erläuterungen in Abschnitt 6.5 werden die beiden Prozesse des Informationssicherheits-Managements und des IT-Risikomanagements in einem einzigen Risikomanagement-Prozess mit der Bezeichnung Informations-Risikomanagement zusammengelegt. Die Differenzierung der unterschiedlichen Risiken findet über die Risikoarten und in der Unterscheidung der Informationskriterien (Systemziele) statt (s. Abschnitt 6.3). Selbstverständlich liegt es in der Eigenheit des Unternehmens die beiden Bereiche Informationssicherheits-Governance und IT-Governance auch mit jeweils eigenständigen Risikomanagement-Prozessen und Management-Rollen (Risk Manager, Security Officer usw.) zu behandeln.

In diesem Teil D des Buches wird veranschaulicht, wie der Informations-RM-Prozess und auch andere RM-Prozesse mit dem Gesamt-RM-Prozess und dem Strategie-Prozess verzahnt werden können. Auch werden die aus der Sicherheits-Perspektive des Unternehmens wichtigen Prozesse der „Geschäftskontinuitäts-Planung“, des „Vulnerability Management“, des „Incident Management“, des „Outsourcing“ und der Auslagerung auf „Cloud-Computing“ aufgezeigt.

12.1**Verzahnung der RM-Prozesse im Unternehmen**

Der Forderung eines Gesamt-RM-Prozesses wird nicht widersprochen, wenn in Teilbereichen eines Unternehmens, z.B. in einer Geschäftseinheit, in einem strategischen Geschäftsfeld, in einzelnen Gruppengesellschaften oder in einzelnen Organisationseinheiten spezifische RM-Prozesse durchgeführt werden.

*Kompatibilität
für Gesamt-RM-
Prozess*

Für einen sinnvollen Gesamt-RM-Prozess müssen jedoch die untergeordneten, nachgeordneten oder übergeordneten Risikomanagement-Prozesse untereinander kompatibel sein.

Mit anderen Worten, die Risiko-Informationen als Output des einen Prozesses müssen als Input bei einem anderen Prozess richtig interpretiert werden können.

*Informationen
über grösste
Risiken*

So erhält beispielsweise der übergeordnete Gesamt-RM-Prozess von einem Informations-RM-Prozess die Assessment-Ergebnisse über die grössten Informations-Risiken. Bestehen bereits Massnahmen, dann werden die Restrisiken und die für die Risiko-Bewältigung eingesetzten Massnahmen an den übergeordneten RM-Prozess „berichtet“.

*Neue Risiko-
Bewertung*

Das Mittel dazu kann der in Abschnitt 2.6.4 vorgestellte Risiko-Katalog sein. Aus der Sicht aller Unternehmens-Risiken und deren Vernetzungen untereinander müssen diese Risiken (resp. Restrisiken) allenfalls neu bewertet werden.

*Entscheide über
Risiko-
Bewältigung*

Von der Ebene des Gesamt-RM-Prozesses werden die Entscheide über die Risiko-Behandlung (z.B. einzuschlagende Risiko-Strategie, Aktionspläne oder Budgets für Massnahmen) an die untergeordneten Risikomanagement-Prozesse zurückgegeben (Abbildung 12.1).

Betrachten wir einen Informations-Risikomanagement-Prozess als einen dem Geschäfts-RM-Prozess nachgeordneten RM-Prozess, dann müssen der Geschäfts-RM-Prozess und der Informations-RM-Prozess ebenfalls kompatibel zueinander sein, da die Informations-Risiken innerhalb der Geschäftsrisiken meist eine wesentliche Rolle spielen. Diese Situation ergibt sich beispielsweise beim „Geschäftskontinuitäts-Plan“, in welchem der nachgeordnete „IT-Notfall-Plan“ entscheidend zur Geschäftskontinuität beiträgt.

*Zeitlich aufei-
nander abge-
stimmte RM-
Prozesse*

Die untereinander kommunizierenden RM-Prozesse müssen auch zeitlich aufeinander abgestimmt sein. Besteht beispielsweise das strategische Ziel, einen bestimmten Geschäftsprozess oder Teile davon zu „outsourcen“, dann sind die Informations-Risiken und

deren Konsequenzen vor dem Strategie-Beschluss durch die Fachstellen der Informations-Sicherheit zu analysieren.

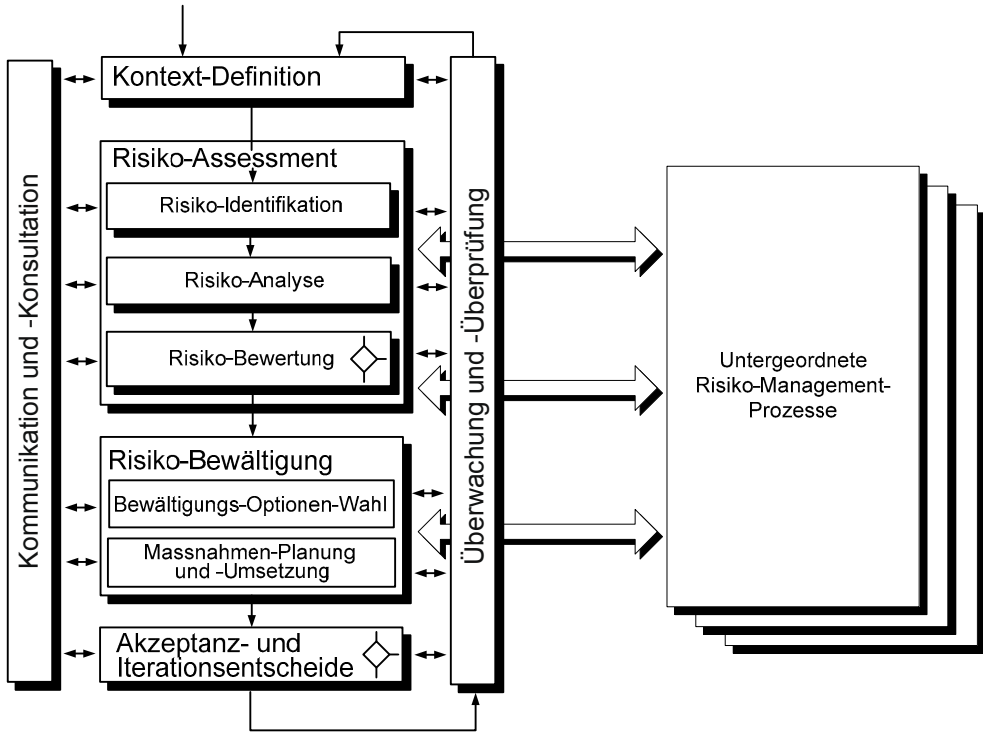


Abbildung 12.1 RM-Prozess mit Sub-RM-Prozessen

12.1.1 Risiko-Konsolidierung

Zur Gewährleistung der Kompatibilität von übergeordneten mit untergeordneten und nebengeordneten Risikomanagement-Prozessen ist, ähnlich einer „Konzernrechnung“, eine Konsolidierung der Risiken notwendig.

Risiken dürfen nicht addiert werden

Im Gegensatz zu den Rechnungslegungsinformationen sind die Risiken statistische Werte, die meist gewisse statistische Abhängigkeiten untereinander haben (Korrelationen). Die Werte dürfen deshalb nicht, wie beispielsweise in einer konsolidierten Buchführung, einfach addiert werden, sondern sind entsprechend ihrer Korrelationen zu aggregieren. Die quantitative Aggregation von Einzelrisiken zu einem Gesamtrisiko durch Bildung eines VaR (Value at Risk) aus den Einzel-Risikopositionen wurde in

den Abschnitten 2.7 und 2.8.1 behandelt, wobei auf die meist ungenügende Datenlage der grossen Informations-Risiken für statistische Aggregationsverfahren hingewiesen wurde. Selbst wenn die Aggregation mittels Monte-Carlo-Methode stochastisch simuliert wird, muss mit grossen Abweichungen der quantitativen Ergebnisse von der Wirklichkeit gerechnet werden. Zur Entscheidungsfindung über die Risikolage können die Risiken aber auch mit geeigneten Kennzahlen und „semiquantitativen Scores“ berichtet werden (s. Abschnitt 2.8.2).

Ordnen der Risiken

Für eine Gesamt-RM-Betrachtung ist es oft auch sinnvoll, die Risiken nach ihrer Höhe unter Angabe ihrer Abhängigkeiten lediglich zu ordnen (s. Abschnitt 2.7). Bei der Ordnung der Risiken für eine Gesamt-RM-Betrachtung spielt die Aktualität der Erhebung eine wichtige Rolle. Abbildung 12.2 zeigt die Parameter, die an den Schnittstellen der Risikomanagement-Prozesse kompatibel sein müssen.

Kompatible Parameter

- ☐ Häufigkeits-Metrik (z.B. „selten“ = 1 mal in 10 Jahren, s. Abbildung 2.4)
- ☐ Schadens-Metrik (d.h. Zuordnung von kardinal oder ordinal eingestuftem Schweregraden zu bestimmten Schadenskategorien, s. Abbildung 2.5)
- ☐ Risiko-Metrik (s. Abbildung 2.4)
- ☐ Massnahmenkosten-Metrik
- ☐ Zeitperiode und Konfidenzintervall bei quantitativer Aggregation mit VAR

Abbildung 12.2 Kompatible Parameter für verschiedene Risikomanagement-Prozesse

12.1.2

Subsidiäre RM-Prozesse

Risiken behandeln, wo sie entstehen oder Schaden anrichten

Ein wesentlicher Grund für die Einrichtung eines Risikomanagements, insbesondere eines Informations-Risikomanagements, ist die Behandlung und Bewältigung der Risiken mit entsprechenden Massnahmen. Werden die Massnahmen bereits mit den subsidiären Risikomanagement-Prozessen durch die dafür verantwortlichen Organisationseinheiten ergriffen und umgesetzt, dann verbleiben für den Gesamt-RM-Prozess lediglich die „Restrisiken“ zu konsolidieren und mit entsprechenden Strategien und Massnahmen zu steuern. Ganz allgemein gilt, dass Risiken dort behandelt werden müssen, wo sie entstehen oder wo sie primär

ren Schaden anrichten können. Dabei orientieren sich die Risiken wie auch die Massnahmen an den Zielvorgaben des Unternehmens. Für das Zusammenspiel der Sub-Prozesse mit dem Gesamt-RM-Prozess müssen die Sub-Prozesse über kompatible Schnittstellen den Gesamt-RM-Prozess mit den notwendigen Risikomanagementinformationen alimentieren. Nur so kann die Unternehmensführung und Unternehmensaufsicht Einblick in die Restrisiken sowie die getroffenen und zu treffenden Massnahmen erhalten und ihrer Verantwortlichkeit bezüglich des Risikomanagements nachkommen. Auch ist es nur so möglich, die Risikokosten (z.B. in der Form von Eigenkapital) und die Massnahmenkosten in ausgewogener Weise den Risikobereichen (z.B. den einzelnen Geschäftsfeldern) zuzuordnen. Hier rufen wir die „Balanced Scorecard“ in Erinnerung, welche die Ausgewogenheit der strategischen Zielsetzungen unter den vier Unternehmensperspektiven „Lernen und Entwickeln“, „Interne Geschäftsprozesse“, „Kunden“ und „Finanzen“ anstrebt und alle Aktivitäten im Unternehmen auf die Strategie fokussiert.

Bottom-up-Vorgehen

Im Abschnitt 3.7 haben wir das Top-Down-Vorgehen für das RM im Unternehmen diskutiert. Zu einem wirksamen Risikomanagement und einer optimalen Gesamtsicht über die Risiken gehört aber auch das Bottom-up-Vorgehen. In den einzelnen Geschäftseinheiten, Organisationseinheiten und Prozessen werden beispielsweise projektspezifische, systemspezifische und prozess-spezifische Risiko-Analysen durchgeführt. So dient die im Abschnitt 10.1 gezeigte Erstellung von Sicherheitskonzepten, in der Struktur eines Risikomanagement-Prozesses, einem solchen Bottom-up Vorgehen. Dabei gehen lediglich die nach der Umsetzung der Sicherheitskonzepte verbleibenden **grossen** Restrisiken in den übergeordneten Risikomanagement-Prozess ein.

Grosse Restrisiken in übergeordneten Risiko-Arten

Im übergeordneten Risikomanagement-Prozess werden diese Risiken allenfalls noch in übergeordnete Risiko-Arten zusammenfasst und konsolidiert.

Verschiedene System-Ausfall-Risiken innerhalb eines wichtigen Geschäftsprozesses werden beispielsweise auf der übergeordneten Ebene zu einem einzigen Ausfall-Risiko des gesamten Geschäftsprozesses aggregiert und konsolidiert. In der Terminologie der operationellen Risiken sind dies dann nicht die „erwarteten“ kleinen Verluste, sondern die „unerwarteten“ und „katastrophalen“ grossen Verluste (s. Abschnitt 2.8.1, Abbildung 2.10).

Prinzip der Wesentlichkeit

Allgemein müssen im Unternehmen die Kommunikation und die Behandlung der Risiken dem „Prinzip der Wesentlichkeit“ gehorchen und stufengerecht erfolgen. So sollte die oberste Führungsstufe nur die grössten Risiken behandeln (Erfahrungswert: Twenty is plenty). Die kleineren Risiken werden lokal behandelt und an das zuständige Management respektive den Risiko-Owner des Bereichs berichtet. Auch dort gilt, dass im Bereich einer Linienverantwortung sinnvollerweise nicht mehr als 20 hauptsächliche Risiken bearbeitet werden sollten (vgl. [Brüh03], S. 110 ff).

12.1.3**Informations-RM und Rollenkonzepte im Gesamt-RM**

Die Unterstützung fast aller Geschäftsprozesse durch die IT führt dazu, dass die Informations-Risiken fast in allen Bereichen anfallen. Im vorigen Abschnitt haben wir die lokale Behandlung der Risiken als notwendig hervorgehoben.

Risiko-Ownership

Bei der Frage, wie Risiko-Ownership den Informations-Risiken zugeordnet werden könnte, bietet sich beispielsweise die IT-System-Ownership an. Bei der IT-System-Ownership werden aus der Geschäftsperspektive die verschiedenen IT-Verantwortlichkeiten rund um ein IT-System aufgeteilt.

Im Falle eines kleinen Unternehmens wird für alle Risiko-Aspekte eines IT-System (komplette Anwendung mit Server-Plattform und zugehöriger Clients) ein sogenannter „Owner“ bestimmt. Sind es mehrere IT-Systeme, dann kann deren „Ownership“ verschiedenen Personen, aber auch einer einzigen Person zugeteilt werden.

Einem solchen Owner obliegen die Aufgaben, Verantwortlichkeiten und Kompetenzen zum Management der Risiken im Zusammenhang mit den durch „seine“ IT-Systeme zu bearbeitenden Informationen und Prozesse. Diese Person sollte insbesondere in der Lage sein, die Risiken in seinem Verantwortungsbereich zu erkennen und einzustufen.

Risk Owner

Als „Risk Owner“ wird diese Person die Informations-Risiken an den Gesamt-RM-Prozess berichten. Hinsichtlich der Sicherheits-Verantwortung kann diese Person auch für die Anfertigung eines IT-Sicherheitskonzeptes verpflichtet werden. Natürlich kann die Ownership-Verantwortung dieser Person auch auf weitere Risiko-Arten als die Informations-Risiken ausgedehnt sein.

Im Zusammenhang mit den IT-Risiken fallen bei entsprechenden Ereignissen für die Owner auch dringlich zu bewältigende Aktivi-

	täten an, weshalb zu den Ownern auch deren „Owner-Stellvertreter“ nominiert werden.
<i>Unterschiedliche Verantwortlichkeiten</i>	In grossen Unternehmen mit vielen und umfangreichen Geschäfts-Anwendungen und Server-Plattformen können einem Geschäftsprozess und seinen IT-Unterstützungsprozessen auch entsprechend spezifische „Owner-Funktionen“ zugeordnet werden. Z.B. Geschäfts-Owner verantwortlich für den Geschäftsprozess (oder die Anwendung), Betriebs-Owner verantwortlich für den Betrieb der Applikation und Plattform-Owner für die Client und Server-Plattformen und die Hardware.
<i>Geschäfts-Owner</i>	Der Geschäfts-Owner wird die SLAs bestimmen und für die Erstellung eines IT-Sicherheitskonzepts basierend auf einem Risiko-Assessment sorgen. Die anderen am Geschäftsprozess beteiligten Owner werden im Rahmen der SLAs und der unternehmensweiten Sicherheitsweisungen ihren Beitrag zu einem gemeinsamen Sicherheitskonzept für den Geschäftsprozess beisteuern (s. Abschnitt 10.1). Darüber hinaus obliegt es dem Geschäfts-Owner, im Jahres-Rhythmus die Aktualität der in seinem Verantwortungsbereich liegenden Sicherheitskonzepte zu überprüfen und die aktuelle Risikosituation verbindlich an den Gesamt-RM-Prozess zu berichten.
<i>Berichterstattung</i>	Die zu berichtende „aktuelle Risikosituation“ beinhaltet, unter Bezugnahme auf die Geschäftsanforderungen und die strategischen Ziele, die grossen Restrisiken und die wichtigen Massnahmen (Ist- und Soll-Massnahmen).
<i>Koordination und Schulung</i>	In einem grossen Unternehmen mit vielen IT-Ownern (resp. Risk-Ownern) bedarf die ständige Aufrechterhaltung einer solchen Organisation eines gewissen Koordinations-Aufwandes. Ebenso bedürfen die lokalen Risikomanagement-Prozesse eines gewissen Masses an Schulung.
<i>Chief Information Security Officer</i>	Die Koordinations- und Schulungsaufgaben für das subsidiäre Management der Informations-Risiken gehören sicherlich in das Pflichtenheft eines „Chief Information Security Officer“.

*Chief Risk Officer
oder
Risk Manager*

Die Koordinations- und Coaching-Aufgaben für die adäquate Lieferung der Risiko-Informationen an den Gesamt-RM-Prozess fallen hingegen in die Verantwortung eines „Chief Risk Officer“ oder eines „Risk Manager“.

Es empfiehlt sich, die Rechte und Pflichten der in ein solches Rollenkonzept eingebundenen Funktionsträger mit entsprechenden Weisungen zu regeln.

Praxistipp:

Für ein funktionierendes Unternehmens-Risikomanagement sind die subsidiären Aufgaben und Verantwortlichkeiten von entscheidender Bedeutung. Es empfiehlt sich deshalb, den Funktionsträgern ihre Rollen und Verantwortlichkeiten hinsichtlich Risikomanagements in klarer und schriftlicher Form (z.B. mittels Weisungen und Funktionsbeschreibungen) aufzuerlegen.

12.2

*Gesamtprozess
und kompatible
Sub-Prozesse*

Risikomanagement im Strategie-Prozess

Bei der Verankerung des RM-Prozesses im Strategieprozess stellen wir fest, dass es, analog zu einer Gesamtstrategie und danach ausgerichteten Unterstrategien, auch ein Gesamt-RM-Prozess und danach ausgerichtete kompatible Sub-RM-Prozesse geben muss (Abbildung 12.3).

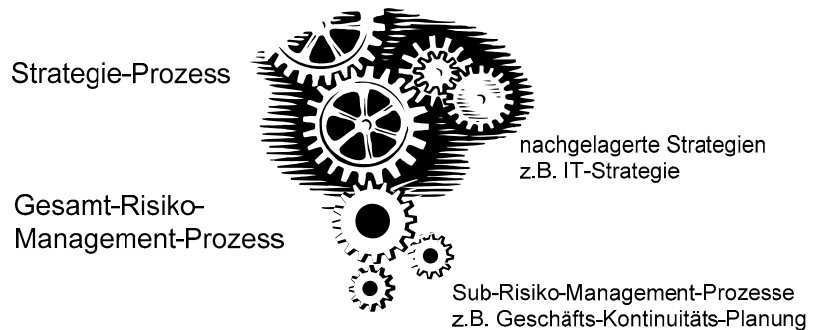


Abbildung 12.3 Risikomanagement-Prozess im Strategie-Prozess

*Makro-
Betrachtung*

Damit erhalten wir eine „Makro-Betrachtung“ auf der Ebene des Gesamt-RM-Prozesses. Hingegen finden in den einzelnen Teilbereichen (z.B. Geschäftsbereiche, Organisationseinheiten, Informatik mit ihren kritischen IT-Systemen) „Mikro-Betrachtungen“ über die spezifischen Risiken in diesen Bereichen statt.

*Mikro-
Betrachtung*

Verfügt das Unternehmen über einen Strategie-Prozess, dann sollte der RM-Prozess fest mit dem Strategie-Prozess gekoppelt oder noch besser in diesen integriert werden (s. Abbildung 12.3).

*Chancen / Risiken-
Abwägung*

Auf diese Weise sind die Voraussetzungen vorhanden, dass die Risiken mit den Chancen abgewogen werden können. Auch kann damit den Folgerisiken aus den Ressourcen-Strategien (z.B. IT-Strategie) für die Geschäfts-Strategien Rechnung getragen werden.

12.2.1

Risikomanagement und IT-Strategie im Strategie-Prozess

*Unternehmens-
Strategie*

In diesem Abschnitt wird gezeigt, wie das Informations-Risikomanagement in einen Gesamt-RM-Prozess und in die Unternehmens-Strategie einfließt.

Praxistipp:

Die Einrichtung eines RM-Prozesses in einem Unternehmen bedarf oft tief greifender organisatorischer Veränderungen. Die Einführung sowie die regelmässige Fortführung des Prozesses müssen auf allen Ebenen des Unternehmens durch das Management getragen und in das Führungssystem integriert werden. Bei fehlenden internen Erfahrungen ist für die Einführung ein externes „Coaching“ ratsam. Wichtig ist vor allem, dass das Risikomanagement mit seinen Zielen, Aktivitäten und Ergebnissen durch die Führungspersonen und die Mitarbeitenden des Unternehmens getragen und gelebt wird.

In Abbildung 12.4 ist das Beispiel eines in die Geschäftsstrategie integrierten Gesamt-Risikomanagement-Prozesses gezeigt. Die IT-Risiken werden dabei im Rahmen der IT-Ressourcen-Strategie berücksichtigt.

Die Durchführung dieses Strategie-Prozesses mit dem integrierten Gesamt-Risikomanagement-Prozess erfolgt im Ein-Jahres-Rhythmus mit einem Betrachtungs-Horizont von 3 Jahren. Die Abbildung 12.4 wird in der darauffolgenden Legende näher erläutert.

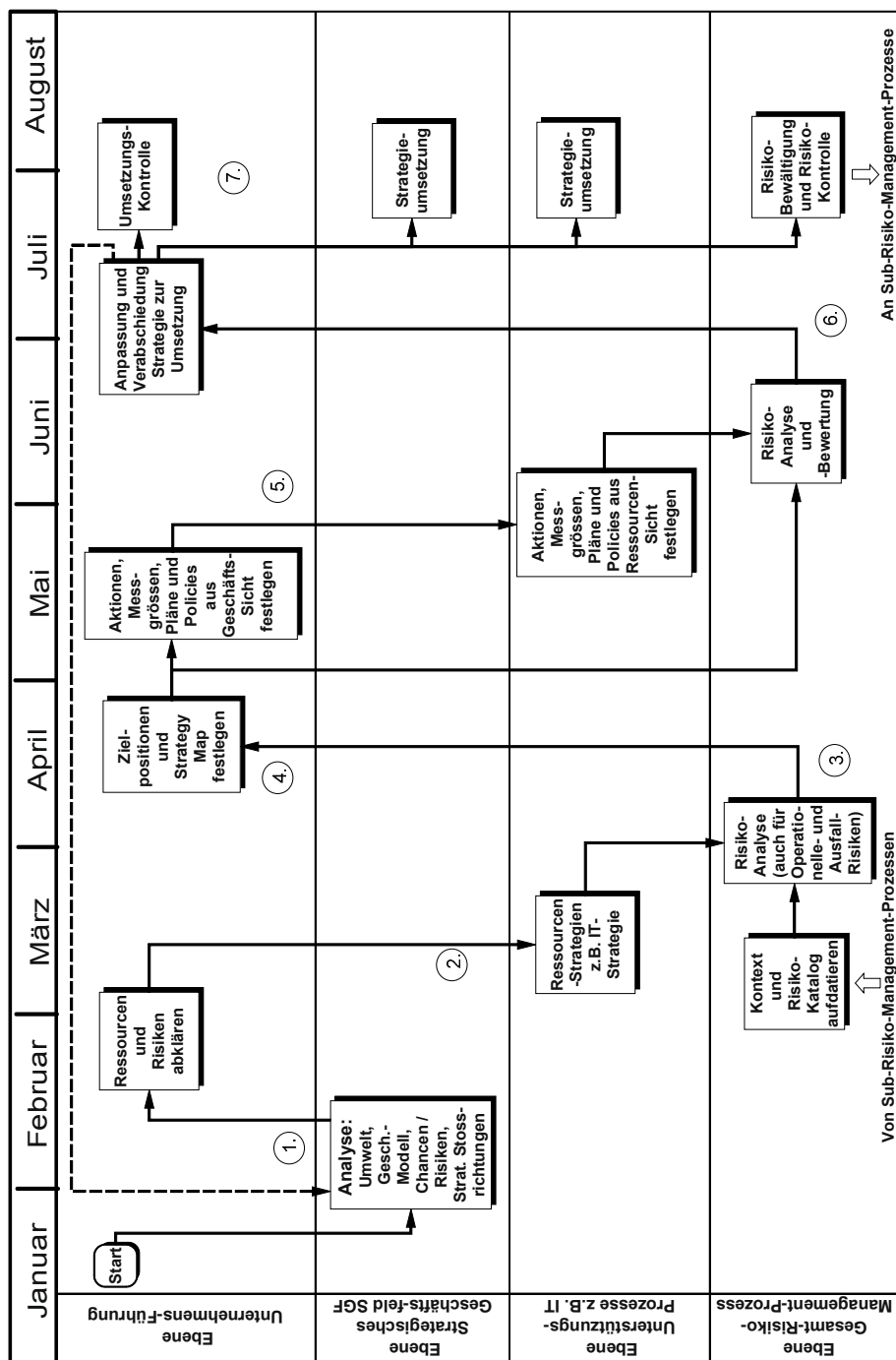


Abbildung 12.4: In Geschäftsstrategie integrierter Gesamt-Risikomanagement-Prozess

*Ablauf Strategie-
und Gesamt-RM-
Prozess*

Legende:

1. In den strategischen Geschäftsfeldern werden aufgrund einer Umwelt-Analyse für das Geschäftsfeld die Chancen und Risiken sowie die Stärken und Schwächen des Geschäftsmodells und entsprechende strategische Stossrichtungen entwickelt.
2. In weiteren Schritten werden nun die Ressourcen, u. a. die benötigten IT-Ressourcen abgeklärt.
3. Danach wird in den Gesamt-RM-Prozess verzweigt, wo die Risiken im Zusammenhang mit den strategischen Stossrichtungen untersucht werden. Der Risiko-Katalog muss dazu bereits in einer aktualisierten Version vorliegen. Im Gesamt-RM-Prozess werden die Risiken im Kontext des Gesamtunternehmens analysiert und zusätzliche Angaben bezüglich Stärken und Schwächen des Unternehmens für die zu betrachtenden strategischen Stossrichtungen gemacht.

Beispiel:

Bedarf die strategische Stossrichtung einer hohen IT-Verfügbarkeit über die Kommunikationsschiene „Internet“, dann sind an dieser Stelle die Bedrohungen und Risiken aus Unternehmenssicht (z.B. Denial of Service-Attacken) aufzuzeigen.

4. Zur Festlegung der konkreten strategischen Ziele und deren Wirkungszusammenhänge in der „Strategy-Map“ liegen nun eine komplette und bereinigte SWOT-Analyse* sowie weitere Informationen über die mit strategischen Stossrichtungen zusammenhängenden Risiken vor.
5. Zur Umsetzung der strategischen Ziele werden die Messgrößen, strategischen Aktionen, Pläne und Policies auf der Ebene der Unternehmensführung und anschliessend auf der Ebene der Ressourcen (Unterstützungsprozesse) definiert.
6. Die gewählten strategischen Aktionen einschliesslich der Messgrößen und Pläne, etc. werden noch einer Risiko-Betrachtung aus Gesamtsicht des Unternehmens (einschl. der Unterstützungsprozesse) unterzogen bevor sie im nächsten Schritt verabschiedet werden.
7. Die Umsetzung der Strategie wird vor allem im Rahmen des regulären Risiko-Reportings überwacht.

* (S=Strengths, Weaknesses, O=Opportunities, T=Threats)

12.2.2**Periodisches Risiko-Reporting**

*Regelmässiges
Reporting an
Geschäftsleitung*

*Risiko-Katalog
mit wichtigsten
Positionen*

Das Risiko-Reporting erfolgt im Rahmen der normalen Berichtssysteme und -Prozesse. So werden der Geschäftsleitung, ähnlich dem Budget-Reporting, regelmässig die Risiko-Positionen unterbreitet. Zum Reporting eignet sich beispielsweise ein monatlich aktualisierter Risiko-Katalog. Dieser sollte sowohl in seiner detaillierten Form als auch für einen möglichst raschen Überblick auf die wichtigsten Positionen zusammengefasst werden. Ebenfalls im Risiko-Katalog enthalten sollten die Massnahmen-Entscheide sowie der Stand und die Wirksamkeit der Massnahmen veranschaulicht sein.

12.3**Zusammenfassung**

In einem integrierten Risikomanagement müssen die verschiedenen Risikomanagement-Prozesse mit dem Gesamt-Risikomanagement-Prozess und dem Strategie-Prozess „verzahnt“ werden. Für einen sinnvollen Gesamt-Risikomanagement-Prozess müssen die übergeordneten, untergeordneten und nebengeordneten Risikomanagement-Prozesse zueinander kompatibel sein.

Eine quantitative Aggregation von Einzelrisiken zu einem Gesamtrisiko kann oft aufgrund der ungenügenden Datenlage der grossen Informations-Risiken und der grossen Abweichungen der Zahlenwerte von der Wirklichkeit nicht sinnvoll durchgeführt werden.

Für eine Gesamt-RM-Betrachtung ist es in solchen Fällen sinnvoll, die Risiken nach ihrer Höhe unter Angabe ihrer Abhängigkeiten zu ordnen. Die Risikolage kann auch mit geeigneten Kennzahlen und semi-quantitativen Scores zur Entscheidungsfindung berichtet werden.

Die Risiken müssen dort behandelt werden, wo sie entstehen und/oder primären Schaden anrichten können. Die in einzelnen IT-Sicherheitskonzepten verbleibenden grossen Restrisiken sind Risiken, die in den übergeordneten RM-Prozess einfliessen sollten.

Im übergeordneten RM-Prozess können auch Risiken zusammengefasst werden, so werden verschiedene Ausfallrisiken auf der Ebene eines Prozesses zu einem einzigen Ausfall-Risiko des gesamten Geschäftsprozesses aggregiert. Dem Prinzip der „Wesentlichkeit“ gehorchend, sollte die oberste Führungsstufe eines Unternehmens höchstens die zwanzig grössten Risiken behan-

deln. Die kleineren Risiken werden lokal behandelt und dem zuständigen Management oder Risiko-Owner berichtet.

Ein „Owner“ über ein bestimmtes IT-System kann gleichzeitig auch Risiko-Owner sein. In grossen Unternehmen mit vielen Geschäfts-Anwendungen und Server-Plattformen können einem System verschiedene Owner mit unterschiedlichen Verantwortlichkeiten zugeordnet werden. Z.B.

- Geschäfts-Owner verantwortlich für den Geschäftsprozess (oder die Anwendung),
- Betriebs-Owner verantwortlich für den Betrieb der Applikation und
- Plattform-Owner für die Client und Server-Plattformen und die Hardware.

Neben dem Risikomanagement mittels zwangsläufig zu erstellen- den Sicherheitskonzepten wird es notwendig sein, im Jahres-Rhythmus die wichtigsten Geschäftsprozesse und Supportprozesse eines Unternehmens auf Informationssicherheits- und IT-Risiken hin zu untersuchen.

Die daraus resultierenden Berichterstattungen an den Gesamt-RM-Prozess müssen entsprechend den regulativen Erfordernissen für die Geschäfts-Berichterstattung sowie zum Startzeitpunkt des jährlichen Strategieprozesses jeweils verfügbar sein.

Der Risikomanagement-Prozess sollte in den Strategie-Prozess integriert oder fest an ihn gekoppelt werden. Auf diese Weise werden auf der Geschäftsleitungs-Ebene die Voraussetzungen geschaffen, dass die Risiken und Chancen gegeneinander abgewogen werden können. Auch der Entstehung von Folgerisiken in den Support-Prozessen (z.B. IT-Strategie) aufgrund der Geschäfts-Strategien kann damit Rechnung getragen werden. Für das Risiko-Reporting werden, ähnlich dem Budget-Reporting, der Geschäftsleitung die wichtigsten Risiko-Positionen unterbreitet. Zum Reporting eignet sich ein monatlich aufdatierter Risiko-Katalog.

12.4

Kontrollfragen und Aufgaben

1. Welche Parameter müssen an den Schnittstellen der RM-Prozesse kompatibel sein?
2. Welchen Vorteil bringt die Integration des RM-Prozesses in den Strategie-Prozess eines Unternehmens?
3. Wie kann die Umsetzung der Strategie überwacht werden?

4. Bei der Zuordnung untenstehender Verantwortlichkeiten für eine IT-Anwendung wird welcher Owner die SLAs für den Betrieb einer Applikation bestimmen?
 - o Owner für den Geschäftsprozess (oder Anwendung),
 - o Owner für den Betrieb der Applikation oder
 - o Owner für die Server-Plattform und Hardware.
5. In einem Unternehmen mit einem fortgeschrittenen Strategie-Prozess und einem vorhandenen Risikomanagement werden Sie welche Variante eines Risikomanagements antreffen?
 - a) Explizites einfaches Risikomanagement, das wenigen Mitarbeitenden und Führungspersonen bekannt ist.
 - b) Explizites, in das Führungssystem und den Strategieprozess des Unternehmens integriertes Risikomanagement, das unternehmensweit kommuniziert ist.
6. Kann die Unternehmens-Strategie verabschiedet werden, ohne die Vorlage der strategischen Aktionen der Ressourcen-Strategien (z.B. IT-Strategie) und ohne ein entsprechendes Risiko-Assessment?

Begründen Sie.

Bedeutung Geschäftskonti- nuität

Aus der ganzheitlichen Sicht der Unternehmens-Risiken, aus der dieses Buch geschrieben ist, kommt der Geschäftskontinuität (Business Continuity) eine hohe Bedeutung zu. In vielen Unternehmen ist die Geschäftskontinuität in einem solchen Mass von den IT-Systemen und den Informations-Ressourcen abhängig, dass bei Ausfällen der IT auch die gesamten Geschäftsprozesse zum Erliegen kommen.

Geschäfts- kontinuität gehört zur Corporate Governance

Bevor wir zur Behandlung der IT-Kontinuität im Einzelnen gelangen, gehen wir auf das übergeordnete Management der Geschäftskontinuität und deren notwendigen Planungsaspekte ein. Das Management der Geschäftskontinuität ist eine „Schlüsselaufgabe“ der Unternehmensführung und gehört zu einer guten Corporate Governance.

Unter dem englischen Begriff des „Business Continuity Management“ (BCM) wird heute ein Management-System verstanden, das ähnlich dem Qualitäts-Management-System oder dem Informationssicherheits-Management-System die Geschäftskontinuität in einem „PDCA-Zyklus“ effektiv und nachhaltig steuert.

BS25999-1 und BS25999-2

Die englische Standardisierungsorganisation „British Standards Institution“ hat deshalb einen Standard mit dem Titel „Business continuity management“ herausgegeben, der sich in zwei Teilen präsentiert: Der erste Teil (BS25999-1:2006 [Buco06]) enthält einen „Code of practice“ und der zweite Teil (BS25999-2:2007 [Busp07]) die „Specification“ auf der Basis eines „PDCA-Zyklus“ (Plan-Do-Check-Act). Inzwischen sind diese Standardisierungswerke ohne bedeutsame inhaltliche Veränderungen durch den internationalen Standard ISO 22301:2012 ersetzt worden. Mit dem PDCA-Zyklus wird insbesondere der Aktualität und der Nachhaltigkeit bei der Geschäftskontinuitäts-Vorsorge Rechnung getragen, da in geplanten Zeitintervallen die Vorkehrungen überprüft, geübt und den aktuellen Umständen angepasst werden müssen.

Planungsgebiete

Wenngleich der Geschäftskontinuitäts-Prozess als ein Management-Prozess verstanden wird, der weit über das alleinige Festlegen von Plänen hinausreicht, unterteilen wir das Geschäftskonti-

nuitäts-Management zunächst in einzelne Planungsgebiete, aus denen entsprechende Pläne resultieren [Nisc02].

Einzelpläne

Einzelne Pläne sind es vor allem deshalb, weil deren Erstellung, Unterhalt sowie deren Einsatz im Notfall unterschiedliche Expertisen und Fertigkeiten bedürfen (z.B. Geschäftskompetenzen, organisatorische und bauliche Expertisen sowie Kenntnisse und Fertigkeiten der IT). Diese Pläne werden meist in der Form von „Handbüchern“ und „Richtlinien-Dokumenten“ für den eventuellen Notfall-Einsatz, aber auch für die periodischen Übungs- und Testaktivitäten vorbereitet.

Koordinierung und Abstimmung der Pläne

Für ein möglichst wirksames Geschäftskontinuitäts-Management müssen die einzelnen Pläne koordiniert und aufeinander abgestimmt sein. Dabei ist nicht nur die Integration der einzelnen Kontinuitäts-Pläne untereinander, sondern auch die Integration mit anderen Managementsystemen (z.B. dem Informationssicherheits-Managementsystem oder des Servicemanagements) als vorteilhaft anzusehen.

13.1

Einzelpläne zur Unterstützung der Geschäftskontinuität

Die Aufteilung in einzelne Planungsgebiete ist weitgehend durch die Art des Unternehmens geprägt. Demzufolge ist die nachfolgend in den Abschnitten 13.1.1 bis 13.1.6 vorgestellte Aufteilung in Einzelpläne beispielhaft zu verstehen [Nisc02]. In den Abschnitten 13.2 und 13.3 werden sodann die zur Geschäftskontinuität gehörenden Prozesse mit Schwergewicht auf die IT-Aktivitäten und -Funktionen näher behandelt.

Präventive Handlungen

Bemerkenswert ist, dass in einem integrierten „Business Continuity Management“ einige Pläne (z.B. Vulnerability- und Incident*-Management) bereits bei Ereignissen ohne Schadensfolgen (z.B. bekanntgewordene Vulnerability) entsprechend eingeübte präventive Handlungen erfordern. Ein effektives Business Continuity Management muss deshalb auch der Prävention genügend Beachtung und Ressourcen einräumen.

* Der englische Business Continuity Standard BS 25999-2:2007 [Busp07] definiert ein „incident“ als eine „situation that might be, or could lead to, a business disruption, loss, emergency or crisis.“

Als Reaktionen auf ein real eingetretenes Schadensereignis sind die Aktionen,

- Notfall-Reaktion,
- Kontinuitätssicherung und
- Wiederherstellung Normalbetrieb

zu unterscheiden (s. Abbildung 13.1).

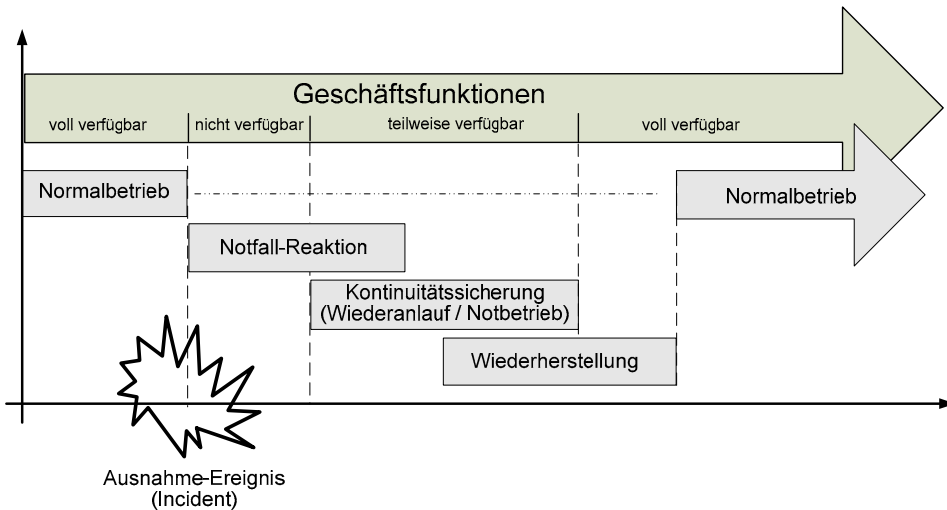


Abbildung 13.1: Ablauf der Aktionen im Ereignisfall.

13.1.1

Geschäftskontinuitäts-Plan (Business Continuity Plan)

*Aufrechterhaltung
der Geschäfts-
funktionen*

Dieser Plan ist auf eine nachhaltige Aufrechterhaltung der Geschäftsfunktionen eines Unternehmens fokussiert. Darin enthalten sind auch Massnahmen zur Aufrechterhaltung kritischer Geschäfts-Prozesse während einer Katastrophe, eines Notfalls oder einer Ausfallsituation. Für einzelne Geschäftsfunktionen können separate Geschäftskontinuitäts-Pläne aufgesetzt werden oder es kann für alle wichtigen Geschäftsprozesse (Key Business Processes) auch ein einziger gemeinsamer Geschäftskontinuitäts-Plan erstellt werden. Dies hängt von der Art des Unternehmens und seinen Geschäftsprozessen ab.

*Geschäftswieder-
erlangungs-Plan*

Für den Fall, dass infolge einer Katastrophe das Geschäft an einem anderen Ort mit einer anderen Infrastruktur und anderen Ressourcen weitergeführt werden soll, wird manchmal neben

dem Geschäftskontinuitäts-Plan ein separater sogenannter Geschäftswiedererlangungs-Plan (Business Recovery Plan) erstellt und unterhalten.

Der Plan zur Sicherstellung der IT-Kontinuität wird dort mit dem Geschäftskontinuitäts-Plan verknüpft, wo die IT die Geschäftsfunktionen unterstützen muss.

Verknüpfung untergeordneter Pläne

Mit dem übergeordneten Plan für die Geschäftskontinuität werden weitere untergeordnete Pläne verknüpft, die im Folgenden kurz erläutert werden. Bei der Ausarbeitung und Überarbeitung eines Geschäftskontinuitäts-Plans müssen die Anforderungen und Ergebnisse der untergeordneten Pläne berücksichtigt werden.

Für den zielgerichteten Einsatz der einzelnen Pläne wird eine für das Unternehmen charakteristische Einstufung der Schadensszenarien vorgenommen. Die Tabelle 13.1 zeigt beispielhaft eine solche Einstufung.

Tabelle 13.1: Beispiel einer Szenarieneinstufung

Stufe	Beispielszenario	Eskalation	Stressbedingung
7	Gebiet/Region grossflächig ausgefallen	Katastrophe	Katastrophaler Verlust (Linderung durch Kontinuitätsmanagement)
6	Betriebswichtiges Gebäude samt Personen ausgefallen		
5	Schlüsselpersonen oder grössere Personengruppen ausgefallen	Krise	Unerwarteter Verlust (Berücksichtigung im Rahmen der Risikovorsorge und des Kontinuitätsmanagements)
4	Betriebswichtiges Gebäude ausgefallen		
3	Einzelpersonen ausgefallen	Notfall	Erwarteter Verlust (Im Normalbetrieb und unter laufenden Kosten zu berücksichtigen)
2	Einzelsysteme ausgefallen		
1	Incident mit lediglich Schadenspotential oder geringer Schadensfolge	Kritischer Zustand	

13.1.2

Betriebskontinuitäts-Plan (Continuity of Operations Plan)

*Andere Standorte/
Personen*

Der Betriebskontinuitäts-Plan (COOP) beinhaltet die Vorkehrungen für die Wiedererlangung der wichtigsten Betriebsfunktionen* für eine begrenzte Zeit an einem anderen Standort (z.B. bei einer Partnerfirma) bis zum Normalbetrieb zurückgekehrt werden kann. Darin enthalten sind organisatorische Regelungen, wie Verantwortlichkeitszuweisungen und Nachfolgeregelungen sowie die Vorkehrungen für die Auslagerung lebenswichtiger Informationen. Nicht notwendigerweise darin enthalten sind die IT-Prozesse, die in einem eigenen IT-Notfall-Plan (s. Abschnitt 13.1.4) behandelt werden.

13.1.3

Ausweichplan (Disaster Recovery Plan)

*Kein Betrieb in
"normaler" Um-
gebung möglich*

Dieser Plan kommt dann zur Ausführung, wenn durch ein katastrophales Ereignis, wie Brand im Hauptgebäude, die Geschäftsprozesse mit ihren Support- und Infrastruktureinrichtungen (z.B. IT-Systeme, Rechenzentrumsgebäude) über eine längere Zeitdauer ganz ausgefallen sind und/oder nicht in ihrer normalen Funktion betrieben werden können. Der Plan beschreibt beispielsweise, wie der Betrieb auf eine Ausweichs-Infrastruktur ausgelagert und von dort betrieben werden kann.

Ungleich dem Geschäftskontinuitäts-Plan enthält dieser Plan keine Massnahmen für die (allenfalls minimale) Aufrechterhaltung von kritischen Geschäftsprozessen während der Katastrophensituation. Deshalb sollte er in geeigneter Weise mit dem Geschäftskontinuitätsplan, der diesem Umstand Rechnung trägt, verknüpft sein. Der Ausweichplan ist oft auf katastrophale Ausfälle der IT-Systeme und -Prozesse fokussiert, kann aber auch die Betriebswiedererlangungs-Prozeduren für andere wichtige Produktionseinrichtungen (z.B. Notbetrieb für Produktionsmaschinen) beinhalten. Nicht enthalten im Ausweichplan sind kleinere Ausfälle oder präventive Aktionen, wie sie im IT-Notfall-Plan (s. Abschnitt 13.1.4) vorgesehen sind.

* Im Unterschied zum zuvor erwähnten Plan für die Geschäftskontinuität werden mit diesem Plan lediglich die wichtigsten Betriebsfunktionen eines Unternehmens (z.B. eines Hauptsitzes) sichergestellt. Gemäss dem „Federal Preparedness Circular, FPC 65“ muss jede Regierungsstelle in den USA einen solchen Plan eingerichtet haben.

13.1.4 IT-Notfall-Plan (IT Contingency Plan*)

*Wiederherstellung
und Aufrecht-
erhaltung der IT-
Prozesse*

Der IT-Notfall-Plan adressiert in erster Linie Störungen und Ausfälle von solchen IT-Systemen, die sowohl der direkten als auch der indirekten Unterstützung der Geschäftsprozesse dienen.[†] Die verschiedenen Supportprozesse und IT-Systeme sind entsprechend ihrem Einfluss auf die kritischen Geschäftsprozesse und deren Priorisierung in den IT-Notfall-Plan einzubeziehen. Der IT-Notfall-Plan ist deshalb stark mit dem Geschäftskontinuitäts-Plan verknüpft. Er enthält neben den Massnahmen zur Wiederherstellung der IT-Funktionen auch die allenfalls notwendigen IT-Support-Massnahmen zur Aufrechterhaltung der Geschäftsprozesse während einer Störung oder einem Ausfall. Im Gegensatz zu dem zuvor behandelten Ausweichplan werden im IT-Notfall-Plan auch die für die Geschäftskontinuität ohne Schadensfolge verlaufenden Problemsituationen sowie die Ereignisse mit (noch) geringen Schadensauswirkungen behandelt. Für „unerwartete“ oder „katastrophale“ Ausfallereignisse wird der IT-Notfall-Plan mit dem Ausweichplan verknüpft.

13.1.5 Vulnerability- und Incident Response-Plan

Neben den unbeabsichtigten Fehlfunktionen der IT-Prozesse sind vermehrt bösartige Angriffe (gezielt oder ungezielt) auf Software (z.B. Windows) zu grossen operationellen Risiken der Unternehmen geworden. Die Angreifer benutzen meist Internet-Applikationen (z.B. Web oder Mail), um auf die zu schädigenden Systeme und deren Informationen zu gelangen. „Als Einschleusungs-Kanäle“ von „bösartigem Code“ dienen aber nicht nur

* Ausführliche Planungshilfen können dem NIST-Dokument „Contingency Planning Guide for Federal Information Technology Systems“ entnommen werden [Nisc10].

† Die direkten Supportsysteme unterstützen in Form von Geschäftsapplikationen direkt einen Geschäftsprozess. Die indirekten Supportsysteme (z.B. Büro-Automation, Administration, Buchhaltung, Dokumentenarchivierung) unterstützen mit entsprechenden Applikationen alle Prozesse einschliesslich der direkten Supportprozesse. Ebenfalls dient die IT-Infrastruktur (z.B. Server, Speichereinheiten, Informationennetze) sowohl den direkten als auch den indirekten Supportprozessen.

Verbindungen ins Internet, sondern auch Datenträger, wie CD's und vor allem die immer handlicher werdenden USB-Sticks.

*Fehlerfunktionen,
Attacken und
Vulnerabilities*

Der „Vulnerability- and Incident Response Plan“ schliesst sowohl die Ereignisse aufgrund von bekannt gewordenen Schwachstellen (Vulnerabilities), als auch Fehlerfunktionen und „Attacken“ (z.B. Hacking, Viren, Würmer, Trojanische Pferde, Denial of Service-Attacken) ein. Dieser Plan enthält beispielsweise Gegenmassnahmen, Eskalationskriterien, Kommunikations-, und Dokumentations-Vorgaben und operiert sowohl in der präventiven Phase, als auch in der akuten Phase eines Ausnahme-Ereignisses. Die Kombination des Vulnerability- und Incident-Managements in einem gemeinsamen Plan bietet sich aufgrund der vielfach überlappenden Fach-Expertisen in diesen Gebieten an; sie ist zudem zweckmässig, da die präventiven Massnahmen zur Behebung der Vulnerabilities (z. B. mittels Patching) meist unvorhergesehen und sofort durchgeführt werden müssen.

Die Kombination in einem Plan muss natürlich den unterschiedlichen Prozesszielen des Vulnerability-Managements und des Incident-Managements in korrekter Weise Rechnung tragen.

13.2

BCMS im Unternehmens-Risikomanagement

*Schlüssel-
Geschäftsziele*

Die Geschäftskontinuität (Business Continuity) gehört in vielen Unternehmen zu den lebenswichtigen Faktoren, da die Schlüssel-Geschäftsziele während und nach einer Betriebsstörung oder -unterbrechung weiterhin aufrecht erhalten werden müssen.

*Geschäftskonti-
nuität als Risiko-
Ziel*

Somit ist es wichtig, die Ziele der Geschäftskontinuität im Rahmen eines „Business Continuity Management Systems“ (BCMS) in die strategischen Zielsetzungen eines Unternehmens einzubinden. Solche Ziele können beispielsweise lauten:

- a) Ausfälle von Geschäftsfunktionen bei Notfall-Ereignissen (z.B. Stromausfall) dürfen nicht länger als 1 Std. andauern;
- b) Ausfälle von Geschäftsfunktionen aufgrund katastrophaler Ereignisse (z.B. Erdbeben, Brände, Überschwemmungen, IT-Ausfälle, Lieferausfälle) dürfen nicht länger als 24 h andauern bis der Geschäftsbetrieb (mit allenfalls geringerer Leistung) fortgesetzt werden kann.

Das in der Standardisierung als „BCMS = Business Continuity Management System“ ausgewiesene „Management-System“ behandeln wir in diesem Buch, analog dem St. Galler Management-

Modell (s. Abschnitt 4.1), als „Managementprozess“, der als wichtiger Subprozess des Unternehmens-Risikomanagements mittels einer eigenen „Business-Impact-Analyse“ und eines auf die Kontinuitätsrisiken zugeschnittenen Risiko-Assessments betrachtet werden kann.

Der Prozess des Geschäftskontinuitäts-Managements mit den Eigenschaften eines PDCA-Zyklus muss vor allem folgende Punkte beinhalten:

- den unternehmensspezifischen Kontext, innerhalb welchem die Geschäftskontinuität sichergestellt werden muss;
- die massgeblichen Aspekte der Führung, der Planung und der Unterstützung durch Ressourcen, Fähigkeiten, Bewusstseinsförderung und Kommunikation;
- die Untersuchung der Kontinuitäts-Risiken und die Verletzlichkeit des Unternehmens sowie die möglichen Szenarien, die zu Kontinuitäts-Risiken führen;
- die Identifikation der vorhandenen Ressourcen und Infrastruktureinrichtungen, die im Normalbetrieb notwendig sind, um die kritischen Funktionen und Prozesse zu unterstützen;
- die Identifikation der Schutzobjekte (z.B. Business-Funktionen, Prozesse, Infrastrukturen, Informationen und Personen), die für die Kontinuität der Geschäftsprozesse im Sinne einer akzeptablen Betriebs-Fortführung geschützt werden müssen;
- die Kriterien für die Auslösung von Sofortmassnahmen, Kontinuitäts- und Wiedererlangungshandlungen;
- ein geplantes Vorgehen, wie die Funktionstüchtigkeit der getroffenen Massnahmen überprüft und an den aktuellen Erfordernissen ausgerichtet werden kann;
- die Bestimmung der Kommunikations-Anforderungen, der Kommunikationsmethoden und -kanäle vor, während und nach einer Betriebsunterbrechung;
- die Mechanismen und Verfahren, um den aktuellen Veränderungen unmittelbar Rechnung zu tragen und um die allfälligen Schwächen und Lücken im Geschäftskontinuitäts-System zu erkennen und im Sinne einer ständigen Verbesserung behandeln zu können und zu korrigieren.

*Geschäftskontinuitäts-Planung
im
Unternehmens-
RM-Prozess*

Die Geschäftskontinuitäts-Planung als Sub-Prozess des integrierten Unternehmens-Risikomanagement-Prozesses (s. Abbildungen 12.3 und 13.2) ist für die Erreichung der Geschäftsziele unerlässlich und als spezieller Risikomanagement-Prozess eng auf die Anforderungen der Geschäftskontinuität bei Notfall- oder Katastrophen-Ereignissen zugeschnitten. Im Folgenden wird dieser Prozess, wie er sich grob aus dem Standard ISO 22301:2012 [Isob12] sowie in einigen Details* aus anderen Standards und den praktischen Erfahrungen des Autors im Wesentlichen ergibt, behandelt.

Die Hauptschritte des Kontinuitäts-Prozesses sind:

- 1) Planung Kontinuitäts-System
- 2) BIA[†] und Risiko-Assessment
- 3) Kontinuitäts-Strategien
- 4) Kontinuitätsverfahren und Pläne
- 5) Tests, Übungen und Wartung der Pläne
- 6) Ständige Überwachung und Überprüfung
- 7) Kontinuierliche Verbesserungen und Wiederholungen

Wie aus der Anlehnung an Standards, vor allem an den Standard ISO 22301:2012[‡] ersichtlich wird, ist für den gesamten Kontinuitäts-Prozess, die Führung, das Commitment des Managements, die sorgfältige Planung, die Verfügbarkeit der Ressourcen und das Risikobewusstsein der Mitarbeitenden und involvierten Stellen von entscheidender Bedeutung.

* Der Standard ISO 22301:2012 wird im Folgenden in wesentlichen Punkten weitgehend inhaltsgetreu wiedergegeben. Für eine Zertifizierung ist jedoch die Genauigkeit des Originalstandards massgebend. Zusätzlich zu den Erfordernissen des Standards werden nützliche anwendungsspezifische Details aus den Erfahrungen des Autors mit der Umsetzung der Standards BS 25999-x, dem Handbuch HB 221:2004 [Anhb04], sowie dem noch nicht veröffentlichten Standard „ISO 22313 Business continuity management systems - Guidance“ [Isog12] in die Ausführungen einbezogen.

[†] BIA=Business Impact Analyse

[‡] Der Standard ISO 22301:2012 ist der erste Standard, der in der ISO nach den, gemäss ISO Guide 83, für alle Managementsysteme gültigen Kapitel- und Textvorgaben abgefasst wurde.

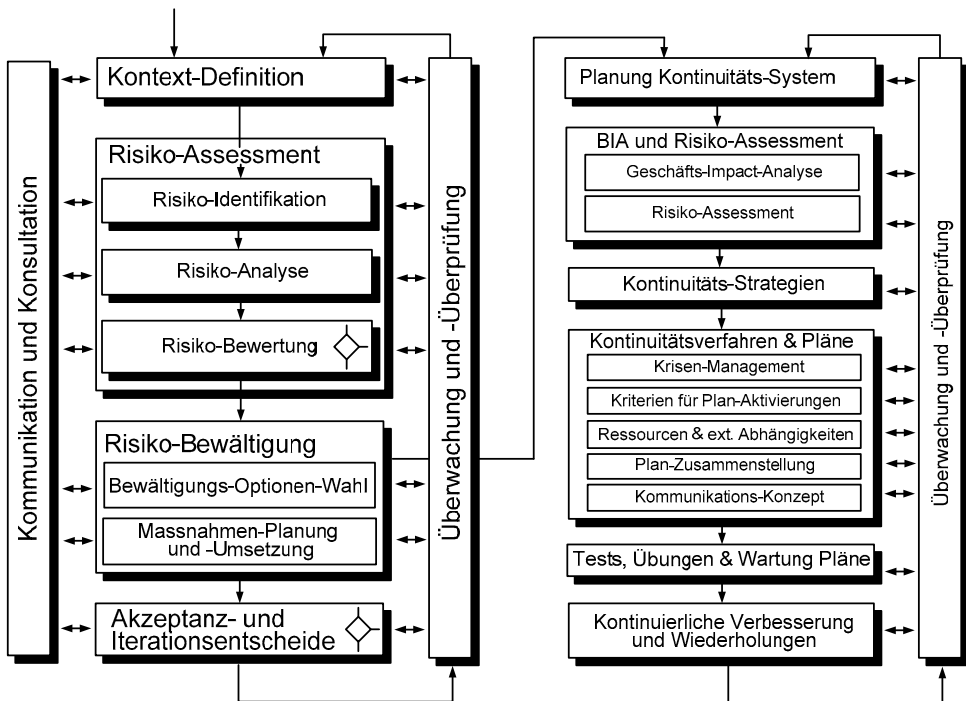


Abbildung 13.2: Geschäftskontinuitäts-Prozess als untergeordneter RM-Prozess

13.3 Planung Kontinuitäts-System

In dieser vor allem für den Aufbau eines Kontinuitäts-Managements wichtigen Prozessphase werden der Rahmen und die wichtigen generellen Aspekte und Voraussetzungen für das Kontinuitäts-Management definiert. Auch werden, wie die nachfolgenden Unterabschnitte zeigen, die Ziele und Aktivitäten für ein allenfalls zu eröffnenden Projekts abgesteckt.

13.3.1 Kontext des Unternehmens

Der zu dokumentierende Kontext ergibt sich aus internen und externen Fragestellungen, die für den Zweck des BCMS relevant sind oder die erwarteten Resultate beeinflussen können. Solche Fragestellungen sind:

- Aktivitäten, Funktionen, Produkte, Dienstleistungen Partnerschaften, Lieferketten, Zusammenhänge mit Anspruchsgruppen sowie der potentielle „Impact“ eines unterbrechenden Ereignisses;

- ☐ Angabe der Verknüpfungen mit Politiken und Zielen des Unternehmens sowie dessen Strategieprozess: z.B. Geschäftsziele, Kritische Erfolgsfaktoren, Schlüssel-Indikatoren sowie von den Geschäftszielen abgeleitete Ziele und Grundsätze für die Geschäftskontinuität;
- ☐ Definition der externen und internen Faktoren, die zu Kontinuitäts-Risiken führen können;
- ☐ Risiko-Kriterien bezogen auf den „Risiko-Appetit“ des Unternehmens;
- ☐ Zweckbestimmung des BCMS im Unternehmen;
- ☐ Aufführen der für das BCMS massgeblichen Anspruchsgruppen und deren Anforderungen;
- ☐ Bestimmung und Einsatz von Verfahren, mittels derer die für die Kontinuität des Betriebs sowie der Produkte und Dienstleistungen massgeblichen legalen, regulatorischen Anforderungen und deren Veränderungen identifiziert und den massgeblichen Stellen kommuniziert werden.
- ☐ Definition des Einsatz- und Geltungsbereichs des BCMS in angemessenen, klaren Begriffen, die den Ausprägungen des Unternehmens sowie den Abgrenzungen, Restriktionen und Ausschlüssen des BCMS Rechnung tragen (z.B. einbezogene Organisationseinheiten, Lokalitäten, Geschäftsprozesse, Produkte, Dienstleistungen, Ausschluss bestimmter geographischer Regionen).

13.3.2

Führung

Beim Management der Geschäftskontinuität geht es zum einen um die Beherrschung grosser Risiken, zum anderen müssen aber auch beträchtliche Kosten durch Aktivitäten und Vorkehrungen unter Einbezug der gesamten Belegschaft berücksichtigt werden. Der Erfolg der Umsetzung eines Prozesses mit dieser Tragweite kann aber nur gesichert werden, wenn der Prozess zum Anliegen sämtlicher Führungsebenen und -funktionen gemacht wird und sich das Top-Management proaktiv dafür einsetzt und sein „Commitment“* demonstriert.

* Commitment: Begriff der anglo-amerikanischen Managementliteratur mit der Bedeutung „Selbstverpflichtung“ oder „freiwillige Bindung“.

So sorgt das Top-Management für:

*Top-Management
Aufgaben*

- ☐ Kompatibilität mit der Unternehmensstrategie;
- ☐ Integration der BCMS-Anforderungen in die Geschäftsprozesse;
- ☐ Bereitstellung der Ressourcen für Aufbau und Unterhalt des BCMS;
- ☐ Kommunikation der Wichtigkeit und der Konformität bezüglich der Anforderungen;
- ☐ Erreichung der erwarteten Ergebnisse;
- ☐ Lenkung und Unterstützung der kontinuierlichen Verbesserung.

*Top-Management
Commitment*

Sein Commitment stellt das Top-Management unter Beweis, u.a. durch,

- ☐ die Erstellung einer Geschäftskontinuitäts-Policy (z.B. Genehmigung und Erlass durch den Verwaltungsrat),
- ☐ die Vergewisserung, dass adäquate Ziele und Pläne eingesetzt sind,
- ☐ die Schaffung von Rollen, Verantwortlichkeiten und Kompetenzen sowie durch die Nomination einer oder mehrerer Personen mit den notwendigen Kompetenzen für Leitung, Aufbau und Betriebs des BCMS.

Das Top Management gewährleistet dabei, dass die Verantwortlichkeiten und Kompetenzen für die relevanten Rollen eines BSMS zugeteilt und im Unternehmen kommuniziert sind und engagiert sich im BCM-Prozess durch,

- ☐ die Definition der Kriterien zur Akzeptanz der Risiken abhängig von ihrer Höhe,
- ☐ die aktive Teilnahme an Übungen und Tests,
- ☐ die Vergewisserung, dass interne Audits über das BCMS durchgeführt werden,
- ☐ die Vergewisserung, dass Überprüfungen durch das Management stattfinden und
- ☐ die Vergewisserung, dass „Non-Konformitäten“ und Lücken behoben und die notwendigen Anpassungen und Korrekturen im Sinne von „Kontinuierliche Verbesserungen“ gewährleistet sind.

*Geschäfts-
kontinuitäts-
Policy*

Eine „**Geschäftskontinuitäts-Policy**“, die das Top-Management erstellt, kommuniziert und dokumentiert:

- ☐ ist auf den Unternehmenszweck ausgelegt, und gibt Aufschluss über die organisatorische Einbettung (Governance);
- ☐ sie enthält die Festlegung der im Prozess wahrzunehmenden Hauptaufgaben, Verantwortlichkeiten und Kompetenzen;
- ☐ sie zeigt die einbezogenen geographische Standorte;
- ☐ sie bietet den Rahmen zur Festlegung von Geschäftskontinuitäts-Zielen;
- ☐ sie enthält ein Commitment, dass die vorliegenden Anforderungen erfüllt werden;
- ☐ sie enthält ein Commitment hinsichtlich kontinuierlicher Verbesserung des BCMS;
- ☐ sie ist zur Kommunikation an alle Personen gerichtet, die im Rahmen des definierten Einsatzbereiches für das Unternehmen arbeiten;
- ☐ sie enthält die Kriterien für die periodische sowie bei signifikanten Veränderungen notwendige Überprüfung und Überarbeitung;
- ☐ sie steht, soweit sinnvoll und durch das Management im Einzelnen bewilligt, auch interessierten Kreisen zur Verfügung.

*Organisatorische
Rollen, Verant-
wortlichkeiten
und Kompetenzen*

Das Top Management sorgt dafür,

- ☐ dass die im Rahmen des BCMS zugeteilten Rollen, Verantwortlichkeiten und Befugnisse im Unternehmen und bei den in das BCMS involvierten Anspruchsgruppen kommuniziert sind und
- ☐ dass es über die aktuelle Leistungsfähigkeit des BCMS (u.a. in den obligatorischen Berichterstattungen) auf dem Laufenden gehalten wird.

13.3.3

Planung

Die für ein Managementsystem obligatorische Planung befasst sich beim Geschäftskontinuitäts-Management vor allem mit den strategischen „Risiken und Chancen“ und den daraus abzuleitenden Zielen sowie mit den Plänen, um diese Ziele umzusetzen.

Aktionen in Bezug auf Risiken und Chancen

Aus dem Verständnis des Unternehmens und der aus seinem Kontext resultierenden Problemstellungen und Anforderungen (s. Abschnitt 13.3.1) sollen die Risiken und Chancen eines BCM aufgezeigt werden, womit erreicht werden soll, dass

- ☐ die durch das BCMS beabsichtigten Resultate erreicht werden,
- ☐ unerwünschte Effekte vermieden und
- ☐ die Chancen für Verbesserungen erkannt werden.

Aus den Risiken und Chancen müssen die Notwendigkeiten zur Planung von Aktivitäten erkannt und beurteilt werden, um in den weiteren BCMS-Prozess integriert werden zu können.

Geschäftskontinuitäts-Ziele und Pläne

Das Top-Management vergewissert sich, dass die Geschäftskontinuitäts-Ziele für die relevanten Funktionen und Ebenen im Unternehmen für alle Funktionen und auf allen Leitungsebenen eingesetzt und kommuniziert werden und gibt die erforderlichen Hinweise, wie die Ziele erreicht werden sollen.

Die Zieldefinitionen sind zu dokumentieren und sollen die folgenden Eigenschaften besitzen:

Eigenschaften von Zieldefinitionen

- ☐ Konsistenz mit der Geschäftskontinuitäts-Policy;
- ☐ Berücksichtigung des minimalen Masses, der für das Erreichen der Geschäftsziele notwendigen Produkte und Dienstleistungen;
- ☐ Messbarkeit und Überwachbarkeit hinsichtlich der gestellten Anforderungen und der Gewährleistung ihrer Aktualität.

Praxistipp:

Um die Kontinuitäts-Ziele umsetzen zu können, muss bestimmt sein: **Was** mit **welchen Ressourcen** bis **wann** getan werden muss und **wer** für die Umsetzung verantwortlich ist und **wie** die Resultate der Umsetzung beurteilt werden.

13.3.4

Unterstützung

Der BCM-Prozess bedarf der Unterstützung sämtlicher Management-Ebenen sowohl mit materiellen als auch mit strukturellen und personellen Ressourcen. Dazu gehören eine adäquate Bewusstseinsbildung (Awareness) sowie die angemessene Einrichtung von Kommunikations- und Dokumentationsverfahren.

Aus den Unterstützungsanforderungen resultieren im Einzelnen die folgenden Notwendigkeiten:

*Ressourcen
Fähigkeiten*

- ☐ Die Ressourcen für das BCMS müssen bestimmt und bereitgestellt werden.
- ☐ Die notwendigen Fähigkeiten der Personen, welche für das BSMS arbeiten, müssen bestimmt werden.
- ☐ Es muss sichergestellt sein, dass die Personen, die für das BCMS arbeiten, über eine adäquate Ausbildung, sowie über Erfahrung und angemessenes Training verfügen oder, wenn nötig, erhalten; die Nachweise über die Fähigkeiten oder die Aktionen zu deren Erwerb sind zu dokumentieren.

*Bewusstseinsbil-
dung (Awareness)*

- ☐ Die unter der Kontrolle des Unternehmens tätigen Personen müssen die Geschäftskontinuitäts-Policy, ihren Beitrag zur Wirksamkeit des BCMS, einschliesslich der Vorteile einer verbesserten BCM-Leistung sowie die Auswirkungen bei Nichteinhaltung der Anforderungen kennen; insbesondere muss diesen Personen ihre im Ereignisfall zukommende Rolle bekannt sein.

Kommunikation

- ☐ Alle interessierten Kreise (Kunden, Mitarbeiter, Aktionäre, Lieferanten, Medien), die in den BCM-Prozess involviert oder davon abhängig sind, müssen in die Kommunikation einbezogen werden.
- ☐ Die Notwendigkeiten und das Vorgehen für die interne und externe Kommunikation, sowohl im Normalbetrieb als auch im Ereignisfall, müssen in der Planung festgelegt werden.

Praxistipp:

Sowohl im Normalbetrieb als auch im Ereignisfall müssen in der Planung festgelegt sein:

- ⇒ **Was,**
- ⇒ **Wann,**
- ⇒ **durch Wen,** und
- ⇒ **an Wen**

hinsichtlich BCM kommuniziert wird.

Geplante Verfahren zur Kommunikation

Die Organisation setzt geplante Verfahren ein für:

- ☐ die interne Kommunikation mit und unter interessierten Kreisen* sowie Mitarbeitern;
- ☐ die externe Kommunikation mit externen interessierten Kreisen einschliesslich der Medien;
- ☐ den Empfang, die Beantwortung und Dokumentation der Kommunikation mit interessierten Kreisen;
- ☐ den Einbezug geeigneter nationaler oder regionaler Beratungs- und Meldedienste bei Planung und Betrieb des BCMS;
- ☐ die Gewährleistung der Verfügbarkeit von Kommunikationseinrichtungen während dem Unterbrechungsereignis;
- ☐ die strukturierte Kommunikation mit den massgeblichen Behörden und die Gewährleistung der Interoperabilität mit den vielfältigen anzusprechenden Organisationen und Personen;
- ☐ das Betreiben und Testen der für den Ereignisfall vorgesehenen Kommunikationseinrichtungen und -fähigkeiten.

Dokumentierte Informationen

Das BCMS enthält sowohl die dokumentierten Informationen, die durch diesen Standard verlangt werden als auch solche, die für die Wirksamkeit des BCM durch die Organisation festzulegen sind (z.B. für Politik, Risiko-Analysen, Übungsaufgebote, Handbücher, Konfigurationspläne, Dokumentklassifikation)

Der vorgeschriebene Prozess für die Erstellung und Aktualisierung der Dokumente beinhaltet:

- ☐ die Identifikation und Beschreibung jedes einzelnen Dokuments (z.B. Titel, Name, Datum, Autor, Nummerierung);
- ☐ die Formatfestlegungen (z.B. Sprache, Software Version) und Medium (z.B. Papier, DVD);
- ☐ den sichtbaren Nachweis der Überprüfung und Genehmigung.

* Interessierte Kreise sind die Anspruchsgruppen des Unternehmens

Sicherung / Kontrolle der dokumentierten Informationen

Die Sicherung und Kontrolle der für das BCMS **dokumentierten Informationen** erstreckt sich über:

- ☐ Verteilung;
- ☐ Zugriff;
- ☐ Speicherung und Aufbewahrung;
- ☐ Auffindbarkeit und Benützung;
- ☐ Änderungen (z.B. Versions-Kontrolle);
- ☐ Lesbarkeit;
- ☐ Vermeidung der Benutzung ungültiger Informationen;
- ☐ Aufbewahrung, Löschung und Entsorgung;

Die von externen Quellen erhaltenen Informationen für Planung und Betrieb sind entsprechend zu bezeichnen und ebenfalls zu kontrollieren.

Bei der Verwendung und Aufbewahrung, aber auch bei der Sicherung und Kontrolle, sind die Dokumente adäquat zu schützen (z.B. Schutz gegen Missbrauch oder unberechtigte Veränderungen, Löschungen).

13.4

Operation

Umsetzung der Geschäfts-kontinuität

Der Geschäftskontinuitäts-Management-Standard ISO 22301 subordiniert die für die **Umsetzung** der Geschäftskontinuität massgeblichen Prozesse und Prozessschritte (folgende Abschnitte 13.5 bis 13.8) im Kapitel „Operation“ und bringt damit die Do-Phase eines PDCA-Zyklus zum Ausdruck.

Betriebliche Planung und Kontrolle

Für eine solche Umsetzung des Management-Systems bestimmt, plant, implementiert und kontrolliert die Organisation die Prozesse, die notwendig sind, um die Risiken und Chancen hinsichtlich der Funktionstüchtigkeit und Wirksamkeit des BCMS zu erkennen und angemessen zu behandeln. Dabei sind die geplanten Veränderungen anhand definierter Kriterien zu kontrollieren und die unbeabsichtigten Veränderungen zu überprüfen, um die allenfalls negativen Auswirkungen zu reduzieren. In die Kontrollen sind die ausgelagerten Prozesse („contracted-out“- und „outsourced“-Prozesse) einzubeziehen.

Programm über Geschäfts-kontinuität

Die Funktionstüchtigkeit, Wirksamkeit und Angemessenheit der Vorkehrungen und Aktivitäten lassen sich am besten anhand eines für die Geschäftskontinuität etablierten „Programmes“ überprüfen und sicherstellen.

13.5**Geschäfts-Impact-Analyse und Risiko-Assessment**

Die Geschäfts-Impact-Analyse und das Risiko-Assessment für das Kontinuitäts-Assessments werden als formalisierte Prozesse definiert und dokumentiert; diese Prozesse beinhalten hauptsächlich:

- ☐ den Kontext mit den Kriterien zur Bewertung der unterbrechenden Incidents;
- ☐ die legalen und sonstigen internen und externen Anforderungen;
- ☐ die systematische Analyse der Kontinuitätsanforderungen und der Risiken im Hinblick auf eine priorisierte Behandlung unter Berücksichtigung der Kosten;
- ☐ einen definierten Output sowohl aus der Geschäfts-Impact-Analyse als auch dem Risiko-Assessment;
- ☐ Behandlungsvorschriften über die Informationen im Zusammenhang mit diesen Prozessen (z.B. hinsichtlich Aktualisierungen oder Vertraulichkeitswahrung).

13.5.1**Geschäfts-Impact-Analyse**

Die Business Impact Analyse (BIA) widmet sich vor allem den folgenden Aufgaben:

- ☐ Identifikation der kritischen Geschäftsfunktionen, Prozesse und Aktivitäten, welche die wichtigen Geschäftsziele (Key Goals) zur Lieferung von Produkten und/oder Dienstleistungen unterstützen. Eine „Prozesskarte“, welche die Verknüpfung der verschiedenen Prozesse (einschliesslich der Support-Prozesse) aufzeigt, ist dafür ein nützliches Hilfsmittel.
- ☐ Aufzeigen der Abhängigkeiten und unterstützenden Ressourcen für die kritischen Geschäftsfunktionen, Prozesse und Aktivitäten, z.B.:
 - Personal;
 - Informationen, Daten und IT-Infrastruktur;
 - Büro- und Spezialarbeitsgeräte;
 - Räume, Infrastruktur und Versorgungseinrichtungen;
 - Lagerbestände;
 - Interne Schnittstellen (z.B. Verbindungen zu anderen Geschäfts- oder Supporteinheiten);
 - Externe Schnittstellen zu relevanten Anspruchsgruppen (z.B. Lieferanten, Kunden, Vertragspartner, Outsourcing-Partner, Regulatoren).

- ❑ Bestimmung von Art und Höhe der Geschäfts-Impacts (finanziell, operationell und strategisch) für den Ausfall einer jeden kritischen Geschäftsfunktion für verschiedene Unterbrechungszeiten (z.B. 4h, 8h, 12h, 18h, 24h, 48h). Dazu kommen Zeitaufwand, Kosten und Ressourcen für die Aufarbeitung der aufgestauten Aktivitäten (Backlogs).
- ❑ Bestimmung der maximal akzeptierbaren Ausfalldauer (MTPD=Maximum Tolerable Period of Disruption oder auch MAO=Maximum Acceptable Outage). Die Lebensfähigkeit des Unternehmens ist unwiderruflich bedroht, wenn innerhalb dieser Zeit die Produkte- oder Dienstleistungslieferung nicht wiedererlangt werden. Die maximal akzeptierbaren Schäden (Impacts) werden oft im Verhältnis zum Betriebserfolg vor Abschreibung (EBIT-DA) eines Unternehmens angegeben.
- ❑ Ausgehend von den ermittelten MTPD-Zeiten und der analysierten Impacts werden für jede kritische Geschäftsfunktion (resp. jeden kritischen Geschäftsprozess) die **maximalen Soll-Zeiten sowie die Prioritäten** für
 - Wiederanlauf* und
 - Wiederherstellung†sowie die Zeiten der
 - minimal notwendigen Notbetriebsdauer‡ und der
 - maximal tolerierbaren Notbetriebsdauer§definiert.

* Nach dieser Zeit ist die Kontinuität in einem allfälligen Notbetrieb hergestellt. Diese Dauer muss unter der MTPD-Zeit liegen. Das Ziel wird auch als "RTO = Recovery Time Objective" bezeichnet. Diese Dauer muss unter der MTPD-Zeit liegen.

† Nach dieser Zeit wird aus dem Notbetrieb wieder in den Normalbetrieb zurückgekehrt.

‡ Die minimal notwendige Notbetriebsdauer muss so bemessen sein, dass der Wiederanlauf in der vorgesehenen Leistungsfähigkeit bis zur Wiederherstellung der Prozesse für den Normalbetrieb gewährleistet ist; (Beispiel: Kraftstoffvorrat für Notstromdiesel bis zur Wiederherstellung der normalen Stromversorgung).

§ Die maximal tolerierbare Notbetriebsdauer gibt die Zeit an, nach der spätestens in den Normalbetrieb zurückgekehrt sein muss, z.B. aufgrund von negativen Nebeneffekten des Notbetriebs.

- Ein weiteres wichtiges Ziel einer jeden kritischen Geschäftsfunktion ist der minimale „Service Level“ (MBCO=Minimum Business Continuity Objective), der erreicht werden muss. Dabei muss nicht nur die Aufrechterhaltung einer minimalen Produktivität und Verfügbarkeit, sondern auch der durch den Notbetrieb sich allenfalls ergebenden Rückstand betrachtet werden.

Wiederanlaufzeit

Die **Wiederanlaufzeit** ist von entscheidender Bedeutung für die unmittelbare Sicherung der Kontinuität, wenn auch mit allenfalls reduzierter Leistung. Die Zeiten und Prioritäten des Wiederanlaufs ergeben sich sowohl aus externen Anforderungen und internen Abhängigkeiten als auch dem potentiellen Schadensausmass aufgrund der Betriebsunterbrechung.

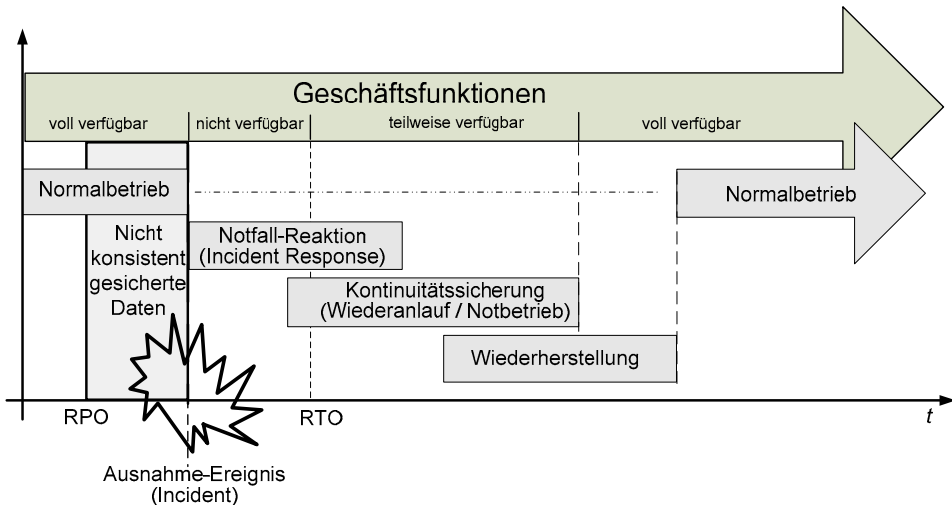


Abbildung 13.3: Zeiten und Kontinuitätsziele im Ereignisablauf

Wiederherstellungszeit

Aber auch die Zeit für die **Wiederherstellung** unterliegt oft kritischen Anforderungen. So können beispielsweise die Leistungseinschränkungen eines Notbetriebs oder dessen Kosten nicht über längere Zeit toleriert werden. Gerade in der IT sind oft während dem Notbetrieb die im Normalbetrieb vorhandenen Redundanzen nicht mehr vorhanden und bedeuten somit eine neue Gefährdung, die möglichst rasch beseitigt werden muss. Auch müssen in der Zeit der Wiederherstellung oft Bereinigungen an den Systemen sowie Korrekturen und Erfassungen von inkonsistenten oder verlorenen Daten vorgenommen werden, ohne die nur eine begrenzte Leistungsfähigkeit bei den Geschäftsprozessen möglich ist.

- ❑ Bei IT-Systemen und Daten ist auch der maximal tolerierbare Datenverlust RPO (Recovery Point Objective) zu analysieren, für dessen Dauer zu beachten ist, dass Daten bereits vor dem Ausfallzeitpunkt inkonsistent (unbrauchbar) sein können ([Mose02], S. 40-41).

Die Zeiten und Prioritäten der Wiederherstellung resultieren vor allem aus den Risiken, Kosten und den allfälligen Leistungseinschränkungen des Notbetriebs.

Die Abbildung 13.4. zeigt Beispiele wie die Prozesse eines Unternehmens auf ihre Kontinuitätsanforderungen hin analysiert werden können (vgl. [Röss05], S. 484-491).

Tabelle 1: Entwicklung Geschäfts-Impact				Tabelle 2: Zeiten und Prioritäten für Wiederanlauf						
Prozess	Unterbrechungszeiten [h]	Geschäfts-Impact (BI) monetär [T €]	MOA	Prozess	Kategorie	Wiederanlaufzeit [h]	MBCO [%]	MOA [h]	Wiederanlauf-Priorität	Mindestdauer Notbetrieb [Tage]
Produktion A	4	90		Produktion A	Kerngeschäft	8	80	36	2	4
	8	150		Produktion B	Kerngeschäft	8	70	48	3	4
	12	300		Call Center	Unterstützung	8	60	72	4	4
	24	1'000		Office-IT	Unterstützung	18	80	-	7	6
	36	10'000	x	Prod.-IT	Infrastruktur	8	90	36	1	5
	48	30'000		Entwicklung	Unterstützung	72	50	-	11	8
Produktion B	72	> 50'000		Geschäftsleitung	Unterstützung	48	90	-	8	8
	4	10		Finanzwesen	Unterstützung	72	40	-	9	8
	8	50		An- und Auslieferung	Unterstützung	8	80	72	5	6
	12	200		Personalwesen	Unterstützung	72	40	-	12	8
	24	800		Gebäudedienste	Infrastruktur	36	60	-	6	7
	36	3'000		Fuhrpark	outsourced	48	80	-	10	30
Call Center	48	10'000	x	Tabelle 3: Zeiten und Prioritäten für Wiederherstellung						
	72	> 30'000		Prozess	Kategorie	Wiederherstellung [Tage]	Wiederherstellungs-priorität			
	4	30		Produktion A	Kerngeschäft	4	3			
	8	50		Produktion B	Kerngeschäft	3	2			
	12	100		Call Center	Unterstützung	4	4			
	18	300		Office-IT	Unterstützung	4	6			
...	24	600		Prod.-IT	Infrastruktur	2	1			
	48	1'000		Entwicklung	Unterstützung	7	11			
	72	> 3'000	x	Geschäftsleitung	Unterstützung	4	7			
				Finanzwesen	Unterstützung	5	9			
				An- und Auslieferung	Unterstützung	5	5			
				Personalwesen	Unterstützung	6	10			
				Gebäudedienste	Infrastruktur	6	8			
				Fuhrpark	outsourced	14	12			

Abbildung 13.4: Beispiel Geschäfts-Impact, Wiederanlauf und Wiederherstellung

13.5.2**Risiko-Assessment**

Für eine Zertifizierung gemäss dem Standard ISO 22301:2012 ist die Organisation verpflichtet, einen formalen und dokumentierten Risiko-Assessment-Prozess durchzuführen. Mit dem Assessment-Prozess sollen die Risiken durch eine systematische Identifikation, Analyse und Bewertung, resultierend aus möglichen „Incidents“, ermittelt und beurteilt werden.

Priorisierte Anforderungen und Ziele

Dazu werden, ausgehend von den priorisierten Anforderungen und Zielen, wie sie aus dem übergeordneten Unternehmens-Risikomanagement und der Geschäftsimpact-Analyse hervorgehen, die möglichen Incidents identifiziert und analysiert. Ein solches Risiko-Assessment erfordert vor allem die folgenden Aktivitäten:

- ☐ Spezifische Analysen des Unternehmens und seines Umfeldes bezüglich möglicher Bedrohungen der Kontinuität (z.B. Energie-Engpässe, Telekom-Unterbrechungen, Sabotagen, Seuchen, Feuer);
- ☐ Analyse der Aktivitäten, Prozesse, Systeme, Informationen, Personal, involvierte Anspruchsgruppen und andere Ressourcen und Akteure auf inhärente Verletzlichkeiten und Abhängigkeiten;
- ☐ Aufsuchen der Verletzlichkeiten, Schwachstellen und Abhängigkeiten in den kritischen Geschäftsprozessen;
- ☐ Untersuchung der Abhängigkeit der Geschäfts-Prozesse von den Support-Prozessen (z.B. IT-Prozesse, Liefer- und Transportprozesse) und deren Verletzlichkeiten;
- ☐ Untersuchung der bereits vorhandenen Umgehungs-massnahmen (Workarounds).

Risikoakzeptanz

Die Bewertung der Risiken gemäss den Anforderungen, dem Risikoappetit und den Geschäftskontinuitätszielen zeigt, welche Risiken einer Behandlung bedürfen und welche Risiken akzeptiert werden können.

So zeigt sich beispielsweise beim Vergleich von Soll- und Ist-Werten (s. Abbildung 13.5), bei welchen Prozessen die Wiederanlauf- und Wiederherstellungsziele im Ereignisfalle erreicht werden können und bei welchen Prozessen eine Risikobehandlung notwendig wird.

Prozess	Kategorie	Wiederanlauf-Ziel erreichbar	Wiederherstellungs-Ziel erreichbar
Produktion A	Kerngeschäft	ja	nein
Produktion B	Kerngeschäft	nein	bedingt
Call Center	Unterstützung	ja	ja
Office-IT	Unterstützung	ja	nein
Prod.-IT	Infrastruktur	nein	nein
Entwicklung	Unterstützung	ja	ja
Geschäftsleitung	Unterstützung	nein	nein
Finanzwesen	Unterstützung	ja	ja
An- und Auslieferung	Unterstützung	ja	ja
Personalwesen	Unterstützung	nein	bedingt
Gebäudedienste	Infrastruktur	ja	ja
Fuhrpark	outsourced	ja	ja

Abbildung 13.5: Ziel-Erreichung Wiederanlauf und Wiederherstellung (vgl. [Röss05], S. 491-492).

Die detaillierten und priorisierten Bewertungsergebnisse über die Nichteinhaltung von Anforderungen, Zielverfehlungen, Impact-Entwicklungen und Schwachstellen bilden alsdann die Grundlagen für die im nächsten Schritt zu definierenden BCM-Strategien.

13.6

Geschäftskontinuität-Strategien

Die Massnahmen für die Erfüllung der Anforderungen an die Geschäftskontinuität eines Unternehmens können aufwändig und einschneidend sein. Zur Erreichung der im Rahmen der Geschäfts-Impact-Analyse und dem Risiko-Assessment festgelegten Kontinuitätsziele bestehen jedoch meist mehrere Möglichkeiten, die sich bezüglich Aufwand und Eignung in einem Unternehmen stark unterscheiden können. Einer sorgfältigen Abwägung und Auswahl der geeigneten Massnahmen in der Form von Prozessen, Aktivitäten und Ressourcen kommt deshalb grosse Bedeutung zu. Diese grundlegenden Strategien für die Erhaltung, Wiedererlangung und -herstellung der Geschäftskontinuität müssen festgelegt werden, bevor die Pläne und Vorgehensweisen im Detail ausgearbeitet werden können.

Generell gelten beim Kontinuitäts-Management wie beim Risikomanagement für jede kritische Geschäftsfunktion (Kerngeschäft, Schlüssel-Produkt oder -Dienstleistung) die folgenden

„Risiko-Behandlungs-Optionen“:

- akzeptieren, d.h. das Ausfallrisiko bewusst tragen;
- transferieren (z.B. Versicherungen, Verträge);
- vermeiden;
- reduzieren.

Bei der Option „reduzieren“ soll möglichst ein Optimum durch Reduktion

- der Häufigkeit,
- der Unterbrechungsdauer und/oder
- des Schadens

erreicht werden.

Bei der Entwicklung der Strategien ist es nützlich, an folgende Szenarien zu denken:

- ☐ Prioritäres Schutzbedürfnis der betroffenen und involvierten Menschen;
- ☐ Mangel an Personal und Fachkräften;
- ☐ Ausfall der Technik oder wichtiger Produktionsmittel;
- ☐ Ausfall wichtiger Lieferanten und Partner.

Die im konkreten Fall zu wählenden Strategien hängen vor allem von folgenden Faktoren ab von,

- ☐ Anforderungen aus der Kontinuitäts-Analyse, z.B. maximal tolerierbare Unterbrechungsdauer (MTPD* = Maximum Tolerable Period of Disruption) sowie dem Wiederanlaufziel (RTO=Recovery Time Objective), gegebenenfalls mit schrittweiser Leistungserhöhung während dem Notbetrieb.
- ☐ Aufwand und Kosten,
- ☐ betriebliche Konsequenzen für den Normalbetrieb und den Ereignisfall.

Nachfolgende Tabelle 13.2 zeigt Beispiele von Themen innerhalb einzelner Ressourcen-Gruppen, die in eine geeignete Strategie einfließen können.

* MTPD= MAO (Maximum Acceptable Outage)

Tabelle 13.2 Strategie-Themen von Ressourcen-Gruppen

Ressourcen-Gruppen	Themen-Beispiele für Ressourcen und strategische Optionen
Personal	• Zuordnung Kernkompetenzen auf unterschiedliche Personen zur Vermeidung von „Klumpenrisiken“; • Fähigkeiten und Ausbildung für den Normalbetrieb und den Ereignisfall; • Einsatz externer Kräfte im Ereignisfall. • Führung und Unterstützung der involvierten Personen während und nach dem Ereignisfall.
Informationen und Daten	• Angemessene Vertraulichkeit, Integrität und Verfügbarkeit von kritischen Prozessen und Aktivitäten; • Strategien für die Wiederherstellung von verlorenen oder verfälschten Informationen und Daten; • Alternative Informations- und Datenträger mit notwendigen Informationen während Ereignisfall
Gebäude / Lokationen	• Ausweichstandorte und Distanzen; • Ausweichstandorte bei anderen Unternehmen; • Personaleinsatz in Heimarbeit; • Personalbereitschaft an Ausweichstandort.
Geräte, Einrichtungen und Konsumgüter	• Kommunikationsgeräte, Klimageräte, Werkzeuge, Schutzbekleidung und -geräte; • Einrichtungen für Notaufenthalt (Betten, Tische Stühle, Regale etc.) • Proviant, Vorratshaltung und Verpflegungskanäle.
Technologie (ICT-Systeme)	• Unterhalt redundanter Technologie am Ausweichstandort („heisser“ oder „kalter“ Back-up); • Redundante Telecom-Verbindungen; • Prozesssteuerung via „Remote-Access“; • Automatisierte Back-up-Umschaltung;
Zulieferung, Transport und Versorgung	• Reserve-Lagerhaltung an mehreren Standorten; • Lieferung durch Ausweich-Lieferanten; • Verträge und SLAs mit Notfallklausel; • Alternative Versorgungskanäle.
Anspruchsgruppen	• Berücksichtigung der Interessen von wichtigen „Stakeholders“ (z.B. Kunden); • Ärztliche / psychologische Betreuung.
Offizielle Krisen- und Notfallorganisationen	• Vertrautheit / Vorgehensplanung / Meldwesen mit externem Krisenmanagement, Feuerwehr, Polizei oder Ambulanz.

13.7

Geschäftskontinuitäts-Verfahren und Pläne

Nach der Definition der Kontinuitätsstrategien folgt nun im „BCM-Lebenszyklus“ die Phase der Entwicklung geeigneter Reaktionen und Pläne für ein mögliches „Incident“ (s. Abbildung 13.3).

Die Definition eines „Incidents“ im Zusammenhang mit dem Geschäftskontinuitäts-Management lautet [Buco06]:

Incident

Ein „Incident“ ist eine Situation, welche zu einer Geschäftsunterbrechung, zu einem Verlust, Notfall oder einer Krise führen kann oder könnte.

Das schnelle und folgerichtige Handeln beim Eintritt eines Incidents ist nach Möglichkeit vorzubereiten. Wie bereits erwähnt, kann ein Incident sowohl „schadensminimierende“ als auch lediglich „präventive“ Aktionen zur Verhinderung von Schadensfolgen erforderlich machen.

13.7.1

Krisenmanagement

Eskalationsstufen

Sprechen die Anzeichen eines Incidents für den Einsatz von präventiven Massnahmen oder ist eine Schadenssituation in lediglich geringfügigem Ausmass eingetreten, dann wird diese unterste Eskalationsstufe als „**kritischer Zustand**“ bezeichnet. Hingegen wird der Begriff „**Notfall**“ verwendet, wenn ein Zustand erreicht wird, bei dem ein Prozess in seiner normalen Funktionsweise innerhalb einer definierten Zeit nicht wiedererlangt werden kann. Entsprechend der häufig verwendeten Terminologie werden Ereignisse, die bei einzelnen Geschäftsprozessen mit beachtlichen Schäden einhergehen als „**Krisen**“ bezeichnet. Die Ereignisse der höchsten Eskalationsstufe, bei denen Schadenauswirkungen bei mehreren oder allen Geschäftsprozessen auftreten, werden als „**Katastrophen**“ definiert. Entsprechend dem Eintritt solcher Eskalationsstufen (s. Tabelle 13.1) wird auch das entsprechende „Führungsgremium“ einberufen, das sich mit dem Ereignis zu befassen hat.

Führungs-Gremien

Häufig anzutreffende Bezeichnungen für Gremien, die sich mit der Bewältigung eines bestimmten Ausnahmezustands zu befassen haben, sind die Begriffe „Notfallstab“, „Krisenstab“ oder „Katastrophenstab“.

*Alarmierungs-
verfahren*

Die Einberufung eines derartigen Gremiums erfolgt durch ein **Alarmierungsverfahren**, das nach vorgegebenen Regeln mit vorbestimmten Kommunikationseinrichtungen (z.B. Telefon, Handy, Pager, Lautsprecher-Durchsagen) verläuft und oft in einen „**Incident-Management-Prozess**“ eingebettet ist.

Beim Eintritt einer Ausnahmesituation gilt es, anhand der vorbereiteten Pläne und möglichen Massnahmen-Optionen, das für die Bewältigung optimale Vorgehen zu entscheiden.

*Führungs-
rhythmus*

Das Führen des für die Ausnahmesituation im Voraus nominieren Gremiums* (Notfallstab, Krisenstab oder Katastrophenstab) erfolgt nach einem für derart zeitkritische Führungssituationen definierten Prozess, dem sogenannten „**Führungsrhythmus**“.

*Protokollierung
Einzelschritte*

Das für alle Gremiumsmitglieder sichtbare Protokollieren der Einzelschritte (z.B. mit Flip-Chart, Beamer oder Hellraumprojektor) ist bei komplexen Entscheidungssituationen unverzichtbar. Bei allen Aktivitäten, die durch diesen Prozess ausgelöst werden, sind die Zeiten zu registrieren, budgetieren und zu kontrollieren.

Schritte des Führungsrhythmus:

1. Problemerkfassung
2. Sofortmassnahmen
3. Beurteilung der Lage
4. Entschluss
5. Auftrag
6. Umsetzungssteuerung / Überwachung

Schritt 1: Problemerkfassung

Um beim Auftritt eines Ausnahmezustands bestimmen zu können, welche Sofortmassnahmen und welche Pläne in welcher Form zum Einsatz gelangen sollen, sind durch das aufgebotene Gremium, wir bezeichnen es im Weiteren als Krisenstab, die Problemerkfassung an allererster Stelle durchzuführen. Diese erste Aufgabe besteht darin, sich ein Bild über das eingetretene Ereignis zu verschaffen und eine erste Lagebeurteilung durchzuführen.

* Entsprechend der Organisationsstruktur des Unternehmens können für verschiedenen Problemerkategorien verschiedene Gremien definiert sein, die hierarchisch aufeinander abgestimmt und geführt werden. Es können auch dieselben Gremien entsprechend der Führungsanforderungen personell modifiziert werden.

ren. Die für die Problemerkfassung zu beantwortenden Fragen sollten womöglich anhand einer Checkliste vorgängig eingeübt sein:

*Checkliste
Problemerkfassung
und
Lagebeurteilung*

- ☐ Was ist geschehen und wer ist betroffen?
- ☐ Schäden an Leib und Leben?
- ☐ Betroffene Bereiche, Räumlichkeiten, Einrichtungen?
- ☐ Betroffene kritische Geschäftsprozesse und Auswirkung auf Markt und Kunden?
- ☐ Betroffene Support-Prozesse und IT-Systeme?
- ☐ Bestehen Informationsdefizite und wie können diese geschlossen werden?
- ☐ Haben sich Informationsverluste ergeben?
- ☐ Grobe Schätzung der Schadensauswirkung und Schadenshöhe?
- ☐ Wer wurde bereits informiert?
- ☐ Bereits getroffene Massnahmen?
- ☐ Ist bereits eine Eskalation an andere oder höhere Notfallinstanzen notwendig?
- ☐ Gibt es bereits wichtige Hinweise für die Ursachen im Sinne einer Schadensbegrenzung?
- ☐ Mit welcher Unterbrechungsdauer ist zu rechnen?
- ☐ Besteht das Potential für eine Ausweitung und weitere Schäden?

Schritt 2: Sofortmassnahmen

Aufgrund erster Informationen trifft der Krisenstab die Entscheide für die Beauftragung von Sofortmassnahmen. Solche Sofortmassnahmen sind beispielsweise:

- ☐ sofortige Hilfeleistungen;
- ☐ Alarmierung von Rettungskräften, falls noch nicht erfolgt;
- ☐ Evakuationsanordnung;
- ☐ weitere notwendige Alarmierungen;
- ☐ Massnahmen zur Verhinderung von Schadensausweitungen (z.B. Ordentliches Herunterfahren von Systemen einleiten);
- ☐ Anforderung wichtiger Spezialisten, Materialien, Werkzeuge und Transportmittel;
- ☐ Einholung wichtiger Informationen;

- ❑ Benachrichtigung wichtiger Stakeholder- und Behörden-Instanzen.

Bei den Sofortmassnahmen ist darauf zu achten, dass sie aufgrund des jeweiligen Informationsstands jederzeit möglich sein müssen und dass die später zu treffenden Entschlüsse nicht präjudiziert werden.

Schritt 3: Beurteilung der Lage

Die Lagebeurteilung soll die Grundlagen für die dem Ereignis angemessenen weiteren Entschlüsse liefern. Dafür sind die bereits eingetretenen und die noch zu erwartenden Schäden zu beurteilen. Wichtig sind dabei die Zeitverhältnisse und möglichen Massnahmen zur möglichst effektiven und effizienten Bewältigung sowie zur späteren Rückführung in den Normalzustand. Bereits dieser Schritt erfordert die Darlegung von alternativen Problemlösungen mit ihren Vor- und Nachteilen.

Schritt 4: Entschlüsse

Aufgrund der in der Lagebeurteilung dargestellten Schadensbeurteilungen und Problemlösungen fällt der Krisenstab die zu diesem Zeitpunkt möglichen Entscheide zur Bewältigung des Ausnahmezustands. Die Entschlüsse sollen zielorientiert unter Abwägung der Vor- und Nachteile der relevanten Alternativen gefällt werden. Nach Möglichkeit werden dazu zusätzliche Informationsquellen (z.B. Helpdesk) und die Kommunikation mit internen und externen Instanzen und Anspruchsgruppen beigezogen.

Schritt 5: Aufträge

Die Aufträge an die verschiedenen Teams werden durch den Krisenstab mittels einer Aktivitätenliste verwaltet. Jede Aktivität erhält einen beauftragten „Owner“, einen „Ausgabezeitpunkt“, und ein „Zeitbudget“ sowie einen „Berichterstattungszeitpunkt“, an dem der Fortschritt der Aktivität kontrolliert und abgestimmt werden muss.

Schritt 6: Umsetzungssteuerung / -Überwachung

Die Berichterstattungszeitpunkte ermöglichen dem Krisenstab die Kontrolle über den Bewältigungs-Fortschritt und das Fällen weiterer Entschlüsse. Der Führungsrhythmus ist ein Kreislauf-Prozess, der entsprechend der Entwicklung der Situation, iteriert durchlaufen wird. In der Regel liegt der wiederholte Einstieg in den Führungskreislauf bei der „Beurteilung der Lage“.

13.7.2

Kriterien für Plan-Aktivierungen

Die Pläne enthalten für grundlegende Szenarien sozusagen die vorgefertigten Rezepte und Massnahmen-Konstellationen (Dispositive) für eine effektive und effiziente Problembewältigung. Die Pläne werden nach einem Ereigniseintritt aufgrund bestimmter Kriterien aktiviert. Solche Kriterien sind im Voraus festzulegen (s. Checkliste) und sind beispielsweise:

Kriterien

- ☐ Ereignisart (z.B. Computerviren, Gebäudebrand, Stromausfall, Bombendrohung)
- ☐ Gefährdung von Menschen
- ☐ Schadensausmass für Gebäude und Einrichtungen
- ☐ Kritikalität für kritische Geschäftsprozesse
- ☐ Voraussichtliche Dauer der Störung oder Unterbrechung

Bei einem „Incident“ sind generell die Phasen „Notfall-Reaktion“, „Kontinuitäts-Erhalt“ und „Wiederherstellung“ zu unterscheiden (s. Abbildung 13.3). Einige der in einer Notfallsituation* einzusetzenden Pläne sind im Abschnitt 13.1 bereits kurz erläutert. Schon beim Eintritt eines Ereignisses, in dessen Folge ein Notfall entstehen könnte, sind Massnahmen zu ergreifen, die präventiv zur Schadensverhinderung oder -reduzierung führen.

Plan-Aktivierungen

Entsprechend der Ausnahmesituation und der Phase, in der sich der Ausnahmezustand befindet, wird der entsprechende Plan aktiviert:

Plan-Aktivierung:

- Betrifft die Ausnahmesituation IT-Prozesse, dann kommt der „**IT-Notfall-Plan**“ zum Einsatz.
- Sind bei einer Ausnahmesituation auch kritische Geschäftsprozesse betroffen, dann kommen die für die Ausnahmesituation massgeblichen „**Geschäftskontinuitäts-Pläne**“ zum Einsatz. Die Aktivierung des Betriebskontinuitätsplans, des Ausweichplans und/oder des IT-Notfall-Plans hängen vom Szenario ab und sind dem Geschäftskontinuitäts-Plan untergeordnet.

* Der Begriff „Notfall“ wird oft auch für die Eskalationsstufen „Krise“ und „Katastrophe“ verwendet.

13.7.3

Ressourcen und externe Abhängigkeiten

Bei der Geschäfts-Impact-Analyse und dem Risiko-Assessment sowie den Kontinuitäts-Strategien wurden bereits wichtige Anforderungen und Ressourcen zur Kontinuitätssicherung festgelegt. In diesem Schritt des BCM-Prozesses werden nun die Ressourcen und externen Abhängigkeiten für den notfallbedingten Einsatz in der Form von Listen, Verzeichnissen, Checklisten und Einsatzplänen zusammengestellt.

Ressourcen für den Notfall:

- ☐ Lebenswichtige Informationen und Informationsbestände (vital records);
- ☐ Kontaktlisten für Notfallorganisation und Mitarbeiter (Adressen, Telefonnummern, usw.);
- ☐ Betriebs-Handbücher;
- ☐ IT-Notfall-Plan (einschliesslich Wiederanlaufverfahren);
- ☐ Lager- und Daten-Speichereinrichtungen an Ausweichstandorten mit entsprechenden Zugriffsprozeduren (Zweit- und ggf. Drittstandorte);
- ☐ Ausweichstandorte (falls erforderlich) für kritische Geschäftsprozesse einschliesslich kritischer Support-Prozesse (z.B. Zentral-Computer, vernetzte IT-Arbeitsplätze);
- ☐ Minimale Anzahl notwendiger Mitarbeiter zur Betreuung der notwendigen Prozesse und Funktionen (Auflistung der Mitarbeiter und deren Aufgaben und erforderlichen Fertigkeiten);
- ☐ Notarbeitsplätze
- ☐ IT-Infrastruktur und Applikationen;
- ☐ Telekommunikations-Infrastruktur und -Support;
- ☐ Büro- und Spezialgeräte;
- ☐ Versorgungs-Infrastruktur (z.B. Wasser, Strom, Entsorgung).

Externe Abhängigkeiten:

- ☐ Kontaktlisten für Kontaktpersonen innerhalb und ausserhalb der Geschäftszeiten;
- ☐ Zu erfüllende Anforderungen der Anspruchsgruppen (z.B. minimaler Service-Level, Verpflichtungen);

- ☐ Alternative Fakten im Notfall (z.B. andere Postadressen, geänderte Lieferbedingungen);
- ☐ Alternative Möglichkeiten zur Vertragserfüllung.

13.7.4

Plan-Zusammenstellung

Nachdem in den vorangegangenen Schritten wichtige Anforderungen und Ressourcen zur Kontinuitätssicherung sowie die Ressourcen rund um den notfallbedingten Einsatz ausgearbeitet wurden, erfolgt in diesem Schritt die Zusammenstellung der Pläne für den konkreten Einsatz.

Allen Plänen gemeinsam ist die Definition des Anwendungszwecks und des Einsatzbereichs. Ebenso gehören in die Pläne die mit dem Plan zu erfüllenden Ziele, die Planung der organisatorischen Umsetzung und Inkraftsetzung sowie die Kriterien und Verfahren zu deren Aktivierung.

Die Aktivitäten zur Plan-Zusammenstellung sind:

- ☐ Koordinierung, Konsolidierung und Dokumentation der Pläne über folgende Inhalte:
 - Geschäftsfunktionen, Organisationseinheiten und Standorte;
 - Zur Anwendung gelangende Geschäftskontinuitätsstrategien;
 - Definition von Zeitvorgaben einzelner Aktivitäten während der Notfallsituation und „vorbehaltener Entscheide“* für bestimmte Konstellationen und Massnahmen-Varianten.
- ☐ Festlegung der Notfallorganisation:
 - Definition der Katastrophen-, Notfall- und Krisenstäbe, welche im Ereignisfall für die Abwicklung der Kontinuitätspläne resp. deren Teilpläne verantwortlich sind;
 - Festlegung der Funktionen und Rollen einschliesslich der Verantwortlichkeiten und Kompetenzen für das Not-

* „Vorbehaltene Entscheide“ gelangen zur Ausführung, sobald die im Notfallplan vorgesehenen Bedingungen erfüllt sind. Ein vorbehaltener Entscheid kann beispielsweise lauten, dass nach vergeblichen Reparatur- und Restart-Versuchen von x Stunden ohne weitere Rückfragen die Umschaltung auf ein kaltes Backup-System vorgenommen wird.

fall- und Geschäftskontinuitäts-Management. Besetzung der Funktionen durch Personen und Stellvertreter;

- Festlegung der Eskalations-Kriterien für die Übergabe der Führungsverantwortlichkeiten und Kompetenzen des Normalbetriebs in die Führungsverantwortlichkeiten und Kompetenzen der Notfall- und Krisenstäbe.
- ☐ Festlegung von Krisensitzungs-Räumen mit entsprechenden Sitzungs-Ressourcen (z.B. Konferenz-Telefon, Projektor, Situationspläne);
- ☐ Festlegung der im Ereignisfall relevanten internen und externen Abhängigkeiten und Interaktionen;
- ☐ Verzeichnis der Checklisten, diversen Kontaktlisten (Kunden, Lieferanten und Mitarbeiter);
- ☐ Festlegung der Informations- und Aufgebots-Hierarchie;
- ☐ Festlegung der Anlaufstellen für öffentliche Notfallorganisationen (z.B. Polizei, Feuerwehr, Spitäler);
- ☐ Erstellung der Kontinuitäts- und Notfalldokumentation in mobiler Form und an den diversen Standorten verfügbar. Der Zugriff auf diese Dokumentationen darf nur durch dafür autorisiertes Personal möglich sein. (Die Dokumentation kann in chiffrierter Form auf eine CD gebrannt werden. Die autorisierten Personen erhalten einen Dechiffrier-Schlüssel, sodass sie die Dokumentation mit einem herkömmlichen Notebook dechiffrieren und lesen können);
- ☐ Dokumentationen, Informationsfluss sowie spezielle Kommunikationsanforderungen und Hinweise auf das generelle Kommunikationskonzept im Ereignisfall.

13.7.5

Kommunikationskonzept für Ereignisfall

- ☐ Festlegung der im Notfall (resp. Katastrophen- oder Störfall) zu erreichenden Informationsempfänger:
 - Mitarbeiter und allenfalls ihre Familien-Mitglieder;
 - Aktionäre;
 - Verwaltungsratsmitglieder;
 - Medien (z.B. Presse, Radio und Fernsehen);
 - Behörden, kommunale und staatliche Stellen;
 - Regulatoren;
 - Kunden, Lieferanten und Vertragspartner;
 - usw.

- ☐ Festlegung wie und durch wen informiert wird (z.B. CEO, Public-Relation-Stelle, Personalverantwortliche, Vorgesetzte);
- ☐ Einschränkungen bezüglich Information (z.B. Bankgeheimnis, Informationenschutz, vertragliche Geheimhaltungsvereinbarungen);
- ☐ Festlegung, durch welche Stellen die Abgabe von Informationen autorisiert sein muss;
- ☐ Festlegung der Informationsart an die verschiedenen Empfänger und Vorbereitung von Muster-Texten an die verschiedenen Informations-Empfänger unter Annahme verschiedener Szenarios;
- ☐ Festlegung und Vorbereitung der Informationskanäle (z.B. Telefon, Anlaufstellen bei Medien, Fax, Hotline, Homepage) und der Kommunikations-Intervalle für die verschiedenen Empfänger.

13.8

Tests, Übungen und Plan-Unterhalt

Die Ergebnisse der Tests, Übungen und die Ausrichtung der Kontinuitätsvorkehrungen an den aktuellen Geschäftsanforderungen sind Bestandteil der Kontrollverantwortung der Leitungsorgane (Verwaltungsrat, Geschäftsleitung) eines Unternehmens.

Nachweispflicht

Die Nachweispflicht über die Funktionstüchtigkeit des Kontinuitätsmanagements erstreckt sich jedoch meist noch weiter, indem Auftraggeber, Regulatoren und weitere Anspruchsgruppen periodisch Bericht über die Ergebnisse von realistisch durchgeführten Tests und Übungen verlangen. Viele Unzulänglichkeiten und Fehler treten bei Tests und Übungen, aber auch bei tatsächlich aufgetretenen Ereignissen und Notfällen zutage.

BCM-Kultur

Im Sinne eines kontinuierlichen Verbesserungsprozesses (PDCA-Zyklus) verlangen heutige BCM Standards (z.B. [Isob12]) die Pflege einer auf die Kontinuitätsziele ausgerichteten Unternehmens-Kultur.

Praxistipp:

Zu einer Kontinuitätskultur der kontinuierlichen Verbesserung gehört unter anderem, dass Fehler und Mängel zur Ableitung von Lehren (lessons learned) und korrektiven Massnahmen kommuniziert werden.

13.8.1

Tests

Wirklichkeitsnahe Tests

Die Pläne müssen mit ihren zugrunde liegenden Prozessen, Systemen und Personen möglichst wirklichkeitsnah getestet werden. Beim Testen wird in erster Linie die Logik des Plans sowie die Funktionstüchtigkeit und Angemessenheit der für den Notfall zur Verfügung stehenden Ressourcen (z.B. Systeme, Einrichtungen, Umschalt- und Ausweichprozesse) überprüft.

Finden von Mängeln und Fehlern

Die Tests dienen dem Auffinden von allfälligen Mängeln und Fehlern in der Logik, den Kapazitäten und den Leistungsfähigkeiten der zur Verfügung stehenden Ressourcen.

Die Tests sollen den aus einzelnen Risiko-Szenarien resultierenden Anforderungen unterworfen werden. Aus den gewonnenen Testresultaten können Schlüsse für die Festlegung von wichtigen Parametern (z.B. Auslegung von Noteinrichtungen, Zeitpunkte der Informationensicherungen) sowie der notwendigen Verbesserungen gezogen werden.

13.8.2

Übungsvorbereitungen und -Durchführungen

Vorbereitung auf allfälliges Ereignis

Bei den Übungen geht es in erster Linie um die Vorbereitung der Mitarbeiter, des Managements und vor allem der Mitglieder der am Krisenmanagement beteiligten Gremien und Organisationseinheiten auf ein allfälliges Ereignis.

Lernen und Überprüfen

Sie dienen dem Lernen und der Überprüfung der notwendigen Kenntnisse und Fertigkeiten zur Bewältigung der Notfälle. Aufgrund realistischer Szenarien wird der Ablauf eines Notfalls vom Zeitpunkt des Ereignis-Eintritts, über die geänderte Geschäftsfurtherführung bis hin zur Wiederherstellung des Normalbetriebs durchgespielt.

Fiktive Situationsbeschreibungen

Für nicht real durchführbare Situationen werden entsprechende Situationen durch Meldungen mit fiktiven Situationsbeschreibungen kommuniziert, worauf von den Übungsteilnehmern entsprechende Entscheide, Anordnungen und Aktionen durchgeführt werden müssen (z.B. Evakuations-Übung aufgrund einer fiktiven Katastrophe).

Die Übungen erfordern eine umfangreiche Vorbereitung:

- ☐ Ein entsprechendes Notfallszenario wird mittels eines Drehbuches in eine Übungsabfolge umgesetzt;
- ☐ Die Steuerung der Abfolge kann durch „Marquiere“ erfolgen, die zu gegebenen Zeitpunkten fiktive Lagebeschreibungen und Zusatzinformationen an die Übungsteilnehmer abgeben;

- ❑ Die Aktionen der „Beübten“, aufgrund vorgegebener Lagebeschreibungen, wird durch die Übungsleitung beurteilt und bei den auf die einzelnen Übungssequenzen folgenden Übungsbesprechungen im Sinne von Verbesserungshinweisen mit den Übungsteilnehmern besprochen.

Wichtige Übungsziele sind beispielsweise:

- ❑ Überprüfung und Verbesserung des Führungsverhaltens in Notfall- und Krisensituationen mit zeit- und sachgerechten Entscheidungen;
- ❑ Stufengerechte Informations- und Verantwortungsübertragung;
- ❑ Krisenkommunikation gegenüber Anspruchsgruppen und Medien (einschl. Üben von Fernsehauftritten);
- ❑ Zeitgerechte und angemessene Alarmierungen sowie rechtzeitige Einfeldung am vorgegebenen Treffpunkt (z.B. Krisenraum);
- ❑ Schnelle und reibungslose Evakuationen;
- ❑ Überprüfung des organisatorischen Ablaufes bei der Notfall- und Krisenbewältigung;
- ❑ Schaffung eines angemessenen Risiko- und Sicherheitsbewusstseins unter Führungspersonen und Mitarbeitern;
- ❑ Vertrauensbildung für Anspruchsgruppen, Führungspersonen und Mitarbeiter (Anspruchsgruppen sollen, wo sinnvoll und möglich, auch in die Plan-Überprüfungen einbezogen werden).

13.8.3

Wartung und Überprüfung der Pläne

Periodische und fallweise Prüfung, Anpassung und Kommunikation

Die Pläne müssen periodisch (z.B. jährlich) überprüft und angepasst werden. Bei signifikanten Veränderungen (z.B. Umzügen, Reorganisationen, Veränderung bei den Geschäfts- oder Supportprozessen) müssen die Pläne entsprechend der Veränderungen der Risiken und Massnahmen-Situationen angepasst werden. Wichtig ist, dass die Änderungen der Pläne, Checklisten und sonstigen Utensilien in geeigneter Form an die massgeblichen Stellen kommuniziert werden.

Jahresprogramm

Die Entwicklung und Wartung sämtlicher Pläne, Aktivitäten, Massnahmen, Tests, Übungen usw. werden vorteilhaft in einem entsprechenden „Jahresprogramm“ geplant und festgehalten. Für den Unterhalt des fortlaufenden Kontinuitäts-Programms emp-

fehlt es sich, eine Person oder Organisationseinheit zu beauftragen.

Praxistipp:

Zur Nachführung der Pläne müssen dazu verantwortliche Personen nominiert werden. Für einfache Geschäfts- oder Supportfunktionen kann das Nachführen durch eine Person nebenamtlich durchgeführt werden. Für komplexe Funktionen bedarf es hauptamtlicher Stellen oder Teams, die für das Nachführen verantwortlich zeichnen. Die Richtigkeit und Aktualität ist nach dem „Vieraugenprinzip“, wenn nicht sogar durch eine fachliche Kontrollstelle, regelmässig zu überprüfen.

Bei den periodisch durchzuführenden Übungen soll unter anderem die Aktualität der Pläne ein Kriterium der Übungsbeurteilung sein. Die Pläne sind vor allem übersichtlich und nur mit wichtigen und für den Ereignisfall absolut notwendigen Informationen aufzubauen. Ansonsten können sie kaum aktuell gehalten werden und können im Ereignisfall zu Fehlentscheiden und unnötigen Verzögerungen führen.

13.9

Leistungsbewertung

13.9.1

Überwachung und Überprüfung

Überwachung

Durch die ständige Überwachung wird sichergestellt, dass Ereignisse, die auf die Kontinuität einen Einfluss haben können, kurzfristig hinsichtlich korrektiver Eingriffe erkannt werden.

Überprüfung

Die Überprüfungen, welche periodisch oder aufgrund besonderer Anlässe (z.B. infolge signifikanter Veränderungen der Gefahrenlage oder der Geschäftsprozesse) erfolgen, dienen mehrheitlich der Erkennung von grossen Abweichungen von den beabsichtigten Ergebnissen.

Für eine sinnvolle Überwachung und Überprüfung der Leistung des BCM-Systems sind einige grundsätzliche Voraussetzungen zu erfüllen, die vorteilhaft in einem Überwachungs- und Prüfkonzept festgehalten werden.

Ein solches Überwachungs- und Prüfkonzept gibt beispielsweise die Antwort auf folgende Fragen:

- ☐ Was kann mit welchen Metriken wie geprüft und gemessen werden, um die Wirksamkeit des Kontinuitätsprogramms mit allenfalls korrekativen Massnahmen sicher zu stellen?
- ☐ Zu welchen Zeitpunkten oder Anlässen sollen die Messungen, Überprüfungen und Auswertungen durchgeführt werden?
- ☐ Wer ist für die Durchführung verantwortlich und an wen geht die Berichterstattung?
- ☐ Was wird in welcher Weise dokumentiert?
- ☐ Werden die Erreichung von Policy-Vorgaben, der Anforderungs-Ziele sowie der Konformität der zugrundeliegenden BCM-Prozesse adäquat gemessen und überprüft?

Selbstüberprüfung Die Überprüfung des im vorigen Abschnitt erwähnte „BCM-Jahresprogramms“ könnte als Selbstüberprüfung (Selfassessment) anhand einer Prüfliste erfolgen, welche die Prüfpunkte des gesamten BCM-Prozess enthält.

In geplanten Intervallen sind auch Überprüfungen durch die „Interne Kontrolle“ oder durch „Externe Reviews“ (Audits) durchzuführen, wodurch gegenüber der Selbstüberprüfung eine grössere Unabhängigkeit in den Bewertungen gewährleistet wird.

13.9.2

Internes und externes Audit

Interne Audits

Der internationale Standard ISO 22301:2012 verlangt, in geplanten Intervallen sogenannte „Interne Audits“ durchzuführen. Diese Audits sollen zur Überprüfung beitragen,

- ☐ ob das BCM-System zu den Anforderungen des Unternehmens und
- ☐ zu den Anforderungen des obengenannten Standards konform und wirksam umgesetzt und betrieben wird.

Im deutschen Sprachgebrauch fällt diese Aufgabe der Internen Revision zu und wird meist im Rahmen der gesetzlich verlangten „Internen Kontrolle (IKS)“ des Unternehmens abgewickelt. Diese Aufgabe kann durch eine interne Abteilung aber auch im „Outsourcing“ durch eine externe Firma ausgeübt werden.

Externe Audits

Die Externe Revision (external audit) ist ein unternehmensexternes Prüfungsorgan, das zum einen den gesetzlich vorge-

schriebenen Geschäftsabschluss prüft, zum anderen vermehrt aber auch Interne Prozesse wie das Geschäftskontinuitäts-Management in ihre Prüfergebnisse einbezieht. Auch besitzen einige externe Revisionsgesellschaften die „Akkreditierung“, die „Zertifizierung“ des eingesetzten BCM-Systems nach ISO 22301:2012 durchzuführen.

*Behebung Nicht-
konformitäten*

Es ist jedoch Aufgabe und Verantwortung des für den auditierten Bereich zuständigen Managements, dafür zu sorgen, dass die durch die Audits aufgezeigten „Nichtkonformitäten“ sowie deren Ursachen in nützlicher Zeit behoben werden. Es entspricht der praktischen Logik, dass anhand von Folgeüberprüfungen die Korrekturen überprüft und die Resultate in die Berichterstattung aufgenommen werden müssen.

13.9.3

Überprüfung durch Management

In den vorhergehenden Schritten des Kontinuitätsmanagement-Prozesses waren die Übungen und Tests wie auch die Wartung des aufgebauten „Kontinuitätsprogramms“ sowie der gesamte Prozess durch die jeweils in ihrem Bereich zuständigen Stellen zu überwachen und zu überprüfen.

*Überprüfungen
durch Oberleitung*

Aus der Sicht der Oberleitung des Unternehmens (Verwaltungsrat und Geschäftsleitung) ist es wichtig, die Angemessenheit des vorhandenen Kontinuitätsmanagement-Prozesses zu überwachen und auf Effektivität und Effizienz zu überprüfen. Dabei geht es beispielsweise um folgende Fragen:

- ☐ Ist die definierte Kontinuitätspolitik den aktuellen externen und internen Geschäftsanforderungen angemessen?
- ☐ Ist ein wirksames Kontinuitätsprogramm erstellt und wird es umgesetzt?
- ☐ Welche Übungen und Tests wurden durchgeführt und was sind die Ergebnisse?

*Regelmässige Be-
richterstattungen*

Solche Informationen erhalten die Leitungsgremien eines Unternehmens zum einen aus geplanten regelmässigen Berichterstattungen und zum anderen aus aktiven Mitwirkungen im Prozess. Für die Leitungs-Instanzen prädestinierte Mitwirkungsaktivitäten sind die Festlegung von Meilensteinen, die Impact-Bewertungen, die Abnahme von Zwischenergebnissen und das Füllen von wichtigen Entscheidungen bei der Planung und der Umsetzung des Kontinuitätsmanagements.

*Überwachung
Konformität*

Dabei achten die Leistungs-Instanzen darauf, dass, beispielsweise durch Audit-Aufträge, die Konformität zum beabsichtigten Prozess vorhanden ist und die gesetzten Ziele erreicht werden.

Zur Nachweissicherung* für alle möglichen Situationen sind die Ergebnisse der Überwachungen und Prüfungen auch zu dokumentieren.

*Einbezug Lei-
tungsgremien*

Als konkrete Beispiele für den Einbezug der Leitungsgremien in den BCM-Prozess können genannt werden:

- ☐ Genehmigung von Policy-Dokumenten sowie der Pläne und Projekte zur Kontinuitäts-Verbesserung;
- ☐ Bestimmung periodischer Meilensteine zur Überwachung und Überprüfung und Berichterstattung (z.B. Festlegung von Übungs- und Prüfaktivitäten sowie Berichterstattungsterminen);
- ☐ Anordnung von Überprüfungen, Bewertungen und Berichterstattung bei signifikanten Veränderungen (z.B. Neue Geschäftsprozesse, Organisations-Restrukturierung)
- ☐ Akzeptanz grosser Risiken aus Unternehmenssicht;
- ☐ Lehren resultierend aus aufgetretenen Fällen;
- ☐ Überprüfung der Compliance zu gesetzlichen, regulatorischen und vertraglichen Anforderungen.

*Aussagekräftige
Indikatoren*

Zur Berichterstattung an die Leitungsgremien sind, unter anderem, aussagekräftige Indikatoren einzusetzen, die auf möglichst vergleich- und reproduzierbaren Fakten beruhen. Dabei ist dem Umstand Rechnung zu tragen, dass im Unternehmen schwere Ausfälle womöglich nicht oder nur sehr selten vorkommen und somit wenig Erfahrungsmaterial liefern.

*Kennzahlen ohne
Ereigniseintritt*

Deshalb müssen die Leistungskennzahlen so definiert werden, dass sie über Effektivität und Effizienz Auskunft geben können, ohne dass entsprechend schwere Ereignisse eingetreten sind. Solche Indikatoren beruhen beispielsweise auf erfolgreich abgewehrten oder häufig eingetretenen Ausnahmeereignissen mit geringen Schäden aber hohem Schadenspotential. Aussagekräftige Indikatoren können auch durch unangemeldete Tests (z.B. Reaktionszeiten nach Probealarmierungen) aufdatiert werden.

* Unter anderem gilt es für das zuständige Management zu bedenken, dass es für Unterlassungen mit allfälligen Konsequenzen verantwortlich gemacht werden kann.

Aussagekräftige Indikatoren ergeben sich auch aus dem wiederholten Auftreten gleichartiger Fälle.

*Hypothetische
Ereignisszenarien*

Wichtig sind auch regelmässige Aussagen über mögliche Massnahmen in rein hypothetische Ereignis-Szenarien, die unter gewissen Bedingungen eintreten könnten (z.B. „Blended Threats“, Insider-Angriffe).

13.10

Kontinuierliche Verbesserungen und Wiederholungen

Das BCM-System wird, wie der Abschnitt 13.9 zeigt, in allen Aspekten überwacht und überprüft und die Resultate den allfälligen Entscheiden zugeführt. Dabei sollen alle wesentlichen Schritte dokumentiert werden. Jedoch zeigen sich sowohl in der Qualität und Angemessenheit der Aktivitäten einzelner Prozessschritte als auch in der Erfüllung von Anforderungen und der Zielerreichung immer wieder Lücken mit entsprechendem Handlungsbedarf.

Lücken mit Handlungsbedarf

Zum Schliessen der Lücken sowie zur Anpassung an neue Gegebenheiten ist es oft notwendig, einzelne Schritte oder sogar den gesamten BCM-Prozess im Sinne einer Verbesserung oder mit neuem „Input“ wiederholt durchzuführen.

*Nichtkonformität
und korrigierende
Aktivitäten*

Dort wo die beabsichtigte Funktionstüchtigkeit des Prozesses, z.B. in Anlehnung an den Standard ISO 22301, Lücken oder „Nicht-Konformitäten“ aufweist, sind entsprechende Aktionen zu definieren und durchzuführen, um die Lücken zu beseitigen.

*Kontinuierliche
Verbesserungen*

Die Eignung, Angemessenheit und Wirksamkeit des BCMS soll im Sinne eines PDCA-Zyklus kontinuierlich verbessert werden. Die Verbesserung kann vor allem über die Teilprozesse, Führung, Planung und Leistungsbewertung des BCMS erreicht werden.

13.11

IT-Notfall-Plan, Vulnerability- und Incident-Management

IT-Notfall-Plan

Der IT-Notfall-Plan wurde im Abschnitt 13.1.4 grob vorgestellt. Die einzelnen Prozess-Schritte und die Methode des Aufbaus sind dem Geschäftskontinuitäts-Plan ähnlich, deshalb wird sein detaillierter Aufbau im Folgenden nicht weiter behandelt. Die Vernetzung des IT-Notfall-Plans mit dem Geschäftskontinuitäts-Plan ist jedoch von Unternehmen zu Unternehmen stark verschieden. In Unternehmen mit überwiegend IT-Dienstleistungen können die Geschäftskontinuitäts-Pläne und IT-Notfallpläne in vielen Punkten miteinander verschmolzen werden.

*Integration
Vulnerability-
und Incident-
Plan*

Für den IT-Notfall-Plan ist die Integration des „Vulnerability- und Incident-Plans“ von grosser Bedeutung. Beim Vulnerability- und Incident-Management geht es zum einen um die meist sofortige Prävention gegenüber bösartiger Attacken, die heute zum grossen Teil über das Internet erfolgen*. Zum anderen können die Ausnahmeereignisse auch aus unbeabsichtigtem Fehlverhalten von Personen oder von Fehlern und Ausfällen technischer Einrichtungen herrühren. Dabei kümmert sich das Incident Management jeweils in erster Linie um die schnellstmögliche Kontinuitätssicherung des Geschäftsbetriebs, aber auch um das Ziel, den „Normalbetrieb“ in nützlicher Frist wieder herzustellen. Dazu gehören die unmittelbare Kommunikation des Ausnahmeereignisses an die für die Beseitigung zuständigen Stellen sowie die Handlungen zur Bewertung und Aufzeichnung hinsichtlich einer kontinuierlichen Verbesserung der Sicherheitslage.

Incident

Wie bereits unter Abschnitt 13.7 aufgeführt, ist ja ein Incident eine Situation, die zu einer Geschäftsunterbrechung, einem Verlust einem Notfall oder einer Krise führen könnte oder kann(vgl. [Buco06]).

*Integration inter-
ne und externe
Ursachen*

Somit ist es sinnvoll, alle extern und auch intern verursachten IT-Ereignisse, die plötzlich zu grossen Schadensereignissen eskalieren können†, in diesen Management-Prozess zu integrieren. Die Vereinigung des Vulnerability-Managements mit dem Incident-Management ist zweckmässig, da die präventiven Massnahmen zur Behebung der Vulnerabilities (z. B. Patching) meist unvorhergesehen und unverzüglich durchgeführt werden müssen.

Zu solchen Ereignissen gehören Hackings, Viren, Würmer, Trojanische Pferde sowie die plötzlich bekannt werdenden „Vulnerabilities“ und „Exploits“ in der Software, die mit entsprechenden Massnahmen (u.a. Software Patches) behoben werden sollen.

IT-Notfall

Wie die Abbildung 13.6 zeigt, werden Ereignisse, solange sie lediglich einen Einfluss auf die IT-Infrastruktur haben, als „Kritischer Zustand“ oder IT-Notfall“ bezeichnet.

* Die „NIST-Richtlinie“ „Contingency Planning Guide for Information Technology Systems“ beschränkt solchen Plan auf einen „Cyber Incident Response Plan“ [Nisc02].

† Sowohl der Standard ISO/IEC 27002:2005 [Isoc05] als auch das CobiT Framework [Cobf00] schlagen ein „Security Incident Management“ für die Behandlung sämtlicher Ereignisse und Schwachstellen vor.

Krise

Bei steigender Bedrohung oder bei erfolgten Schadenseintritten werden Ereignisse, die sich auf einzelne Geschäftsprozesse beziehen, als Krisen bezeichnet. Zur Problembehandlung bei Krisen werden die für die Geschäftsprozesse zuständigen Krisenstäbe einberufen.

Katastrophe

Sobald die Ereignisse Auswirkungen auf mehrere oder alle Geschäftsprozesse haben, werden sie als Katastrophen bezeichnet*. Zum Management einer Katastrophe wird der „Katastrophenstab“ einberufen. Zur integrierten Bewältigung aller „IT-Incidents“ über alle Eskalations-Ebenen dient der „IT-Notfall-Plan“.

Eskalations-Zustand

In diesem Plan ist auch festgelegt, bei welchem Eskalations-Zustand die Führung durch ein übergeordnetes Gremium übernommen wird.

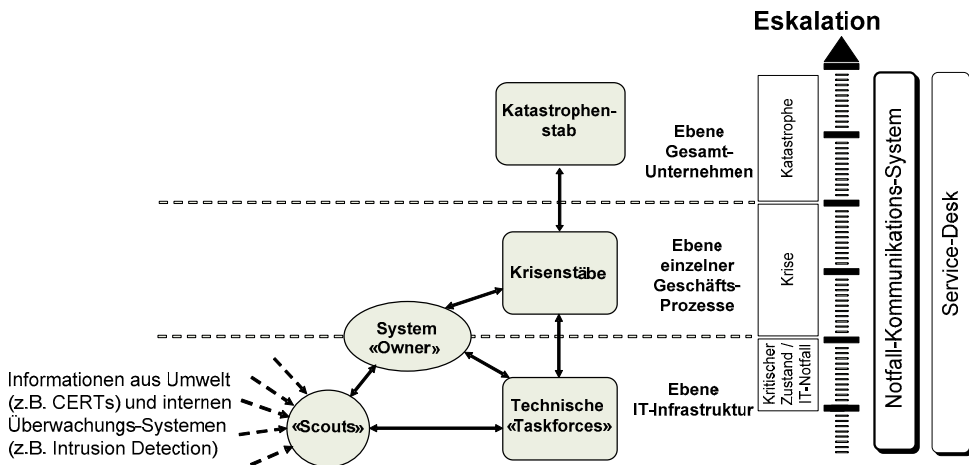


Abbildung 13.6: Eskalations-Ebenen der „IT-Notfall“-Planung

Vulnerability- und Incident Management

Die unterste Ebene des „IT-Notfall-Plans“ (s. Abbildung 13.6), die sich in erster Linie mit dem „Vulnerability- und Incident-Management“ befasst, ist die Ebene IT-Infrastruktur.

* Die Begriffe für die einzelnen Eskalationsstufen werden von Unternehmen zu Unternehmen unterschiedlich verwendet; so ist beispielsweise auch die Verwendung des Begriffs „Notfall“ für eine der „Krise“ übergeordnete Eskalationsstufe anzutreffen. Wichtig ist die einheitliche Verwendung der Begriffe in einem Unternehmen.

Management“ befasst, ist mit Aufgaben, Funktionsstellen und Kommunikations-System im Abschnitt 13.11.1 näher behandelt.

13.11.1

Organisation eines Vulnerability- und Incident-Managements*

Nachfolgend wird an einem Beispiel gezeigt, wie ein Vulnerability- und Incident- Management organisatorisch aufgebaut werden kann. Aufgrund der IT-Organisation sowie der unterschiedlichen Bedrohungsarten und deren Auswirkungen können folgende System-Bereiche unterschieden werden:

- ☐ Office-Systeme
- ☐ Netzwerk- und Midrange-Systeme
- ☐ Mainframe-Systeme
- ☐ Krypto-Systeme

Organisatorische Funktionen

Für jeden dieser System-Bereiche (Taskforces) werden Mitarbeitende mit folgenden organisatorischen Funktionen nominiert:

- ☐ Scout
- ☐ Taskforce-Mitglied und Taskforce-Leiter

Funktion „Scout“

Störungsereignisse überwachen

Die Aufgabe der Scouts besteht darin, im zugeteilten Aufgabengebiet (z.B. Windows Clients, Oracle Datenbank) die Störungsereignisse zu überwachen und die möglichen Gefahren und Schwachstellen zu erkunden, z.B. Überwachung mit den zugeteilten Monitoring-Systemen und tägliche Sichtung von Sicherheits-Informationen der CERTs*.

Problembehandlung

Relevante Informationen für mögliche Ereignisse werden durch die „Scouts“ sofort an die für die Problembehandlung zuständigen Stellen weiter geleitet (u.a. an die zuständigen Taskforce-Leiter). Im Rahmen ihrer eigenen stellenbedingten Fachaufgaben werden sie die in ihren Kompetenzbereich fallenden Problemlösungen direkt einleiten.

* In einem IT-Notfall-Plan ist die Verknüpfung des „technischen“ Vulnerability-Managements mit dem Informationssicherheits-Incident-Management eine naheliegende Lösungsvariante, um möglichst zeitnahe Aktionen zu ermöglichen. Das Informationssicherheits-Incident-Management sollte natürlich auch in geeigneter Weise mit einem Incident-Management für die „Geschäftskontinuität“ verknüpft werden.

* CERT = Computer Emergency Response Team

*Incident-
Informations-
System*

Jedes für das Unternehmen relevante Ereignis wird sofort mit einer Risiko-Einschätzung in einem „Incident-Informationssystem“ dokumentiert. In diesem System werden auch die einzelnen Problemlösungsschritte sowie Veränderungen der Situation (ggf. des Risikos) mit automatischem Zeitstempel und Bearbeiternamen nachgetragen.

*Notfall-
Kommunikations-
System und
Service Desk*

Jedes Ereignis wird auch mit einem Ticket im „Notfall-Kommunikations-System“ versehen. Ereignis-Meldungen aus dem Unternehmen werden an einem „Service Desk“ in einem „System Control Center“ rund um die Uhr entgegengenommen und bearbeitet (Pikettendienst).

Funktion „Taskforce“

*Rasche fachge-
rechte Lösung*

Die interne Taskforce ist eine aus den Scouts im betreffenden Fachgebiet zusammengestellte Gruppe von Personen. Die Taskforce nimmt sich ab einer bestimmten Risiko-Stufe der Problemsituationen an und sorgt für die rasche und fachgerechte Lösung oder initialisiert entsprechend risikomindernde Massnahmen. Eine Schlüsselrolle kommt dem ebenfalls nominierten permanenten Leiter einer Taskforce zu. Dieser Taskforce-Leiter beruft bei gegebener Risikosituation seine Taskforce ein und ist Ansprechstelle für Fragen, welche die Taskforce betreffen. Für den Taskforce-Leiter sind ständige Stellvertretungen nominiert und organisiert.

*Eskalation an
Owner und
Krisenstab*

Falls ein eingetretenes Problem droht, bestimmte Geschäftsprozesse zu beeinflussen, wird an die dafür zuständigen System- oder Prozess-Owner und Krisenstäbe eskaliert.

❑ **Office-Taskforce**

Behandelt die Bedrohungen und Schwachstellen im Office-Bereich, einschliesslich der Probleme (z.B. Malware) im Desktop- und Mobil-Computing-Bereich.

❑ **Netzwerk- und Midrange-System-Taskforce**

Behandelt die Bedrohungen und Schwachstellen hinsichtlich Systemattacken und unautorisierten Zugriffen, einschliesslich der Probleme im Firewall-, Netzwerk-, und Midrange-System-Bereich.

❑ **Mainframe-Taskforce**

Behandelt die Bedrohungen und Schwachstellen hinsichtlich Systemattacken und unautorisierten Zugriffen im Mainframe-Umfeld.

□ Krypto-Taskforce

Behandelt bereits erfolgte oder zu erwartende Kompromittierungen sowie bekannt gewordene Schwachstellen in den Kryptographie- und Key-Management-Systemen (z.B. Zertifikatschwächen, PIN-Kompromittierungen).

Service Desk*Service Desk*

Das „Service Desk“ als Kommunikationsplattform übernimmt als Anlaufstelle u.a. wichtige kommunikative Aktivitäten des Incident-Managements. Solche Aktivitäten sind die Aufnahme der Incidents von den Anwendern und das Alarmieren und Aufbieten der zur Behandlung des Ausnahme-Ereignisses prädestinierten Management- und Fachpersonen. Zur Auskunftserteilung bei Problemen, die den Betrieb/Service akut beeinflussen, steht das „Service Desk“ mit einer permanent besetzten „Hotline“ zur Verfügung. Ebenfalls übernimmt das Service Desk Aktivitäten für die Prävention im Sinne eines ständigen Verbesserungsprozesses wie die Kategorisierung und Priorisierung aller Incidents oder die Durchführung von Anwenderbefragungen.

Notfall-Informationen-System

Die rasche und zweckdienliche Kommunikation und Dokumentation in den einzelnen Problemlösungs-Phasen und Eskalations-Stufen erfolgt mittels eines dafür speziell eingerichteten Systems.

*Interdisziplinäre
Kommunikation
bei der
Problemlösung*

In einer dem systemischen Problemlösungs-Prozess angepassten Benutzerführung dient es der interdisziplinären Kommunikation über den Fortgang der Problemlösung der in den Prozess eingeschalteten Fachpersonen (Scouts, Taskforce-Leiter, Owner). Ebenfalls zeigt es ein sukzessives Reporting der Problembehandlung. Die zuständigen Führungspersonen haben ebenfalls Zugriff auf dieses System.

Tickets

Abgeleitet vom Stand der Problemlösung werden entsprechende „Tickets“ ausgefüllt und kommuniziert, aus denen eine allfällige Problembehebung oder Problemeskalation ersichtlich ist. Das Notfall-Informationen-System beinhaltet ein „Incident-Informationen-System“, das im Abschnitt 13.11.2 näher beschrieben ist.

13.11.2

Behandlung von plötzlichen Ereignissen als RM-Prozess

Wie aus dem vorangegangenen Abschnitt hervorgeht, liegt dem Vulnerability- und Incident-Management das Gerüst eines Risikomanagement-Prozesses zu Grunde.

Bei der Auslegung des oben angeführten „Incident-Information-Systems“ wurde diesem Umstand Rechnung getragen.

Initialisierung RM-Prozess

Die Initialisierung des Risiko-Management-Prozesses erfolgt aufgrund einer als relevant erkannten Störung, Attacke oder Vulnerability oder eines sich anbahnenden Schadensereignisses.

Problem- erkennung und -lösung

Die Eingabe-Maske des Incident-Information-Systems verlangt zur Problemerkennung und -lösung der Reihe nach folgende Informations-Eingaben:

- ☐ Problemerkfassung und Kontext;
- ☐ Identifikation des Risikos;
- ☐ Einschätzung des Risikos;
- ☐ Bewertung des Risikos für das Unternehmen;
- ☐ Problemlösungs-Strategie (z.B. Selbst lösen, Taskforce einberufen, oder Problem eskalieren);
- ☐ Problem bewältigen (z.B. Patch einspielen, Schaden einschränken durch Stoppen von Prozessen, Schaden beheben, Normalbetrieb herstellen);
- ☐ Problemlösung sowohl hinsichtlich zukünftiger Verbesserungen als auch zur Prävention retrospektiv aufarbeiten.

Das System ist gleichzeitig Kommunikations-Werkzeug und hinterlässt die „Spur zum Nachvollzug“ des Problemlösungs-Prozesses und der aus dem Fall gezogenen Konsequenzen.

Eskalation an übergeordneten Kontinuitäts- Management Prozess

Wird das Problem an die nächsthöhere Notfall-Instanz eskaliert, dann bedeutet dies eine Verzweigung an das Incident-Management des übergeordneten Kontinuitätsmanagement-Prozesses.

Der Unterschied zu einem planerischen Risikomanagement-Prozess (z.B. IT-Sicherheits-Konzept) besteht darin, dass im Ereignisfalle die einzelnen Schritte mit vorgefertigten Schablonen möglichst rasch durchgeführt werden müssen.

13.12**Zusammenfassung**

In vielen Unternehmen ist die Geschäftskontinuität in einem solchen Masse von den IT-Systemen abhängig, dass bei Ausfällen der IT auch die gesamten Geschäftsprozesse zum Erliegen kommen. Die Geschäftskontinuitäts-Planung setzt sich aus einer Reihe einzelner Massnahmen-Plänen zusammen. Einzelne Massnahmen-Pläne sind es vor allem deshalb, weil die Ausarbeitung, der Unterhalt sowie deren Einsatz im Notfall unterschiedlicher Expertisen und Fertigkeiten bedürfen (z.B. Geschäfts-Expertise, organisatorische und bauliche Expertise sowie IT-Expertise). Im Rahmen eines integrierten Geschäftskontinuitäts-Managements müssen die einzelnen Pläne koordiniert und aufeinander abgestimmt sein. Die Pläne müssen periodisch (z.B. jährlich) überprüft und angepasst werden. Bei signifikanten Veränderungen (z.B. Umzügen, Reorganisationen, Veränderung bei den Geschäfts- oder Supportprozessen) müssen die Pläne entsprechend der Veränderungen der Risiken und Massnahmen-Situationen überarbeitet werden.

Die Einzelpläne zur Unterstützung der Geschäftskontinuität sind:

- Geschäftskontinuitäts-Plan (Business Continuity Plan)
- Geschäftswiedererlangungs-Plan (Business Recovery Plan)
- Betriebskontinuitäts-Plan (Continuity of Operation Plan)
- Ausweich-Plan (Disaster Recovery Plan)
- IT-Notfall-Plan (IT Contingency Plan)
- Vulnerability- und Incident Response Plan

Die Geschäftskontinuitäts-Planung ist ein Sub-Prozess des integrierten Unternehmens-Risikomanagement-Prozesses und wird in der Struktur eines Risikomanagement-Prozess entwickelt und dokumentiert. Die Haupt-Schritte bei der Geschäftskontinuitäts-Planung sind:

- 1) Planung Kontinuitäts-System
- 2) BIA und Risiko-Assessment
- 3) Kontinuitäts-Strategien
- 4) Kontinuitätsverfahren und Pläne
- 5) Tests, Übungen und Wartung der Pläne
- 6) Ständige Überwachung und Überprüfung
- 7) Kontinuierliche Verbesserungen und Wiederholungen

Der „**IT-Notfall-Plan**“ ist stark mit dem Geschäftskontinuitäts-Plan verknüpft. Er enthält neben den Massnahmen zur Wiederherstellung der IT-Support-Funktionen auch die allenfalls notwendigen IT-Support-Massnahmen zur Aufrechterhaltung der Geschäftsprozesse während einer Störung oder einem Ausfall.

Bei dem in den IT-Notfall-Plan integrierten „**Vulnerability- und Incident-Plan**“ geht es zum einen um die meist sofort notwendige Prävention gegenüber bösartigen Attacken, die zum grossen Teil über das Internet eingeschleust werden. Zum anderen kümmert sich das Incident Management bei jedwelchen Störungen um die schnellstmögliche Wiederherstellung des normalen Dienstleistungsbetriebs unter minimaler Beeinflussung des Geschäftsbetriebs.

Die auf der Ebene der IT-Infrastruktur behebbaren Ereignisse werden als „Kritische Zustände“ oder „IT-Notfälle“ bezeichnet. Diejenigen Ereignisse, die sich auf einzelne Geschäftsprozesse beziehen, werden als „Krisen“ und die Ereignisse, die sich auf mehrere oder alle Geschäftsprozesse beziehen, als „Katastrophen“ behandelt. Im IT-Notfall-Plan ist festgelegt, bei welchem Eskalations-Zustand die Führung an ein übergeordnetes Gremium abgegeben wird.

In einem Beispiel, wie das „Vulnerability- und Incident-Management“ im IT-Notfall-Plan aufgebaut werden kann, kommen auf der untersten Stufe, wo es neben dem Incident Management auch um die Prävention von negativen IT-Ereignissen geht, sogenannte „Scouts“ zum Einsatz.

Die Aufgabe der Scouts besteht darin, im zugeteilten Aufgabengebiet (z.B. Windows Clients, Oracle Datenbank) die Störungsergebnisse zu überwachen und die möglichen Gefahren und Schwachstellen zu erkunden, z.B. durch die Überwachung mit den zugeteilten Monitoring-Systemen und die tägliche Sichtung von Sicherheits-Informationen der CERTs.

Eine interne **Taskforce** nimmt sich ab einer bestimmten Risiko-Stufe (Eskalationsstufe) der Problemsituationen an und sorgt für die rasche und fachgerechte Lösung oder initialisiert entsprechend risikomindernde Massnahmen. Die Taskforce setzt sich aus den Scouts im betreffenden Fachgebiet zusammen.

Die rasche und zweckdienliche Kommunikation und Dokumentation während den einzelnen Problemlösungs-Phasen und Eskalations-Stufen erfolgt mittels eines „**Notfall-Information-Systems**“ und einem integrierten speziellen „**Incident-**

Informations-System“. Der Prozess, bei der Behandlung eines Incidents oder einer Vulnerability, wird vorteilhaft als Problemlösungsprozess gemäss dem Muster eines Risikomanagement-Prozesses aufgebaut.

13.13

Kontrollfragen und Aufgaben

1. Erklären Sie den Zweck des Geschäftskontinuitäts-Plans.
2. Erklären Sie den Zweck des Geschäfts-Wiedererlangungs-Plans und seine Abgrenzung zum Geschäftskontinuitäts-Plan?
3. Was sind die Unterschiede zwischen dem Ausweich-Plan und dem IT-Notfall-Plan?
4. Nennen Sie 5 Aktivitäten, mit denen das Top-Management eines Unternehmens sein Commitment zu einem BCMS unter Beweis stellen kann.
5. Nennen Sie 5 Aktivitäten bei der Geschäfts-Impact-Analyse.
6. Nennen Sie 5 Aktivitäten beim Risikomanagement im Geschäftskontinuitäts-Prozess.
7. Nennen Sie 5 Aktivitäten für das Kommunikationskonzept im Geschäftskontinuitäts-Prozess.
8. Was wird beim Testen der Geschäftskontinuitäts-Planungen vor allem überprüft?
9. Nehmen Sie eine Unterscheidung und Charakterisierung der verschiedenen Arten und Möglichkeiten von Tests und Übungen im Rahmen eines BCM-Systems vor, wie sie für ein Unternehmen mittlerer Grösse mit hoher IT-Abhängigkeit und integriertem IT-Notfall-Plan in Frage kommen könnten.
10. Welchen Zweck hat das Üben der Geschäftskontinuitäts-Planungen und Aktivitäten?
11. Welche Situationen deckt der im Beispiel gezeigte „Vulnerability- und Incident-Management-Plan“ ab?
12. Erläutern Sie die Funktionen Scout und Taskforce im beispielhaft gezeigten Ansatz eines „Vulnerability- und Incident-Management-Systems“.
13. Welche Aufgaben und Aktivitäten können Sie aus der Sicht eines IT-Notfall-Plans dem „Service Desk“ zuordnen?

Risikomanagement im Lifecycle von Informationen und Systemen

Die mit der Informationssicherheit und IT-RM-Prozessen zu schützenden Güter sind die Informationen und ihre technologischen Gefässe, namentlich die IT-Systeme. Zu diesen Gefässen zählen wir die Codierungen der Informationen und Prozeduren (z.B. Programme) sowie die IT-Prozesse, die Hardware und die technischen Kommunikations-Einrichtungen.

Die Informationen und die IT-Systeme sind während ihres gesamten Lebenszyklus zu schützen.

14.1

Schutz von Informationen im Lifecycle

Schutzphasen

Der Lifecycle der Informationen kann grob in die Schutz-Phasen

- Entstehung,
- Bearbeitung,
- Übertragung (Übermittlung),
- Speicherung (Archivierung) und
- Entsorgung (Löschung)

unterteilt werden.

Einer jeden dieser Phasen liegt ein bestimmter Zweck und ein bestimmter Schutzbedarf zugrunde. Der Schutzbedarf ergibt sich aus der Art und der Sensibilität der Informationen aufgrund einer bezüglich „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ durchgeführten Risiko-Einschätzung.

14.1.1

Einstufung der Informations-Risiken

Informations-Klassierung

Für einen praktikablen Umgang mit Informationen wird eine Impact-Einschätzung anhand einiger Kriterien oft pragmatisch in nur wenigen Impact-Stufen vorgenommen. Dieser Impact-Einschätzungsprozess wird meist als „Informations-Klassierung“ bezeichnet.

*Intern,
Vertraulich und
streng Vertraulich*

Als Impact-Stufen für schützenswerte (unternehmensinterne) Informationen werden für das System-Ziel „Vertraulichkeit“ oft die drei Stufen „INTERN“, „VERTRAULICH“ und „STRENG VERTRAULICH“ eingesetzt. Für eine solche Informations-Einstufung ist es nicht praktikabel, bereits die Wahrscheinlichkeit eines möglichen Schadens in die Einstufung einzubeziehen, da das Bedrohungs-Umfeld zum Zeitpunkt der Informations-Einstufung noch gar nicht bekannt ist.

*Worst-Case-
Kriterien*

Die Einstufung erfolgt somit nach „Worst-Case-Kriterien“ oder allenfalls nach äusseren Anforderungen (gesetzlich, regulativ oder vertraglich).

Im Anhang dieses Buches (Tabelle A.3.1) ist anhand eines Beispiels gezeigt, wie die Einstufungskriterien in einem Unternehmen für die System-Ziele „Vertraulichkeit“ und „Integrität“ zusammengestellt werden können.

14.1.2

Massnahmen für die einzelnen Schutzphasen

*Pro Schutzphase
und Einstufung
spezifische Mass-
nahme*

Für jede der oben genannten Schutz-Phasen können auch typische Bedrohungen definiert werden. Anhand dieser Bedrohungen können pro Schutzphase für jede Einstufung spezifische Massnahmen im Sinne von Sicherheits-Mechanismen zugeordnet werden.

Beispiel:

Während der Schutzphase „Übertragung (Übermittlung)“ besteht die Bedrohung „Abhören von Informationen“.

Haben die Informationen die Einstufung „vertraulich“, dann lautet die spezifische Massnahme „Übertragungs-Chiffrierung“. Im Anhang (Tabellen A.3.3 und A.3.4) sind solche Massnahmen, bezogen auf die Schutz-Phase und die Einstufung der Information, zusammengestellt.

*Informationen
risikogerecht
schützen*

Der pragmatische Ansatz der Informations-Einstufung und der Zuordnung von Massnahmen erlaubt, dass jeder Mitarbeitende seine Informationen selbst einstufen und mit dem als Policy ausgearbeiteten „Massnahmen-Rezept“ risikogerecht schützen kann (die Massnahmen sind ggf. im Arbeitsplatz-Computer bereits als „Werkzeuge“ verfügbar). Das Beispiel eines solchen Massnahmen-Rezepts ist im Anhang (Tabellen A.3.3 und A.3.4) gezeigt.

14.2

Risikomanagement im Lifecycle von IT-Systemen

Die IT-Systeme eines Unternehmens durchlaufen in groben Phasen den folgenden für die Sicherheit relevanten Lebenszyklus:

Lebenszyklus-Phasen

- 1) Anforderungs-Analyse
- 2) Anforderungsdefinition und Entwurf
- 3) Entwicklung oder Beschaffung
- 4) Integration und Test
- 5) Einführung und Ausbreitung
- 6) Systembetrieb
- 7) Systemoptimierung
- 8) Systemabbau, -archivierung und Entsorgung

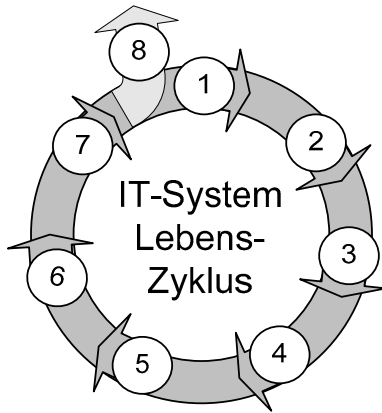
Je nachdem, ob das System entwickelt oder extern beschafft wird, ergeben sich Unterschiede in der feineren Unterteilung der Schritte.

Es gibt eine Anzahl von Lifecycle-Modellen mit entsprechend feinen Phasen-Unterteilungen, die meist primär für die Software-Entwicklung zugeschnitten sind. Beispiele dafür sind das für deutsche Bundes-IT-Projekte gebräuchliche „V-Modell“ oder das bei Schweizer Bundesstellen gebräuchliche „Hermes“ zu erwähnen.

ITIL-Applikations-Management-Prozess

In Ergänzung zum ITIL-Servicemanagement-Prozess ist gemäss dem Applikations-Lebenszyklus auch ein ITIL*-Applikations-Management-Prozess formuliert (s. Abbildung 14.1).

* ITIL=IT Infrastructure Library: hersteller-unabhängiges Regelwerk der zentralen Informationsberatungsstelle der britischen Regierung früher CCTA = Central Computer and Telecommunications Agency, jetzt OGC = Office of Government Commerce.



System-Lebenszyklus-Phasen		ITIL Application Management Lifecycle
1)	Anforderungs-Analyse	Requirements
2)	Anforderungsdefinition und Entwurf	Design
3)	Entwicklung oder Beschaffung	Build
4)	Integration und Test	
5)	Einführung und Ausbreitung	Deploy
6)	Systembetrieb	Operate
7)	Systemoptimierung	Optimise
8)	Systemabbau, - Archivierung und Entsorgung	

Abbildung 14.1: Für Risiken wichtige IT-System Lebenszyklus-Phasen

*Durchgängiges
IT-Risiko-
management*

Der Vorteil dieses Ansatzes ist, dass die Prozesse vom Geschäftsbedarf über die Entwicklung bis hin zur betrieblichen Lieferung der IT-Dienstleistung durchgängig definiert sind (s. Abbildung 14.2). Ein solcher Ansatz ist auch für ein durchgängiges IT-Risikomanagement hilfreich.

		ITIL Service Lifecycle				
		Service Strategy	Service Design	Service Transition	Service Operation	Continual Service Improvement
Application Management Lifecycle	Requirements	x	x			
	Design		x			
	Build			x		
	Deploy			x		
	Operate		x	x	x	
	Optimise		x			x

X: Abstimmungsaktivitäten zwischen den Lebenszyklen

Abbildung 14.2: ITIL Lebenszyklen (vgl. [Itss08], S. 5)

14.3

Synchronisation RM mit System-Lifecycle

Einbringen der Sicherheitsanforderungen

Das Einbringen der Sicherheitsanforderungen in die IT-Systeme ist bereits bei der Strategiefindung sowie in einem konkreten Entwicklungs-Projekt in den Phasen Anforderungs-Analyse und „Entwicklung oder Beschaffung“ sehr wichtig. Zu spät erkannte Anforderungen können oft nicht mehr eingebracht werden oder führen zu Unverträglichkeiten und zu unpraktischen und teuren Lösungen.

Die Sicherheitsanforderungen resultieren vor allem aus den Geschäftsanforderungen und dem technischen und organisatorischen Umfeld (Kontext) eines Systems, in welchem es später betrieben werden soll.

IT-RM-Prozess im Projektvorgehen

Im Folgenden wird ein pragmatischer Ansatz eines IT-Risikomanagement-Prozesses gezeigt, der mit der Projekt-Vorgehens-Methode synchronisiert ist:

1. Abnahme nach der „Anforderungs-Analyse“

First Cut

Bereits nach der „Anforderungs-Analyse“ wird eine grobe Risiko-Analyse über das neue System in seinem Umfeld erstellt. Diese als „First Cut“ bezeichnete Risiko-Analyse liefert Anhaltspunkte darüber, ob höhere Risiken vorhanden oder ob die Risiken weitgehend durch bestehende Grundschutzmassnahmen abgedeckt sind. Bestehen grössere Risiken, dann wird bereits zu diesem Zeitpunkt eine detaillierte Risiko-Analyse vorgenommen, die als Input für die nachfolgende Phase „Anforderungsdefinitionen und Entwurf“ dient.

Das ausgefüllte Formular (s. Anhang A.4), mit dem das Ergebnis des „First Cut“ dokumentiert wird, wird vom zuständigen „Owner“ des Systems und weiteren für das Projekt verantwortlichen Personen (z.B. Projektleiter) unterzeichnet. Das unterzeichnete „First Cut“-Dokument gehört zu den Abnahme-Lieferobjekten der Phase „Anforderungs-Analyse“. Zur Durchführung der „First Cut“-Risiko-Analyse befinden sich entsprechende Formulare im Anhang (Tabellen A.4.1, A.4.2 und A.4.3).

2. Abnahme vor der „Entwicklung oder Beschaffung“

Grobes Sicherheitskonzept

Vor der Phase „Entwicklung oder Beschaffung“ wird in der Regel der Beschluss zur Realisierung gefasst, der auf den in der vorangegangenen Phase „Anforderungsdefinition und Entwurf“ ermittelten Systemkosten basiert. Wird das System beschafft, dann werden zu diesem Zeitpunkt die Verträge unterzeichnet.

Zu diesem Zeitpunkt ist es wichtig, die Sicherheits-Massnahmen sowie deren Kosten und Realisierbarkeit zu kennen. Zur Abnahme der Phase „Anforderungsdefinitionen und Entwurf“ wird demzufolge u.a. ein grob mit allen sechs Kapiteln ausgearbeitetes Sicherheitskonzept als Lieferobjekt vorgelegt (s. Abschnitt 10.1). Die Risiko-Analyse muss dafür bereits die grössten IT-Sicherheits-Risiken enthalten.

3. Abnahme vor der „Einführung und Ausbreitung“

*Detailliertes
Sicherheitskonzept*

Vor der Phase „Einführung und Ausbreitung“ wird das definitive, im Detail ausgearbeitete Sicherheitskonzept als Lieferobjekt zur Abnahme vorgelegt. Das Sicherheitskonzept dokumentiert zu diesem Zeitpunkt die Risiken, Massnahmen, Restrisiken und Umsetzungs-Aktivitäten für den späteren einwandfreien Systembetrieb.

*Abnahmehürde
vor Inbetrieb-
nahme*

Systeme, bei denen ein solches Dokument nicht abgenommen ist oder bei denen das Dokument nicht der Realität entspricht, dürfen nicht in Betrieb genommen werden. Bei sicherheitskritischen Systemen ist eine solche letzte Abnahmehürde unerlässlich. Die Praxis lehrt auch, dass Sicherheitskonzepte, welche keine solche Abnahmehürde bestehen müssen, selten ordnungsgemäss fertiggestellt werden. Abbildung 14.3 veranschaulicht die geschilderten Abnahmezeitpunkte im Rahmen des Projekt-Vorgehens.

1)	Anforderungs-Analyse
	↙ Abnahme „First Cut“
2)	Anforderungsdefinition und Entwurf
	↙ Abnahme Sicherheitskonzept „Grobfassung“
3)	Entwicklung oder Beschaffung
4)	Integration und Test
	↙ Abnahme Sicherheitskonzept „Betriebsfassung“
5)	Einführung und Ausbreitung
6)	Systembetrieb
7)	Systemoptimierung
8)	Systemabbau – Archivierung und Entsorgung

Abbildung 14.3: Abnahme-Zeitpunkte von Sicherheits-Dokumentationen

*Entwicklungs-
Vorgehens-
Modelle*

Ein solches Vorgehen kann bei den meisten Entwicklungs-Vorgehens-Modellen eingeschlagen werden. Selbstverständlich erfolgt die Erarbeitung der Risiko- und Massnahmen-Beschreibungen innerhalb der feinen Verästelungen der Sub-Prozesse eines Vorgehens-Modells, wie es an Ausschnitten des V-Modells ersichtlich ist (s. Abbildung 14.4).

*Signifikante
Veränderungen*

In der Phase „System-Optimierung“ erfordern allenfalls auftretende „signifikante“ Veränderungen der Risikolage ein „Nachziehen“ des Sicherheitskonzepts mit einer entsprechenden Risiko-Analyse und mit entsprechenden Sicherheits-Massnahmen.

Es empfiehlt sich, die „System-Optimierungen“ wie den „System-Abbau“ projektmässig abzuwickeln, womit die Ordnungsmässigkeit auch dieser Lebenszyklus-Phasen sichergestellt werden kann.

Praxistipp:

Sicherheitsdokumentationen und Sicherheitskonzepte sollten womöglich projektbegleitend durch aktiv im Projekt mitwirkende Personen erstellt werden. Das sicherheitsspezifische know-how kann in Form von „Coaching“ durch einen Sicherheits-Experten eingebracht werden.

14.4**Zusammenfassung**

Die Informationen wie ihre technologischen Gefässe (Informationen, Prozeduren, Hardware usw.) sind während ihres ganzen Lebenszyklus schutzbedürftig. Für die Informationen können die Schutzphasen „Entstehung“, „Bearbeitung“, „Übertragung (Übermittlung)“, „Speicherung (Archivierung)“ und „Entsorgung (Löschung)“ unterschieden werden. Ein pragmatischer Ansatz, die Information durch jeden Mitarbeitenden risikogerecht zu schützen, besteht darin, die Einstufungskriterien in Form einer kurzen Anleitung den Mitarbeitenden in die Hand zu geben. Die Einstufungskriterien leiten sich von gesetzlichen, regulativen, vertraglichen Anforderungen oder aufgrund von „Impacts“ ab.

Sind die Informationen eingestuft, dann können pro Schutzphase und Informationseinstufung mit einem „Massnahmen-Rezept“ die angemessenen „Werkzeuge“ (z.B. Chiffrier-Programm) direkt am Arbeitsplatz-Computer eingesetzt werden.

Das Risikomanagement der IT-Systeme kann mit folgendem Vorgehen sichergestellt werden:

- ☐ „First Cut“- Risiko-Analyse vor der Phase „Anforderungsdefinition und Entwurf“
- ☐ Sicherheitskonzept in Grobfassung vor dem Entscheid für die System-Entwicklung oder die -Beschaffung und
- ☐ Sicherheitskonzept in der detaillierten Betriebsfassung vor der Systemeinführung und der -Ausbreitung.

Auch die Phasen der Systemoptimierung oder des Systemabbaus bedürfen einer entsprechenden Begleitung mit Sicherheitskonzepten.

14.5

Kontrollfragen und Aufgaben

1. Welches sind die Schutzphasen der Informationen, während denen sie generell unterschiedlichen Bedrohungen unterliegen?
2. Aufgrund welcher generellen Kriterien können die Informationen eingestuft (klassiert) werden?
3. Mit welcher Massnahme (Werkzeug) schützen Sie vertrauliche Informationen bei der elektronischen Übertragung (Übermittlung) gegen unberechtigte Kenntnisnahme?
4. Nennen Sie drei Lieferobjekte, die im Projektablauf abgenommen sein müssen, bevor jeweils die nächste Projektphase begonnen werden darf. Wie heissen die entsprechenden Projektphasen?
5. Wie sollten im Verlauf eines Projektes die Sicherheitsdokumente erstellt werden:
 - 1) zum jeweiligen Abschluss einer Phase?
 - 2) projektbegleitend?
 - 3) durch einen ausserhalb des Projektes eingesetzten Sicherheits-Experten?
 - 4) durch aktiv im Projekt mitwirkende Personen?
 - 5) wie kann ein allenfalls fehlendes Sicherheits-„know how“ eingebracht werden?
6. Ein Unternehmen bietet die sichere Verwahrung von Wertpapieren und Wertgegenständen an. Zur Rationalisierung dieser Dienstleistung plant das Unternehmen ein neues IT-System für die Steuerung und Verwaltung eines Hochregallagers. Das gestartete Projekt für die Entwicklung und Inbetriebnahme dieses IT-Systems wird in Anlehnung an das **V-Modell** abgewickelt. Im Rahmen der Projektabwicklung wird

Ihnen die Rolle des IT-Sicherheitsbeauftragten zugeteilt. In dieser Rolle sind Sie in das Projekt eingebunden, und es fällt Ihnen die Erstellung verschiedener Lieferobjekte zu. Eine Ihrer Aufgaben ist die Erstellung einer „First Cut“-Analyse und eines IT-Sicherheitskonzepts. Das Sicherheitskonzept muss während des Projektablaufs zweimal abgenommen und genehmigt werden und zwar zu einem ersten Vorlagetermin in einer groben Fassung und zu einem zweiten Vorlagetermin in seiner detaillierten Fassung. Sie wissen, dass verschiedene System-Lifecycle-Modelle meist aufeinander abgebildet werden können. Das V-Modell kennt die vier Submodelle:

Systemerstellung

Projektmanagement

Konfigurations-Management

Qualitätssicherung

- a) Zeichnen Sie in der nachfolgenden Abbildung 14.4 der „Aktivitäten“ im Sub-Modell „Systemerstellung“ die Vorlagetermine für die „First Cut“-Dokumentation und für das IT-Sicherheitskonzept ein.

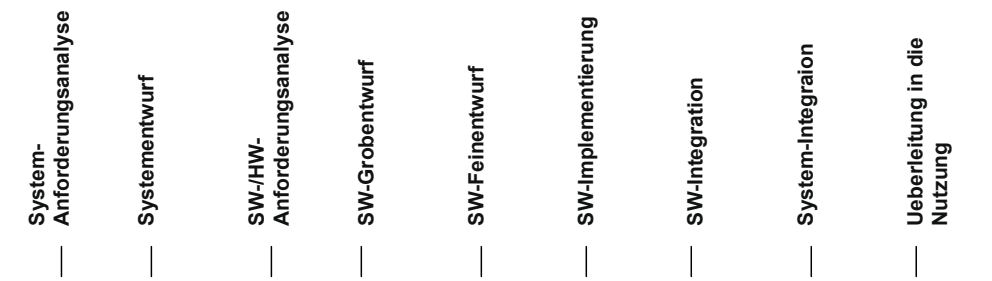


Abbildung 14.4: Aktivitäten im Sub-Modell „Systemerstellung“ des V-Modells

- b) In welchem Kapitel Ihres Sicherheitskonzepts führen Sie die Anforderungen aus dem Datenschutzgesetz auf?

Argumente für Outsourcing

Viele Unternehmen prüfen die Möglichkeiten, einige ihrer aufwändigen Prozesse zu „outsourcen“.

Die Argumente für ein Outsourcing, insbesondere der IT-Prozesse, sind (vgl. [Buch04], S. 185 ff):

- ☐ Komplexitätsreduktion durch Outsourcen von IT-Prozessen, welche die Kernkompetenzen nicht direkt unterstützen;
- ☐ Konsolidierung von historisch gewachsenen IT-Landschaften im Unternehmen;
- ☐ Variabilisierung der Fixkosten durch Ausnützung der Synergien des Outsourcers mit anderen Kunden und dadurch Möglichkeit eines mengenabhängigen Pricings;
- ☐ Verbesserung der Zuverlässigkeit und Innovation durch „kritische Masse“ des Outsourcers für neue technologische Trends und für Massnahmen zur Einhaltung aktueller Sicherheitsstandards;
- ☐ Reduktion von Mitarbeitern und Erzielen von Cash-Effekten und Umlage von Anlagevermögen in Umlaufvermögen.

Kostenerhöhung in Übergangsphase

Die typische Ergebniskurve von IT-Outsourcing zeigt eine Kostenerhöhung für die Übergangsphase durch

- ☐ Aufbau eines „Demand Managements“ (z.B. durch Aufbau notwendiger Ansprechpartner auf der Auftraggeber-Seite);
- ☐ Transferkosten für Eingliederung von IT-Technik und IT-Personal beim IT-Outsourcer;
- ☐ Sichtbarmachung versteckter IT-Kosten, die zuvor erbracht, aber nicht abgerechnet wurden.

Nach einer Übergangsphase von ca. 4 Jahren sollten Kosteneinsparungen von > 20 % möglich sein.

Risiko-Kosten

Einige der auf den ersten Blick einzusparenden Kosten werden durch neue Kosten bezüglich nachträglicher Erfüllung der IT-Sicherheits-Anforderungen und der neuen „Risiko-Kosten“ neu-tralisiert.

Nach sorgfältiger Untersuchung kann es für einige IT-Bereiche und auch Geschäftsprozesse durchaus sinnvoll und wirtschaftlich sein, ein Outsourcing einzugehen.

IT-RM-Prozess

In jedem Falle muss dem Outsourcing von Prozessen mit Informationsabhängigkeiten ein gründlicher IT-Risikomanagement-Prozess zu Grunde gelegt werden.

Praxistipp:

Für beide Outsourcing-Partner gilt von Anfang an zu bedenken, dass die Sicherheitsmassnahmen vorab vereinbart werden müssen und einen Preis haben.

15.1

IT-Risikomanagement im Outsourcing-Vertrag

Rundschreiben der FINMA

Für nach schweizerischem Recht organisierte Banken und Effekthändler sowie für schweizerische Zweigniederlassungen ausländischer Banken und Effekthändler besteht eine Auflage der FINMA* in Form eines Rundschreibens (mit letzter Änderung ab 1. Januar 2008).

Sicherheitsanforderungen vertraglich festlegen und überwachen

Darin wird unter anderem verlangt, dass das auslagernde Unternehmen und der Dienstleister die Sicherheitsanforderung vertraglich festhalten müssen und dass das auslagernde Unternehmen diese überwachen muss.

Sicherheitsdispositiv

Weiter müssen das auslagernde Unternehmen und der Dienstleister ein Sicherheitsdispositiv ausarbeiten, dass die Weiterführung des ausgelagerten Geschäftsbereichs erlaubt, falls der Dienstleister aus irgendwelchen Gründen verhindert ist, seine Leistung zu erbringen. Das Sicherheitsdispositiv hat sämtliche Notfälle abzudecken. Die ordnungsgemässe Geschäftsführung muss jederzeit aufrechterhalten werden können.

Schutz der Kundeninformationen

Unter anderem müssen Kunden-Informationen durch angemessene technische- und organisatorische Massnahmen gegen unbefugte Einsichtnahme und Bearbeitung geschützt werden.

* Durch Eidgenössischen Bankenkommission (EBK) am 26. Oktober 1999 herausgegebenes Rundschreiben für das seit 1.1.2009 die „FINMA“ (Eidgenössische Finanzmarktaufsicht) zuständig ist.

<i>Auslagerungen ins Ausland</i>	Weiter besteht der Grundsatz, dass Auslagerungen ins Ausland vom ausdrücklichen Nachweis der Prüfmöglichkeiten* abhängig gemacht sind.
<i>Gartner Group</i>	Für das häufig erwogene „Offshore Outsourcing“ wird von der Gartner Group† äusserste Vorsicht angeraten: "Service providers are unable to provide standard security solutions because regulations, legislation and consequently risk vary vastly between industries and geographies."
<i>„Due Diligence“</i>	Gemäss Gartner sollte das Unternehmen die Sicherheit früh adressieren und „Due Diligence“ während dem gesamten „Life-cycle“ der Auslagerung durchführen.
<i>Sicherheitskosten im „Off-shore Exposure“</i>	Gartner macht darauf aufmerksam, dass erhebliche Sicherheitskosten anfallen und es nicht kosteneffektiv sei, für jeden Aspekt dasselbe Sicherheits-Niveau im „Offshore Exposure“ bereitzustellen. Deshalb sollten die Unternehmen wissen, welche Aufzeichnungen und Informationen geschützt werden müssen und warum und wie viel sie für die Sicherheit bezahlen wollen. Die Gartner-Empfehlung kann wie folgt zusammengefasst werden:
<i>Gartner-Empfehlung</i>	Die Sicherheitsanliegen müssen möglichst früh in der Sourcing-Strategie und bei der Entwicklung des Vorhabens angegangen werden. Es muss ein detaillierter Dialog mit dem Dienstleister erfolgen, um den Lösungsansatz des Dienstleisters bezüglich Sicherheit zu verstehen. Dabei ist wichtig, die wesentlichen Aspekte des Sicherheits-Managements und der -Kontrolle sowie einige Audit-Mechanismen im eigenen Hause zu behalten. Zusammen mit dem Dienstleister müssen in einem „Framework“ sämtliche Sicherheitsanliegen identifiziert und behandelt werden. Dabei muss die Gültigkeit der Risiken vereinbart und die Höhe der Kosten zur Reduktion der Risiken in die Entscheide einbezogen werden.

* Prüfmöglichkeiten durch das Unternehmen als auch durch seine banken- und börsengesetzliche Revisionsstelle sowie die Bankenkommision

† Partha Iyengar, Research Vice President, Gartner Indien: Gartner says Security becomes Key Concern in Global Sourcing. Gartner Press Release Egham, UK, September 21, 2004

15.1.1

Sicherheitskonzept im Sourcing-Lifecycle

Ein Instrument, um die Risiken, Sicherheitsanforderungen und Massnahmen zugrunde legen zu können, ist das in Abschnitt 10.1 gezeigte Sicherheitskonzept. Sowohl am Beispiel der Forderungen der FINMA als auch gemäss der Empfehlungen der Gartner Group erlaubt ein rechtzeitig und durch die Partner gemeinsam erarbeitetes Sicherheitskonzept, die Sicherheitsuntersuchungen und -Abwägungen schrittweise aufzubauen und gegenseitig abzustimmen.

*Sicherheitskonzept
im Sourcing-
Vertrag*

Das Sicherheitskonzept sollte in seiner abgestimmten Fassung zum integrierenden Bestandteil des Sourcing-Vertrages gemacht werden. Im Lifecycle des Sourcing-Vorhabens (s. Abbildung 15.1) wird eine erste verbindliche Fassung zum Zeitpunkt der Vertragsunterzeichnung fertig gestellt sein.

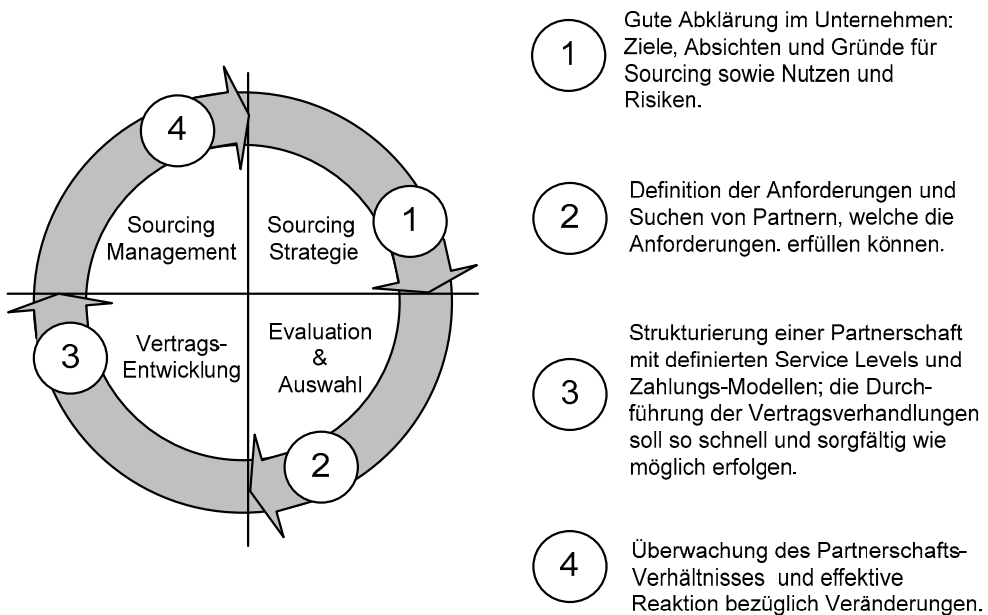


Abbildung 15.1: „Sourcing Lifecycle“ gemäss Gartner*

* www4.gartner.com

Das Sicherheits-Konzept (s. Abbildung 15.2) wird wie folgt erstellt:

Phase 1: Outsourcing-Strategie

Sicherheitskonzept für bestehenden Prozess

Bereits während der Phase der Outsourcing-Strategie wird ein Sicherheitskonzept über den auszulagernden Prozess erstellt. Das Konzept dient der Analyse und Dokumentation des bestehenden Prozesses (ein allenfalls bereits vorhandenes Sicherheitskonzept wird auf seine Aktualität und Zweckmässigkeit hin untersucht).

Risiken, Anforderungen und bestehende Massnahmen

Das Sicherheitskonzept soll Risiken, Anforderungen, bestehende Massnahmen und Anhaltspunkte über die aktuellen Massnahmen-Kosten aufzeigen. Die Erstellung des letzten Kapitels über Massnahmen-Umsetzung kann in dieser frühen Phase entfallen.

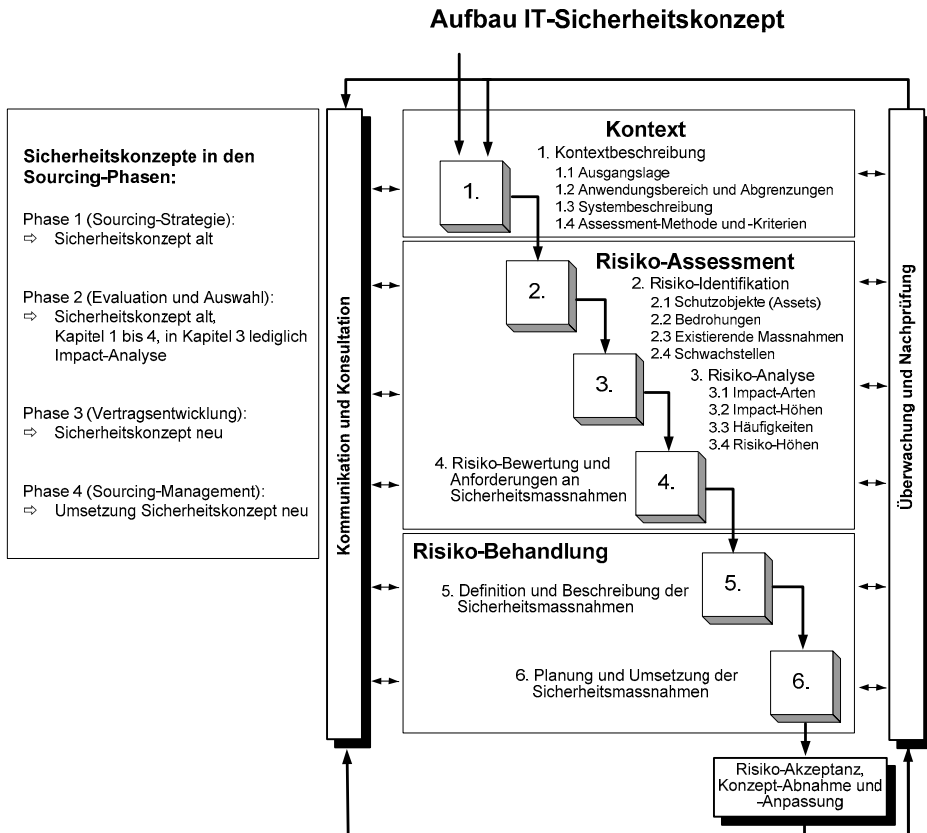


Abbildung 15.2: IT-Sicherheitskonzept in den Sourcing-Phasen

Phase 2: Evaluation und Auswahl

Teile des Sicherheitskonzepts in „Request for Proposal“

In der Phase der Suche eines geeigneten Dienstleisters sollen die für diese Phase wichtigen Teile aus Kapitel 1 bis 4 des Sicherheitskonzepts in den „Request for Proposal“ (RFP) aufgenommen werden:

- ☐ Kapitel 1: Kontext, einschliesslich System- respektive Prozessbeschreibung
- ☐ Kapitel 2: Risiko-Identifikation
- ☐ Kapitel 3: Nicht die volle Risiko-Analyse, sondern lediglich die Impact-Analyse
- ☐ Kapitel 4: Anforderungen an die Sicherheits-Massnahmen

Die aus der Sicht des auslagernden Unternehmens erstellte volle Risiko-Analyse (Kapitel 3) ist für den RFP nicht relevant und wird deshalb nicht herausgegeben.

Phase 3: Vertragsentwicklung

Neues Umfeld im Sicherheitskonzept

In dieser Phase werden mit dem Dienstleister zusammen alle Kapitel 1 bis 6 des Sicherheitskonzepts unter Berücksichtigung des neuen Umfelds gemeinsam überarbeitet.

Bei der Risiko-Analyse steuert das auslagernde Unternehmen vor allem die Impact-Analyse, der Dienstleister hingegen vor allem die Analyse der Bedrohungen und Schwachstellen zur Risiko-Analyse bei.

Gemeinsame Risiko-Bewertung

Nach gemeinsamer Risiko-Bewertung werden die neuen Anforderungen an die Sicherheitsmassnahmen gemeinsam definiert. Grosse Aufmerksamkeit und Sorgfalt ist auch bei der Massnahmen-Beschreibung (Kapitel 5), beim Umsetzungs-Plan (Kapitel 6) sowie der anschliessenden Rest-Risiko-Betrachtung notwendig.

Im Kapitel 6 über die Umsetzung der Sicherheitsmassnahmen sind die Bedingungen zur späteren Überarbeitung des Sicherheitskonzepts aufzunehmen. Solche Bedingungen sind beispielsweise signifikante Veränderungen des Auslagerungs-Gegenstands und der Risiko-Lage. Die Überarbeitung kann auch auf Grund einer Überprüfung (Revision) durch den Auftraggeber notwendig sein. Das Vorgehen und die Periodizität von solchen Überprüfungen (z.B. jährlicher Review) gehört auch im Umsetzungsplan beschrieben. Ein solches gemeinsam erarbeitetes Sicherheitskonzept kann nur dann seinen Zweck erfüllen, wenn es als integrierender Bestandteil des Vertrags deklariert wird.

Phase 4: Sourcing-Management

Während dieser Betriebsphase können alle Überwachungen und Weisungs-Möglichkeiten ausgeschöpft werden, die im Vertrag und dem Sicherheitskonzept vereinbart wurden. Kontrollmöglichkeiten durch den Chief Information Security Officer sowie interne oder externe Revisions-Stellen sind nützlich und aufgrund regulativer Auflagen (z.B. FINMA, Sarbanes-Oxley Act) sogar unumgänglich.

Koordination und Überwachung auf Auftraggeber-Seite Auf der Auftraggeber-Seite sollte wenigstens eine Person für die Koordination und Überwachung mit entsprechendem Einsichtsrecht definiert und eingerichtet sein. Auch eine zusätzliche Person eines unabhängigen Beratungs-Unternehmens mit einschlägigen Erfahrungen mit Einblick in die Geschehnisse ist zu empfehlen.

15.1.2

Sicherheitskonzept beim Dienstleister

Der Ablauf bezüglich Festlegung der Sicherheitsanforderungen auf der Seite des Dienstleisters wird weitgehend durch den Auftraggeber bestimmt. Doch hat der Dienstleister zum einen eigene Sicherheits-Interessen bezüglich seiner IT-Umgebung und zum anderen das Interesse, die Massnahmen kostengünstig zu gestalten.

Niedrige Kosten Niedrige Kosten steigern die Konkurrenzfähigkeit. Strebt der Dienstleister eine dem Dienstleistungs-Objekt nicht angemessene zu niedere Sicherheit an, kann dies seinem Ruf und damit seiner Konkurrenzfähigkeit schaden.

1) Sicherheits-Strategie des Dienstleisters (Phase 1)

Der Dienstleister wird an einer möglichst effektiven und angemessenen Lösung der Sicherheits-Anforderungen interessiert sein. Werden die Sicherheits-Anforderungen erst spät oder gar nach dem Betrieb des Outsourcings erkannt und definiert, dann können Streitereien über Vertragsinhalte unvorhergesehene Kosten hervorrufen und eine gute Partnerschaft in Frage stellen.

Einholen der Sicherheitsanforderungen Zu diesem Zwecke wird der Dienstleister sich möglichst früh die Sicherheitsanforderungen einholen. Für Sicherheitsdienste wie Benutzer-Authentisierung, Übertragungs-Chiffrierung oder Zugriffskontrolle wird er aus Risiko- und Kostensicht unterschiedlich starke Dienste mit unterschiedlichen Preisen anbieten können.

2) Angebot des Dienstleisters (Phase 2)

Um ein günstiges Angebot mit entsprechend günstigen Sicherheits-Massnahmen unterbreiten zu können, wird der Dienstleister versuchen, die Sicherheitsanforderungen auf der Basis der wirklichen IT-Risiken zu verifizieren.

Stellt ihm der Kunde die im vorigen Kapitel erwähnten Inhalte eines Sicherheits-Konzepts nicht zur Verfügung, dann sollte der Dienstleister (ggf. in Interviews) mit dem Kunden zusammen die Informationen für ein solches Sicherheits-Konzept zusammenstellen. Vom Kunden benötigt er dazu weitgehende Informationen über:

*Informationen für
Sicherheitskonzept*

- ☐ Kontext des Outsourcing-Gegenstandes;
- ☐ Prozess- respektive Systembeschreibung;
- ☐ Angaben über die Schutzobjekte und möglichen Schäden (Impacts);
- ☐ Anforderungen an die Sicherheitsmassnahmen.

*Grobes Sicher-
heitskonzept bei
Angebotssstellung*

Zur Ausarbeitung eines Angebots stellt sich der Dienstleister ein Sicherheitskonzept mit sämtlichen Kapiteln zusammen, wobei die Ausarbeitung gemäss dem zu diesem Zeitpunkt vorhandenen Informationsstand nur grob sein kann.

Bei der Angebotsausarbeitung muss der Dienstleister bedenken, dass es zu seiner Sorgfaltspflicht gehört, die mit dem Outsourcing notwendigen gesetzlichen und regulatorischen Auflagen an das outsourcende Unternehmen (z.B. Sarbanes-Oxley) einzuhalten. Bei den Risiken werden auch die durch das Projekt eingeführten neuen IT-Risiken des Dienstleisters aufgeführt sein (z.B. Zugriffe über das Internet, Abschottung verschiedener Kundensysteme gegeneinander). Auch diese neuen Risiken bedürfen zusätzlicher Massnahmen. Die wesentlichen Massnahmen und Umsetzungen müssen im Sicherheitskonzept des Dienstleisters formuliert sein. Nur dann können die groben Kosten und folglich die Preise im Angebot angegeben werden.

3) Vertragsentwicklung (Phase 3)

*Sicherheitskonzept
als Vertrags-
bestandteil*

Der Dienstleister und der potentielle Vertragspartner erarbeiten gemeinsam ein Sicherheitskonzept, das die detaillierten Anforderungen des Sourcing-Projekts erfüllt. Eine solche Version des Sicherheitskonzepts wird zum integrierenden Bestandteil des Sourcing-Vertrags und muss von beiden Vertragspartnern akzeptiert und eingehalten werden.

4) Sourcing Management (Phase 4)

*Gemeinsame und
überprüfbare
Basis*

Der Dienstleister hält sich an die im Sicherheitskonzept enthaltenen Massnahmen und an den Umsetzungsplan. Das Sicherheitskonzept bildet somit die gemeinsame und überprüfbare Basis für die Sicherheit des ausgelagerten Prozesses oder Systems.

15.2

Zusammenfassung

Das „Outsourcing“ kann für ein Unternehmen eine Reihe von Vorteilen haben, wie Komplexitätsreduktion, Variabilisierung von Fixkosten; vor allem aber die Reduktion der Kosten in der Grössenordnung von 20 %.

Bei aller Attraktivität eines Outsourcing müssen die neuen Kosten, vor allem die der Sicherheit und der Risiken, frühzeitig in die Betrachtungen einbezogen werden.

Für die Auslagerung von Prozessen mit hoher Informationsabhängigkeit muss dem Vorgehen ein gründliches Risikomanagement zugrunde gelegt werden. Es ist zu beachten, dass Gesetze, Regulative und vertragliche Abmachungen Sicherheitsmassnahmen vorschreiben und dass die Sicherheit auch ein „Qualitätsmerkmal“ ist. Die Sicherheit muss daher auf einem angemessenen Niveau nachhaltig gewährleistet werden.

Die Gartner Group empfiehlt u.a. anhand ihres Sourcing-Lifecycle-Modells die sorgfältige Analyse und Berücksichtigung der Risiken bis zum Vertragsabschluss in den Phasen der „Strategiefindung“, der „Evaluation“ und der „Vertragsdefinition“. Im ganzen Outsourcing Lifecycle soll das auslagernde Unternehmen „Due Diligence“ ausüben.

Als Instrument zur Analyse und Abstimmung der IT-Risiken und Massnahmen zwischen den Partnern bietet sich ein IT-Sicherheitskonzept mit den Eigenschaften eines Risikomanagement-Prozesses an.

Auch für den Dienstleister ist die Kenntnis der Sicherheitsanforderungen bereits zum Zeitpunkt des Angebotes wichtig, zumal jede Sicherheitsmassnahme ihren Preis hat. Vom Kunden benötigt der Dienstleister die Angaben zur Erstellung der Kapitel 1 bis 4 eines Sicherheitskonzepts. Zum Zeitpunkt der Angebotsstellung erstellt der Dienstleister in seinem Interesse ein Sicherheitskonzept in grober Fassung mit allen sechs Kapiteln.

Das als integrierender Bestandteil des Outsourcing-Vertrages geltende Sicherheitskonzept wird im Dialog zwischen Dienstleister und Kunde erarbeitet und abgestimmt. Es bildet somit im

späteren Betrieb die gemeinsame und überprüfbare Basis für die Risiken und die Sicherheit des ausgelagerten Prozesses oder Systems.

15.3

Kontrollfragen

1. Nennen Sie drei Argumente aus Unternehmenssicht für das Outsourcen und drei Gründe für neue Kosten?
2. Zu welchem Zeitpunkt vereinbaren Sie die Sicherheitsmassnahmen mit Ihrem Partner?
3. Nennen und beschreiben Sie die vier Phasen des „Gartner Lifecycle“ für Sourcing-Vorhaben?
4. Nennen Sie mindestens ein Instrument, mit dem Sie Risiken und Massnahmen für Sourcing-Vorhaben systematisch analysieren und die Konsequenzen für Massnahmen und neue Kosten absehen können?
5. Welchen Teilaspekt der Risiken sollte das auslagernde Unternehmen auf jeden Fall analysieren, bevor der Request for Proposal (RFP) ausgegeben wird?
6. Welche Vertragsinhalte werden Sie sowohl als auslagerndes Unternehmen als auch als Dienstleister dringend in die Vertragsausarbeitung einbeziehen?
7. Wie können Sie die Risiken während des Outsourcing-Betriebs unter Kontrolle halten?
8. Wie kann beim Outsourcing die Aktualität der Sicherheitsmassnahmen im Hinblick auf den möglichen Wandel in der Risikolage sichergestellt werden?
9. Aus welchen Gründen, empfehlen Sie dem Dienstleister bereits zum Zeitpunkt der Angebotsstellung, ein grobes Sicherheitskonzept zu erstellen?

16

Risikomanagement bei Nutzung und Angebot Cloud-Computing

*Virtualisierung /
Services aus der
Steckdose*

Dieses Kapitel folgt in logischer Folge dem Kapitel über Outsourcing, da viele Aspekte des „Outsourcing“ sowohl aus der Sicht des Anbieters als auch aus Sicht des Kunden respektive des Konsumenten ebenfalls zutreffen. Auch können die Prozesse für das Risikomanagement und das Sicherheitsmanagement, soweit diese generisch sind, beim Cloud-Computing angewandt werden.

Hingegen erfordert die Virtualisierung von IT-Komponenten und die Inanspruchnahme von IT-Leistungen in der Form von „Services aus der Steckdose“ eine neue Art der Risiko-Ermittlung und Massnahmenbestimmung, um sowohl auf der Anbieterseite als auch auf der Kundenseite akzeptable Restrisiken erreichen zu können.

Um in diesem Buch die Möglichkeiten des Risikomanagements und der Informationssicherheit erfassen zu können, muss vorab das Wesen, die Möglichkeiten und Varianten des Cloud-Computings in den wesentlichen Charakterzügen und Modellen behandelt werden. Für eine allgemein anerkannte Terminologie werden die Definitionen der US-amerikanischen für Standardisierungen zuständigen Bundesbehörde NIST* verwendet [Nide11]. Diese Definitionen der NIST werden mehrheitlich auch in den internationalen Standardisierungsanstrengungen der ISO angewandt (s. ISO/IEC Draft 27017, [Isoc12]).

16.1

Prinzip und Definitionen Cloud-Computing

Generell nimmt beim Cloud-Computing ein Konsument bzw. Abonnent (engl. Consumer oder Subscriber) mit als „Clients“ bezeichneten Zugriffseinrichtungen (z.B. Desktop-PC's, Laptops, Smartphones oder Server) über ein Netzwerk (häufig Internet) und entsprechenden Interfaces die Computer-Dienstleistung eines Anbieters (Provider) in Anspruch. Dabei bleibt dem Konsumenten verborgen, welche physikalischen Ressourcen des

* NIST=National Institute of Standards and Technology

Pool konfigurierbarer Computer-Ressourcen

Cloud-Anbieters zum Einsatz gelangen und wo sich diese im Einzelnen befinden.

Indes kann die Benützung eines vom Provider betriebenen „Pool“ von konfigurierbaren Computer-Ressourcen (z.B. Netze, Server, Datenspeicher, Applikationen und Dienstleistungen) schnell mit minimalem Management-Aufwand bereitgestellt werden. Die Systeme, auf die zugegriffen wird, sind aus Flexibilitäts- und Wirtschaftlichkeitsgründen mit „virtualisierten“ Ressourcen (z.B. Serverplattformen, Speicher) aufgebaut.

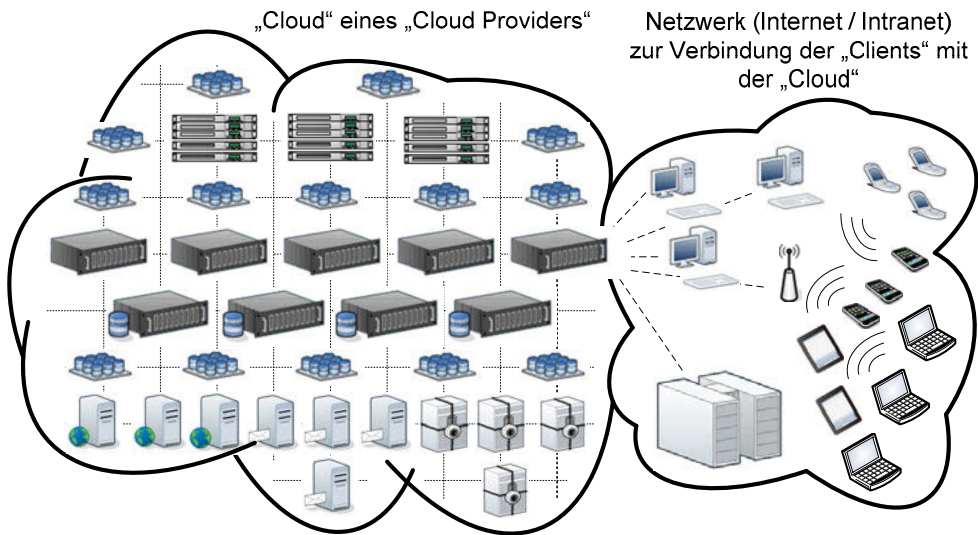


Abbildung 16.1: Prinzipieller technischer Aufbau einer Cloud

Im Gegensatz zum organisatorischen Konzept des „Outsourcing“, wo die IT-Infrastruktur eines Dienstleisters, oder Teile davon, exklusiv durch einen Kunden benutzt werden, ist „Cloud-Computing“ vor allem ein technisches Konzept, bei dem technische IT-Ressourcen, oder Teile davon, von mehreren Benutzern gleichzeitig benutzt werden können.

Dynamische Zuteilung der Ressourcen

Die durch Virtualisierung der IT-Ressourcen mögliche dynamische Zuteilung der Ressourcen erlaubt für den Anbieter (Provider) die Ausnützung von Skaleneffekten, die dem Konsumenten (Subscriber) in der Form niedriger Preise wiedergegeben werden können, wobei der Konsument zusätzlich von einer höheren Flexibilität hinsichtlich seiner Leistungsanforderungen profitieren kann.

Entgegen dem Outsourcing, bei dem der Provider immer externer Dienstleister ist und damit vertraglich für die Dienstleistung verantwortlich gemacht wird, kann beim Einsatzmodell einer „privaten Cloud“ durchaus ein und dasselbe Unternehmen sowohl in der Rolle des Anbieters (Providers) als auch in der Rolle des Konsumenten (Subscriber) agieren.

*Rollen „Provider“
und „Kunde“*

Dennoch macht es Sinn, für die organisatorische Behandlung des Cloud-Computing die Akteure analog dem „IT-Servicemanagement“ in die beiden Rollen „Provider“ auf der einen Seite und „Kunde“ auf der anderen Seite einzuteilen. Der Kunde kann wiederum einen oder mehrere „Benutzer“ als Akteure* enthalten, welche dann oft auch als „Konsumenten“ bezeichnet werden.

Für die Risiken beim Cloud-Computing bestehen somit, ähnlich dem Outsourcing, die zwei unterschiedlichen Sichten und zwar die Sicht des „Providers“ einerseits und die Sicht des „Kunden“ andererseits.

*„Ex-ante-
Betrachtung“ der
Risiken*

Bevor ein Cloud-Provider ein Engagement eingeht oder ein Kunde ein Abonnement oder einen Vertrag mit einem Cloud-Provider abschliesst, ist es im Sinne eines proaktiven Risikomanagements unabdingbar, die Risiken in einer „Ex-ante-Betrachtung“ abzuklären und diese, sowie die allenfalls notwendigen Massnahmen, in den Entscheid über den Vertragsabschluss einzubeziehen.

*Schützenswerte
Informationen bei
Provider*

Dem Kunden muss bewusst sein, dass er neben konkreten Leistungserwartungen vor allem seine schützenswerten Informationen mit all ihren Sicherheitsanforderungen einem Provider anvertraut. Der Cloud-Provider, auf der anderen Seite, trägt die Verantwortung für die Sicherheit dieser Informationen sowie für die Erfüllung der Leistungserwartungen und kann gegebenenfalls zur Haftung herangezogen werden sowie die Beschädigung seiner Ressourcen oder seiner Reputation riskieren.

*„Charakteristik“,
„Service-Modell“
und „Deployment-
Modell“*

Da die Risiken und damit das Sicherheitskonzept nicht alleine von den Akteuren (Cloud-Provider oder Kunden) sondern insbesondere auch von der eingesetzten **„Charakteristik“** sowie dem **„Service-Modell“** und dem verwendeten **„Deployment-Modell“** abhängen, werden diese Gesichtszüge im Folgenden gemäss dem NIST Standard 800-145 näher behandelt [Nide11].

* Die Begriffe für die Akteure des Cloud-Computing auf der Kunden-seite sind derzeit durch die Standardisierung noch nicht gefestigt.

16.1.1

Wesentliche Charakteristiken

- ❑ **On-demand self-service:** Ein Konsument kann einseitig, ohne Hilfe des Providers, die Computer-Leistungseinheiten zusammen- und bereitstellen.
- ❑ **Broad network access:** Auf die Leistungseinheiten des Providers kann über das Netzwerk (z.B. Internet) mittels standardisierter Mechanismen zugegriffen werden, welche die Benutzung eines heterogenen Spektrums von Zugriffs-Geräten (Client Platforms) fördern (z.B. Smartphones, Laptops, Workstations).
- ❑ **Resource pooling:** Die Computer-Ressourcen sind zusammengelegt (pooled) und die verschiedenen physikalischen und virtuellen Ressourcen können dynamisch zu- oder weggeschaltet werden, um die verschiedenen Konsumenten entsprechend ihrer Anforderungen zu bedienen. Dadurch entsteht eine Ortsunabhängigkeit, bei welcher der Konsument im Allgemeinen keine Kenntnis oder Kontrolle über die Lokation der verwendeten Ressourcen hat.
- ❑ **Rapid elasticity:** Die Leistungseinheiten können elastisch bereitgestellt und freigeschaltet werden, dies manchmal auch automatisch, um den Anforderungen entsprechend schnell zu skalieren.
- ❑ **Measured service:** Cloud-Systeme steuern und optimieren die Ressourcen-Nutzung mit entsprechenden Messfähigkeiten, womit die Transparenz sowohl für den Provider als auch für den Kunden über die benutzten Dienstleistungen erreicht werden kann.

16.1.2

Service-Modelle

- ❑ **Software as a Service (SaaS):** Dem Konsumenten werden in einer Cloud-Infrastruktur die Applikationen des Providers zur Benützung bereitgestellt. Der Konsument kann die den Applikationen unterliegende Cloud-Infrastruktur (Netzwerke, Server, Betriebssysteme, Speicher etc.), abgesehen von begrenzten benutzerspezifischen Konfigurationseinstellungen, weder steuern noch kontrollieren.
- ❑ **Platform as a Service (PaaS):** Dem Konsumenten werden Plattformen für seine Applikationen (selbst- oder

fremdentwickelte) zur Benützung bereitgestellt. Dabei werden durch den Provider bestimmte Programmiersprachen, Libraries, Services und Tools unterstützt. Der Konsument kann die den Applikationen unterliegende Cloud-Infrastruktur (Netzwerke, Server, Betriebssysteme, Speicher etc.) weder steuern noch kontrollieren, hat aber die Kontrolle über seine bereitgestellten Applikationen sowie allenfalls über die Konfigurationseinstellungen der Applikations-Umgebung.

- ❑ **Infrastructure as a Service (IaaS):** Dem Konsumenten werden in einer Cloud-Infrastruktur des Providers grundlegende Computer-Ressourcen wie Prozessorkapazität, Speicher, Netzwerke usw. zur Benützung bereitgestellt. Der Konsument kann auf dieser Infrastruktur beliebige Software mit entsprechenden Betriebssystemen und Applikationen einsetzen, wobei er die unterliegende Cloud-Infrastruktur weder steuern noch kontrollieren kann. Jedoch kontrolliert der Konsument seine bereitgestellten Betriebssysteme, Speicher und eingesetzten Applikationen sowie, in allenfalls begrenztem Umfang, bestimmte Netzwerk-Komponenten (z.B. Host Firewalls).

16.1.3

Deployment-Modelle

Für den Einsatz der Cloud-Services aus Benutzersicht sind hauptsächlich die folgenden sogenannten „Deployment-Modelle“ zu unterscheiden:

- ❑ **Private cloud:** Die Cloud-Infrastruktur ist für eine einzige Organisation* mit allenfalls mehreren Konsumenten (z.B. Geschäftseinheiten) bereitgestellt. Die Cloud-Infrastruktur kann entweder durch die Organisation selber oder durch eine Drittpartei oder einer Kombination dieser besessen, verwaltet und/oder betrieben werden. Auch kann sich die Cloud-Infrastruktur innerhalb oder ausserhalb der Organisations-Gebäude befinden.
- ❑ **Community cloud:** Die Cloud-Infrastruktur ist für eine spezifische Gemeinschaft von Konsumenten verschiedener Organisationen bereitgestellt, welche gemeinsame Interessen verfolgen (z.B. hinsichtlich Mission, Sicherheitsanforderungen, Policy und Compliance). Diese

* Organisation im Sinne einer juristischen Person

Cloud kann durch eine oder mehrere Organisationen der Community, durch eine Drittpartei oder durch eine Kombination dieser besessen, verwaltet und betrieben werden. Sie kann sich innerhalb oder auch ausserhalb der Gebäude der Gemeinschaft befinden.

- ❑ **Public cloud:** Die Cloud-Infrastruktur ist für die offene Benützung durch die Öffentlichkeit bereitgestellt. Diese Cloud kann durch eine geschäftliche, akademische, oder eine Regierungs-Organisation oder einer Kombination dieser besessen, verwaltet und betrieben werden. Sie befindet sich innerhalb der Gebäude des Providers.
- ❑ **Hybrid cloud:** Diese Cloud-Infrastruktur ist eine Zusammenführung von zwei oder mehreren einzelnen Cloud-Infrastrukturen (Private, Community oder Public) die zwar einzigartige Einheiten bleiben, aber mittels standardisierten oder hauseigenen Technologien verbunden sind, welche die Portabilität von Daten und Applikationen ermöglichen (z.B. cloud bursting).

16.2

Informationssicherheitsrisiken beim Cloud-Computing

Bei den Ausführungen über das Risikomanagement beim Cloud-Computing beschränken wir uns in diesem Buch auf die wichtigen und vieldiskutierten Informationssicherheits-Risiken (Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit). Andere IT-Risiken, wie z.B. Compliance-Risiken des Providers oder Leistungseinschränkungen beim Kunden (Konsumenten), werden nicht speziell behandelt, können aber nach ähnlichen Gesichtspunkten behandelt werden.

Aus den im Abschnitt 16.1 aufgeführten Definitionen und Funktionsweisen des Cloud-Computing wurde offensichtlich, dass die eingesetzte Charakteristik sowie die unterschiedlichen Modelle für Service und Deployment auch zu unterschiedlichen Risiken führen. Selbstverständlich tragen die Massnahmen des Cloud-Providers sowie die Befolgung der Benutzungspolicy auf der Konsumentenseite zu einem „Mehr oder Weniger“ hinsichtlich der Informationssicherheits-Risiken bei.

16.3

Cloud-Sourcing als Service aus der Kundenperspektive

Bevor wir das Risikomanagement beim Cloud-Computing im Einzelnen behandeln, wenden wir uns einem strukturierten Vorgehen bezüglich dem „Sourcing“ und dem Management der

*Ganzheitliche
Betrachtung
mittels IT-
Servicemanage-
ment*

Cloud-Services zu. Dazu gilt es zu erwähnen, dass die Service-Orientierung des Cloud-Computing ein IT-Servicemanagement nach ITIL-V3 oder ISO/IEC 20000 nahelegt.

Ein solches IT-Servicemanagement erlaubt eine von den Geschäftsanforderungen ausgehende ganzheitliche Betrachtung der Leistungserbringung, unter anderem auch für das Risikomanagement und die Informationssicherheit.

Die für die Geschäfts- und Kundenanforderungen massgeblichen „Service Level Agreements“ (SLA) enthalten die vom Provider zu erbringenden Leistungen, welche womöglich mit KPIs* messbar sein sollten.

Praxistipp:

Ohne ein strukturiertes, festgeschriebenes Serviceabkommen ist in der Regel für ein Unternehmen kein nachhaltiges Niveau der Serviceleistungen erzielbar, d.h. ein Cloud-Computing-Angebot ohne festgeschriebene Leistungsvereinbarungen kann für kritische oder sensible Serviceanforderungen nicht in Frage kommen.

*Verträge für in-
terne und externe
Serviceleistungen*

Die Kunden des „Cloud-Service-Provider“ sind entweder direkt die Konsumenten oder ein für die Konsumenten zuständiger „IT-Service-Provider“ (z.B. die interne IT-Abteilung eines Unternehmens). Die Verträge, die ein solcher interner IT-Service-Provider mit einem externen Cloud-Service-Provider abschliesst, werden in der ITIL-Terminologie als „Underpinning contracts“ bezeichnet. Für die intern auf der Kundenseite zu erbringenden Serviceleistungen, welche ebenfalls Cloud-Services sein können, dienen die sogenannten „Operational Level Agreements“ (OLA). Verpackt in diese Abkommen werden unter anderem die bereits erwähnten, für die Kommunikation und Nachprüfung der Geschäfts- und Kundenanforderungen wichtigen „Service Level Agreements“.

Für ein funktionstüchtiges und für den Kunden nützliches Servicemanagement und Sicherheits-Management genügt es nicht, wenn sich der Provider alleine einem Servicemanagement-System unterworfen hat.

*End-to-end-
Paradigma*

Das End-to-end-Paradigma heutiger Management-Systeme macht es erforderlich, dass auch auf der Kundenseite die mit dem Pro-

* KPI = Key Performance Indicator

vider und seinen Unterlieferanten abgestimmten Prozesse und Massnahmen umgesetzt werden müssen. So gilt es beispielsweise auf der Kundenseite, die Zugriffsrechte für die Benutzer festzulegen und die Zugriffs-Policies zu befolgen.

Die organisatorischen Beziehungen zwischen den Akteuren in einem in ein IT-Servicemanagement integriertes „Cloud-Sourcing“ sind in der Abbildung 16.2 veranschaulicht.

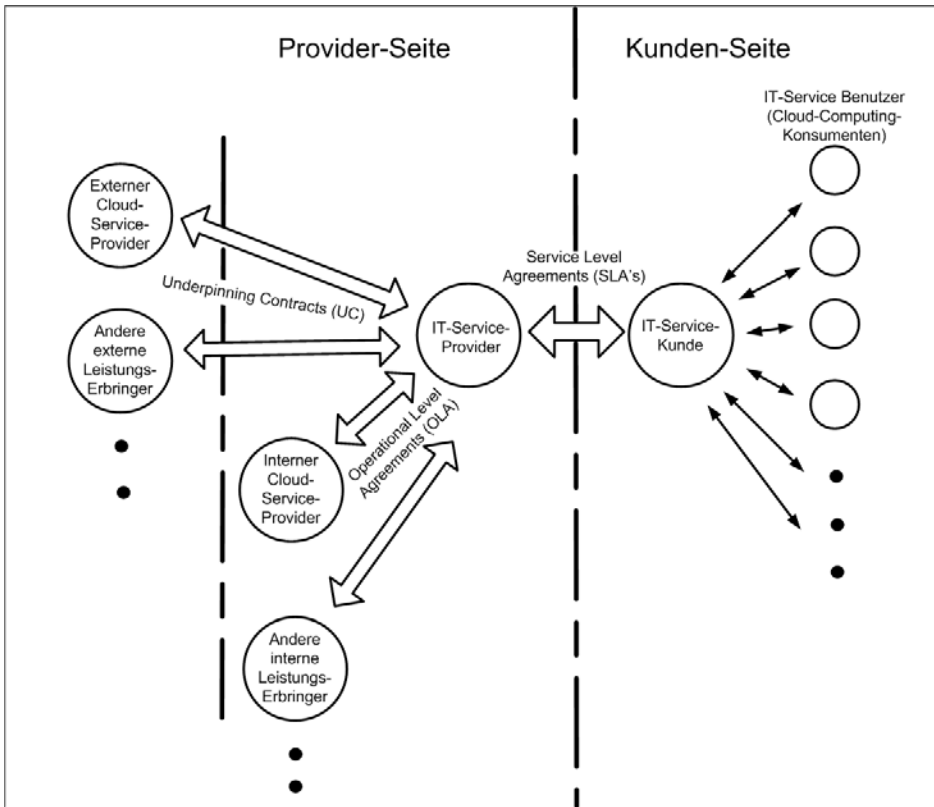


Abbildung 16.2: Beziehungen im IT-Servicemanagement mit Cloud-Services

Cloud-Sourcing-Vertrag

Das Sourcing-Abkommen, egal ob ein externes Sourcing, d.h. ein „Outsourcing“, oder ein „Internes Sourcing“ angewandt werden soll, bezeichnen wir in beiden Fällen der Einfachheit halber als „Cloud-Sourcing-Vertrag“.

Cloud- Sourcing- Lifecycle

Die Aktivitäten des Cloud-Sourcings orientieren wir am Cloud-Sourcing-Lifecycle, der in Abschnitt 15.1.1 bereits als Sourcing-Lifecycle gezeigt wurde. Dieser Cloud-Sourcing-Lifecycle hat die Phasen,

- „Cloud-Sourcing-Strategie“,
- „Evaluation und Auswahl“,
- „Vertragsentwicklung“ und
- „Cloud-Sourcing Management“

und wird idealerweise, wie Abbildung 16.3 zeigt, in den IT-Service-Lifecycle nach ITIL V3 eingebettet.

			ITIL Service Lifecycle				
			Service Strategie	Service Design	Service Transition	Service Operation	Continual Service Improvement
Cloud Sourcing Lifecycle	1	Cloud-Sourcing-Strategie	x				x
	2	Evaluation und Auswahl		x			x
	3	Vertragsentwicklung		x			x
	4	Cloud Sourcing Management		x	x	x	x

Abbildung 16.3: Einbettung Cloud-Sourcing-Lifecycle in ITIL Service Lifecycle

IT-Sicherheitskonzept

Den in allen Phasen des Cloud-Sourcing notwendige Risikomanagement-Prozess nehmen wir anhand eines auf den standardisierten Risikomanagement-Prozess abgestimmten IT-Sicherheitskonzepts vor. Ein solches Sicherheitskonzept bezieht sich auf die mit dem Cloud-Computing realisierten Services.

Es enthält in einer groben für die Evaluation massgeblichen Fassung ein Risiko-Assessment, das vor allem die Sicherheitsanforderungen an die Evaluation aufzeigt. In einer zweiten, für

den Betrieb der Services massgeblichen Fassung des Sicherheitskonzepts werden sodann die Risiken, Massnahmen, sowie der Massnahmen-Umsetzungsplan und die Restrisiken der Realisierung mit dem ausgewählten Provider dokumentiert. Aufgrund der Dokumentation der Aktionen mit ihren Ergebnissen eignet sich das IT-Sicherheitskonzept nicht nur für die Abstimmung der SLA's mit dem Cloud-Provider, sondern auch als „Prüfspur“ und als Kontrollwerkzeug zur Überwachung und für die fallweisen Sicherheits-Audits der mit Cloud-Computing realisierten Services.

16.3.1

Phase 1: Cloud-Sourcing-Strategie

Am Anfang und im Zentrum des Cloud-Sourcing-Lifecycle steht die Cloud-Sourcing-Strategie, die im Rahmen eines IT-Servicemanagements Teil der Service-Strategie ist. Folgende Fragestellungen sind zu klären:

- ☐ Passen Cloud-Services in die Servicestrategie, Architekturplanung und in die Sourcing-Strategie?
- ☐ Für welche Geschäftsprozesse soll Cloud-Computing angewandt werden?
- ☐ Welche hauptsächlichen Ziele verfolgen die Geschäftsprozesse, die für Cloud-Computing in Frage kommen?
- ☐ Welche hauptsächlichen Governance-, Compliance, Leistungs- und Sicherheitsanforderungen haben die Geschäftsprozesse, die für Cloud-Computing in Frage kommen?
- ☐ Welche Kombination von „Charakteristik“, „Service-Modell“ und „Deployment-Modell“ soll angewandt werden?
- ☐ Welche Kombinationen von „Charakteristik“, „Service-Modell“ und „Deployment-Modell“ könnten, abhängig von den verfügbaren Angeboten, ebenfalls in Frage kommen?
- ☐ Welche Vorteile werden erwartet oder in Betracht gezogen? (z.B. Fixkostenabbau, Kostenreduktion, Kapazitäts- und Leistungsagilität, Freisetzung eigener Kapazitäten, kurze Realisierungsdauer etc.)
- ☐ Welche Nachteile können in Kauf genommen werden (z.B. Kontrollverlust beim Servicemanagement, Anbieter-Lock-in, Einschränkungen in der Anwendungsflexibilität etc.)?

- ❑ Welche Nachteile verhindern Inanspruchnahme eines Angebots (z.B. Deployment in geographische Zonen mit inkompatiblen Rechtsvorschriften, unverbindliche Leistungs- oder Sicherheitszusagen)?
- ❑ Besteht für die auszulagernden Prozesse bereits ein Sicherheitskonzept mit den wichtigsten zum Zeitpunkt bekannten Sicherheitsanforderungen und Business-Impacts?
- ❑ ...

Cloud-Computing kann sowohl für die Übertragung von IT-Prozessen eines bestehenden Geschäftsmodells zum Einsatz gelangen als auch für die Übertragung von IT-Prozessen eines neuen Geschäftsmodells in die Cloud.

IT-Prozesse eines Geschäftsmodells

Falls die IT-Prozesse eines Geschäftsmodells bereits ohne Cloud-Computing bestehen, dann können aus einem allenfalls bestehenden Sicherheitskonzept die „Business-Impacts“ und die Anforderungen an die Sicherheitsmassnahmen sowie die bereits bestehenden Massnahmen abgeleitet werden.

Anhaltspunkte für Vergleiche und strategische Bewertungen

Auch ergeben sich aus einem bestehenden Sicherheitskonzept Anhaltspunkte für Vergleiche einer Cloud-Lösung mit einer herkömmlichen Realisierung. Bestehen die IT-Prozesse noch nicht, dann kann ein grobes Sicherheitskonzept mit den bis dahin bekannten Fakten (z.B. Compliance-Anforderungen und Business-Impacts) die Anhaltspunkte für die strategischen Bewertungen und Festlegungen hinsichtlich der Informations- und IT-Sicherheit liefern.

16.3.2

Phase 2: Evaluation und Auswahl

Das Spektrum von möglichen „Subscriber-Provider-Beziehungen“ reicht vom einfachen Anlegen eines Benutzer-Accounts in einer „Public-Cloud“ (z.B. Dropbox) bis hin zum Aufbau einer „Private-Cloud“, bei der beispielsweise der Betrieb an einen externen Provider ausgelagert ist (z.B. HP, IBM). Für die Bereitstellung von geringen Cloud-Kapazitäten oder Stückzahlen (z.B. Anzahl Server) an einen Kunden bestehen die Leistungs- und Sicherheitszusagen des Cloud-Anbieters meist lediglich in einseitig vom Provider ausgegebenen Leistungsangeboten, Nutzungsbedingungen und Richtlinien (Policies). Bei der Nutzung solcher „einfachen“ Angebote werden die einseitigen Nutzungsbedingungen und Sicherheitsrichtlinien automatisch akzeptiert.

Rigorese Ablehnung von Verantwortlichkeiten

In den Nutzungsbedingungen einiger öffentlicher Cloud-Angebote (z.B. Dropbox) werden gar die Verantwortlichkeiten und Haftungsgründe des Providers rigoros abgelehnt; dazu kommt, dass der Anbieter in seinen Nutzungsbedingungen darauf hinweist, dass die Nutzung der Services vom Provider jederzeit eingestellt oder die Services ohne Benachrichtigung zeitweilig oder endgültig beendet werden können. Es ist offensichtlich, dass ein solches Angebot nur für wenige Geschäftsprozesse überhaupt in Frage kommen kann, da beispielsweise eine anderweitig notwendige zusätzliche Absicherung gegen Datenverluste oder Betriebsunterbrechungen die vermeintlichen Vorteile des Angebots (z.B. niedere Kosten) zunichte macht.

Anforderungen berücksichtigende Angebote

Für die IT-Abwicklung von Geschäftsprozessen müssen demzufolge solche Angebote erwogen werden, die ein auf die Strategie-Anforderungen abgestimmtes Evaluationsverfahren möglich machen. Einige der Fragestellungen einer solchen Evaluation werden im Folgenden kurz beleuchtet:

- ☐ Sind die wichtigsten Sicherheitsanforderungen und Business-Impacts resultierend aus dem IT-Sicherheitskonzept in den „Request for Proposal“ (RFP) aufgenommen?
- ☐ Sind die Sicherheitsanforderungen und Business-Impacts im Rahmen eines IT-Sicherheitskonzepts mit den internen Business-Ownern abgestimmt (s. Abschnitt 16.4)?
- ☐ Gehen die Sicherheitsanforderungen nicht nur des Kunden, sondern auch des Endbenutzers (z.B. geheime Personendaten) aus dem IT-Sicherheitskonzept hervor?
- ☐ Sind die Anforderungen an den Provider womöglich in klaren unmissverständlichen SLAs aus Sicht der Geschäftsprozesse formuliert und quantifiziert?
- ☐ Sind die Anforderungen des Kunden an das „Change Management“, „Service Asset Management“ und „Configuration Management“ abgedeckt?
- ☐ Entsprechen die vom Provider offerierten Serviceleistungen den Anforderungen des RFP?
- ☐ Ist der Provider für das Informationssicherheits-Management seines Angebots zertifiziert?
- ☐ Ist der Anbieter bereit, sich vertraglich auf seine Zusagen festzulegen?
- ☐ Fallen Anbieter aus der „Shortlist“ der Anbieter-Evaluation heraus, weil sie vorab definierte „Killerkrite-

rien“ (z.B. wichtige Compliance-Anforderungen zum Datenschutz) nicht erfüllen?

☐ Kann die Provider-Auswahl aufgrund einer Nutzwert-Analyse getroffen werden?

☐ ...

16.3.3

Phase 3: Vertragsentwicklung

Bei der Vertragsentwicklung mit dem ausgewählten Provider sollten möglichst viele Prozesse, womöglich in Anlehnung an ein Servicemanagement (ITIL oder ISO/IEC 2000) festgelegt werden. Das Servicemanagement soll durchgängig sein und betrifft auch Prozesse auf der Kundenseite. So sind beispielsweise die wichtigen Festlegungen für die Prozesse „Incident Management“, „Change Management“, „Availability Management“, „IT Service Continuity Management“, „Information Security Management“ und „Service Desk“ zu treffen. Resultierend aus den abgestimmten Festlegungen kann ein definitives, für den zukünftigen Betrieb massgebliches IT-Sicherheitskonzept auf der Kundenseite erstellt werden. Anhand der Service-Orientierung sowie dem mit dem ausgewählten Provider abgestimmten IT-Sicherheitskonzept auf der Kundenseite sind allenfalls sogar auf den „Scope“ des Kundenservices zugeschnittene Zertifizierungen für das Servicemanagement nach ISO/IEC 20000 sowie für das Informationssicherheits-Management nach ISO/IEC 27001 möglich.

*Compliance über
IT-
Sicherheitskonzept*

Die Compliance zu ISO/IEC 27001 kann über das IT-Sicherheitskonzept hergestellt werden. Das IT-Sicherheitskonzept kann dabei die Resultate sämtlicher Schritte eines durch das Management getragenen Informations-Risikomanagements, vom Sicherheits-Assessment bis hin zur pragmatischen Massnahmenplanung und -umsetzung enthalten. Letztlich kann es auch als Prüfspur für die Überwachung der Aktivitäten und der fallweisen notwendigen Überprüfungen dienen.

*Fragestellungen
in Vertrag*

Die folgenden Fragestellungen fliessen in geeigneter Form in den Vertrag ein:

- ☐ Sind die Servicemanagement-Prozesse und die Sicherheits-Management-Prozesse auf beiden Seiten Provider sowie Kunde definiert und aufeinander abgestimmt?
- ☐ Sind die einzuhaltenden Protokolle und Interfaces bestimmt?

- ☐ Sind die zusätzlich notwendigen Systemkomponenten und -funktionen (z.B. Client-Funktionen) vereinbart und konzipiert?
- ☐ Sind die Leistungen und das Leistungsniveau (z.B. SLA's) entsprechend den Erwartungen ausgewiesen?
- ☐ Sind die Kosten und der Zeitplan abgestimmt und festgehalten?
- ☐ Sind die Anforderungen aus dem IT-Sicherheitskonzept mit den gegenseitigen Pflichten abgestimmt und festgelegt?
- ☐ Sind den zukünftigen Anforderungen, neuen Risiken, sowie der kontinuierlichen Verbesserung in abgestimmter Weise auf beiden Seiten Rechnung getragen?
- ☐ ...

16.3.4**Phase 4: Cloud-Sourcing-Management**

In dieser Phase kann das auf einem soliden Vertrag aufgebaute Servicemanagement* und das Informationssicherheits-Management betrieben werden. Dazu gehört eine IT-Service-Organisation, die sich mit dem Aufbau, Unterhalt und allenfalls auch dem Abbau der IT-Prozesse im Zusammenspiel mit der Service-Organisation des Cloud-Service-Providers befasst.

*Operational
Service Lifecycle*

Bleiben wir in der ITIL-Terminologie, dann enthält diese Phase den „Operational Service Lifecycle“ mit wichtigen Sub-Prozessen wie:

- ☐ Service Catalogue Management,
- ☐ Service Level Management,
- ☐ Availability Management
- ☐ Capacity Management,
- ☐ Change Management
- ☐ IT Service Continuity Management,
- ☐ Information Security Management,
- ☐ Access Management und
- ☐ Incident Management.

* ITIL und ISO/IEC 20000

	Für die Prozesse „Availability Management“, „IT Service Continuity Management“, „Access Management“ und das „Information Security Management“ dient sicherlich das IT-Sicherheitskonzept als Ausgangspunkt und Grundlage.
<i>Anlaufstelle / Service Desk</i>	Wie beim Outsourcing muss es sowohl auf Seiten des Providers als auch auf Seiten des Kunden eine Anlaufstelle geben. Über die Anlaufstelle (Service Desk) des Kunden werden die Störungen, Sicherheitsereignisse, Wünsche, Anforderungen und Fragen der Konsumenten gemeldet und verwaltet und mit der Anlaufstelle des Providers ausgetauscht.
<i>Service-Betrieb auf Kundenseite</i>	Für den eigentlichen Service-Betrieb auf der Kundenseite sollten zudem die Prozesse ☐ Event Management ☐ Incident Management, ☐ Request Fulfilment ☐ Problem Management und ☐ Access Management (Zugriffverwaltung) etabliert sein und Schnittstellen zu den analogen Prozessen beim Provider besitzen.

16.4

Risikomanagement für Cloud-Computing aus Kundensicht

Nachdem der grosse Vorgehensrahmen durch den Cloud-Service-Lifecycle vorgegeben ist, kann nun das eigentliche IT-Risikomanagement für Cloud-Computing behandelt werden. Der Risikomanagementprozess kann auf verschiedene Arten abgewickelt werden. In diesem Buch haben wir die pragmatische Lösung mittels eines IT-Sicherheitskonzepts gewählt (s. Abbildung 16.4). Ein solches Sicherheitskonzept kann angepasst an den Fortschritt im Cloud-Sourcing-Prozess sukzessive erstellt und in Auszügen mit den Partnern des Sourcing- und Servicemanagements abgestimmt werden.

<i>Abnahme-Versionen IT-Sicherheitskonzept</i>	Entsprechend dem Fortschritt im Sourcing-Lifecycle ist es empfehlenswert, das Sicherheitskonzept in zwei Abnahme-Versionen zu erstellen: 1. Grobfassung mit Anforderungen an die Provider-Evaluation; 2. Fein detaillierte Betriebsfassung entsprechend der Implementierung mit dem ausgewählten Provider.
--	---

16.4.1

Kontext im Sicherheitskonzept für Cloud-Computing-Einsatz

Ausgangslage

In der **Ausgangslage** des Sicherheitskonzepts werden vor allem die strategischen Festlegungen aus dem Sourcing-Lifecycle aufgeführt, welche für die Sicherheit massgeblich sind: z.B. Angaben über das Geschäftsmodell und die involvierten Geschäftsprozesse sowie deren Ziele, Governance-, Compliance-, Performance- und Security-Anforderungen.

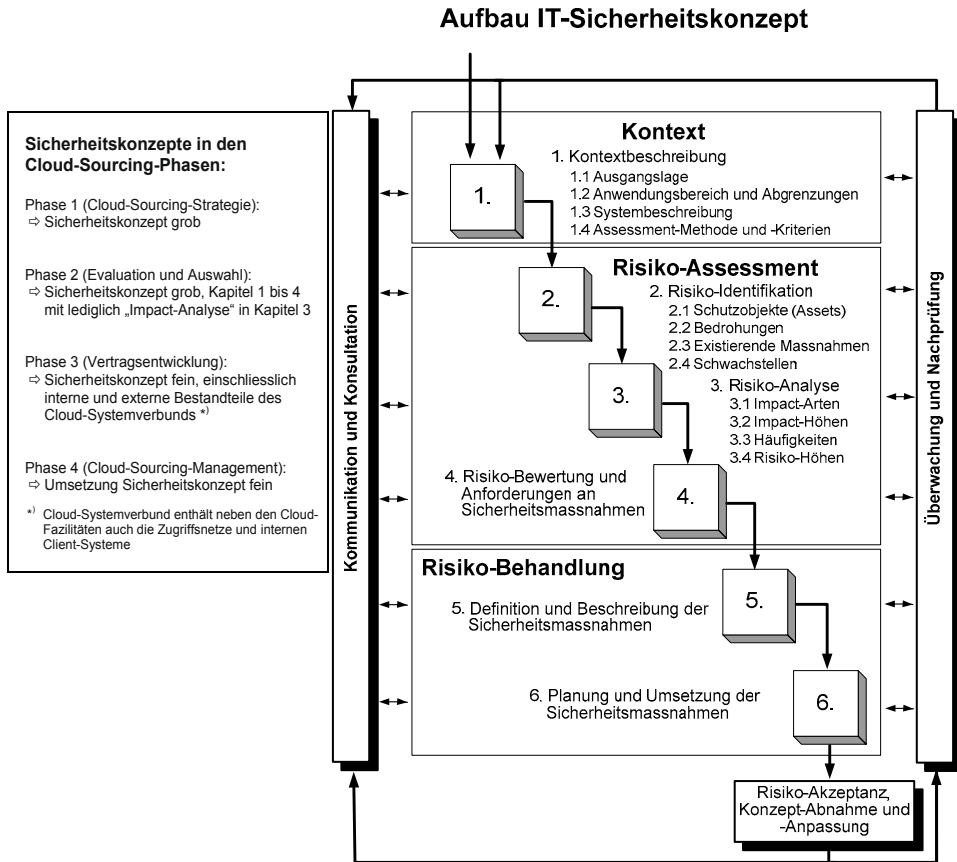


Abbildung 16.4: Risikomanagement im Cloud-Sourcing mit IT-Sicherheitskonzept

*Anwendungs-
bereich und
Abgrenzungen*

In der Beschreibung des **Anwendungsbereichs und der Abgrenzungen** werden vor allem die durch das Sicherheitskonzept behandelten Geschäftsprozesse und Risikoarten festgelegt sowie die Einschränkungen für deren Behandlung vorgenommen (Z.B. Nichtbehandlung der Client-Sicherheit und Beschränkung der

Sicherheitsziele auf Vertraulichkeit, Integrität und Verfügbarkeit). Werden in der Grobversion des IT-Sicherheitskonzepts beim Risiko-Assessment lediglich die Höhe der Impacts für den „worst case“ analysiert und lediglich die Anforderungen zur Behebung der Schwachstellen als Input für den Evaluationsprozess spezifiziert, dann wird dies ebenfalls im Abschnitt „Abgrenzungen“ ersichtlich.

*System-
beschreibung*

Der Abschnitt **Systembeschreibung** zeigt sodann die vom Kunden vorgesehenen Service-Prozesse und die angestrebte Cloud-Computing-Variante. Weiter werden die technischen und organisatorischen Systemkomponenten in ihrem Verbund sowie die allenfalls auf der Kundenseite bereits vorhandenen Sicherheitsmassnahmen (z.B. Firewalls, Zugriffskontrollsysteme) beschrieben.

*Assessment-
Methoden und -
Kriterien*

Im Abschnitt des Sicherheitskonzepts über die **Assessment-Methoden und -Kriterien** werden, neben Angaben über die Risikoermittlung für das nachfolgende Risiko-Assessment, eine Risiko-Matrix* festgelegt, die sowohl die ordinalen Bewertungsstufen als auch die Kriterien für die Risiko-Akzeptanz vorgibt (s. Abbildung 16.5).

Impact Häufigkeit		sehr klein	klein	mittel	gross	sehr gross
		0	1	2	3	4
sehr oft (mehrmals pro Jahr)	4	4 mittel	5 mittel	6 gross	7 gross	8 gross
oft (1 mal in 1 – 3 Jahren)	3	3 mittel	4 mittel	5 mittel	6 gross	7 gross
selten (1 mal in 3 – 10 Jahren)	2	2 klein	3 mittel	4 mittel	5 gross	6 gross
sehr selten (1 mal in 10 – 30 Jahren)	1	1 klein	2 klein	3 mittel	4 mittel	5 gross
unwahrscheinlich (1 mal in mehr als 30 Jahren)	0	0 klein	1 klein	2 mittel	3 mittel	4 mittel

Risikoeinstufung gemäss Risikoakzeptanz:

- akzeptiertes „kleines Risiko“: 0-2
- nicht akzeptiertes „mittleres Risiko“: 3-5
- nicht akzeptiertes „grosses Risiko“: 6-8

Akzeptanzlinie

Abbildung 16.5: Beispiel Risiko-Matrix mit Akzeptanzkriterien

* Risiko-Matrix an ISO/IEC 27005:2011, Anhang E.2.1 angelehnt

16.4.2

Risiko-Assessment

Gartner nennt sieben die Sicherheit betreffende Fragestellungen, die im Rahmen eines Sicherheits-Assessments geklärt werden sollten, bevor mit einem Cloud-Provider ein Vertrag abgeschlossen werden kann [Brod08]:

1. **Privilegierte Zugriffsrechte:** Ein potentieller Provider sollte Auskunft darüber geben, wie privilegierte Administratoren bei ihrer Einstellung überprüft, bei ihren Aktivitäten kontrolliert und vor allem wie ihre Zugriffe überwacht werden.
2. **Gesetzliche und regulatorische Compliance:** Cloud-Computing-Provider, die eine eingehende Überprüfung von Compliance-Anforderungen verweigern, kommen lediglich für triviale Services in Frage.
3. **Daten-Lokalisierung:** Der Provider sollte sich auf das Verarbeiten und Speichern der Daten innerhalb bestimmter Jurisdiktionen und auf die Nennung und die Beachtung der lokalen Datenschutz-Anforderungen verpflichten.
4. **Daten-Segregation:** Die Abschottung der Daten von anderen Kunden (Konsumenten) kann zwar mit Chiffrierung wirksam durchgeführt werden. Diese muss einerseits konsequent durchgeführt sein und darf andererseits die Verfügbarkeit (z.B. im Fehlerfalle) nicht beeinträchtigen. Der Provider sollte deshalb beweisen, dass die angewandten Chiffrier-Schemata funktionstüchtig entworfen und getestet sind.
5. **Recovery:** Die Frage ist zu klären, wie mit Desaster umgegangen wird, u.a. die Fähigkeit einer kompletten Restaurierung innerhalb konkreter Zeiterfordernisse.
6. **Unterstützung bei Nachforschungen:** Falls der Cloud-Computing-Provider sich nicht vertraglich verpflichten kann, die Nachforschungen mit entsprechenden Nachvollzugsmethoden (z.B. Logging) zu unterstützen und/oder keine Beweise dafür erbringen kann, muss davon ausgegangen werden, dass im Bedarfsfalle keine Nachforschungen möglich sein werden.
7. **Langfristige Überlebensfähigkeit:** Der potentielle Provider muss die Frage beantworten, was mit den Daten

im Falle einer Unternehmensaufgabe oder -fusion passiert. Ob beispielsweise in solchen Fällen die Daten vollständig in einem derartigen Format und in einer Weise ausgegeben werden, dass sie in einem alternativen Serviceangebot wieder importiert werden können.

Durchführung Risiko-Assessment

Angelehnt an das Risiko-Assessment einer Studie von ENISA [Encr09] werden im Folgenden beispielhafte Ansätze gezeigt, wie anhand des Risikomanagement-Prozesses, im Rahmen eines Sicherheitskonzepts, die Details für das Risiko-Assessment ermittelt werden können. Natürlich können für eine konkrete Anwendung in einem Unternehmen, unter Berücksichtigung der gewählten Cloud-Architektur und der spezifischen Gegebenheiten, gänzlich andere Assessment-Aussagen und -Werte resultieren.

Schutzobjekte (Assets) beim Cloud Computing

Für den Cloud-Service-Kunden fallen allfällige Schäden in erster Linie an den „Primären Assets“ und zwar den „Informationen“ und „Prozessen“ an, die bezüglich Verfügbarkeit, Vertraulichkeit und Integrität beeinträchtigt werden könnten (s. Abbildung 16.6). Selbstverständlich können bei PaaS und IaaS für Cloud-Service-Kunden noch zusätzliche Schadensauswirkungen an den „Unterstützenden Assets“ (z.B. Software oder Plattformen) anfallen.

	Schutzobjekt (Asset-Bezeichnung)	Owner
	<i>Primäre Assets</i>	
1	Endbenutzer-Services	
1.1	Kursverwaltung (als PaaS)	Hans Holbein
1.2	Vertrags- und Berechtigungs-Mgmt. (als PaaS)	Fritz Sauber
1.3	...	
2	Informations- oder Datenobjekte	
2.1	Börsenkursdaten	Hans- Holbein
2.2	Vertragsdaten	Fritz Sauber
2.3	Zugriffsberechtigungsdaten (Passwörter, Berechtigungsprofile etc.)	Fritz Sauber
2.3	...	
3	...	
...	...	

Abbildung 16.6: Beispiel Asset-Register

Risiken der Endbenütze-Services

Dienen die mit Cloud-Computing abzuwickelnden IT-Prozesse* mehreren Geschäftsprozessen mit unterschiedlichen Sicherheitsanforderungen, dann sind diese IT-Prozesse als separate Assets zu analysieren. In diesem Beispiel gehen wir davon aus, dass die Risiken sämtlicher Schutzobjekt-Arten (z.B. Client-Soft- und -Hardware, Netzwerk) sich im Endeffekt auf die „Primären Assets“, d.h. die „Endbenütze-Services“ und die „Informationen“ vererben. Deshalb sollen in diesem Beispiel lediglich die Risiken der Endbenütze-Services, in denen auch die Informationsrisiken enthalten sind, untersucht werden.

Schwachstellen-Identifikation in der Evaluationsphase (Phase 2)

Die Risiko-Identifikation bezüglich der Informationssicherheit im Rahmen eines IT-Sicherheitskonzepts ist vor allem in der Phase der Evaluation und Auswahl eines Cloud-Providers (Cloud-Sourcing-Phase 2) zur Spezifikation der Sicherheitsanforderungen wichtig. Geht es doch in dieser Sourcing-Phase unter anderem darum, die Risiken der verschiedenen Anbieter zu vergleichen, um eine entsprechend den Sicherheitsanforderungen gute Auswahl zu treffen.

Schwachstellen-liste

Zur Risiko-Identifikation dient eine Schwachstellenliste, anhand derer die verschiedenen Cloud-Angebote bezüglich Schwachstellen bewertet und verglichen werden können. Die Abbildung 16.7 zeigt das Beispiel einer solchen Liste von möglichen Schwachstellen, die in der Praxis den aktuellen Gegebenheiten angepasst werden soll. Die Ergebnisse beim ausgewählten Provider werden in der späteren endgültigen Fassung des Sicherheitskonzepts berücksichtigt.

Schwachstellen-Bewertung

Bei der Bewertung der Schwachstelle wird davon ausgegangen, dass diese durch eine relevante Bedrohung in entsprechendem Masse ausgenützt werden kann.

* Als „IT-Prozesse“ gelten in diesem Zusammenhang nicht die generischen Management-Prozesse (z.B. wie bei CobiT), sondern Unterstützungsprozesse, die mittels der IT einen „Endbenütze-Service“ liefern.

Nr.	Schwachstelle	Bewertung *) Exploit: 0-4 0: unwahrsch. Bemerkung *)
1	Intransparente Rechtsituation	
2	Unvorhersehbare gesetzliche Rahmenbedingungen und Rechtdurchsetzung	
3	Mangelnde Daten- und Service Portabilität	
4	Mangelnde Transparenz in Benutzungsbestimmungen	
5	Mangel an standardisierten Technologien und Lösungen	
6	Mangelhafte Zuteilung und Überwachung von Rollen und Verantwortlichkeiten	
7	Ungenügende Mitarbeiterkompetenz	
8	Ungenügendes Mitarbeiter-Screening	
9	„Vieraugen-“ und „Need-to-know“-Prinzip“ bei Unterstützungs- und Administrations-Aktivitäten nicht umgesetzt	
10	Keine oder schwache Datenchiffrierungsverfahren	
11	Schwachstellen in Komponenten und OS (z.B. kein Hardening)	
12	Schwaches Authentisierungs-, Autorisierungs- und/oder Account-System	
13	Schwächen im Benutzer-Bereitstellungsprozess (Provisioning)	
14	Schwächen im Benutzer-De-Provisioning	
15	Remote Access zum Management Interface	
16	Hypervisor-Exploit	
17	Mangelnde Ressourcen-Isolation	
18	Mangelnde Reputation-Isolation von anderen Kunden	
19	Schwächen in der Kommunikations-Chiffrierung	
20	Mängel bei Chiffrierung von Daten in Datenbanken, Archiven und Transfers	
21	Unmöglichkeit der Verarbeitung von Daten in chiffrierter Form	
22	Mängel in den Key-Management-Verfahren	
...	...	

*) Bewertung und Bemerkung erfolgt aufgrund des Proposals oder der Auskunft des Providers.

Abbildung 16.7: Beispiel einer Cloud-Computing-Schwachstellenliste
(vgl. [Encr09], S. 53-61)

* Need-to-know = Zugriffsberechtigungen und Dateneinsicht auf das absolut Notwendige eingeschränkt.

Impact-Analyse in der Evaluationsphase (Phase 2)

Zur Spezifikation der Sicherheitsanforderungen in der Evaluationsphase interessieren vor allem die Impacts. Da die aktuellen Bedrohungen und Schwachstellen, die ja noch der Evaluation unterliegen, noch nicht vorliegen, ist es sinnvoll, zur Anforderungsspezifikation die Geschäfts-Impacts in einer „Worst-case“-Betrachtung zu definieren.

*Worst-case
Betrachtung*

Dabei ist mit „Worst-case“ der maximale Schaden für die Geschäftstätigkeit aus Vertraulichkeits-, Integritäts- oder Verfügbarkeitsverletzungen zu verstehen. Die Abbildung 16.8 gibt das Beispiel einer solchen Impact-Einschätzung in den vorgegebenen ordinalen Impactstufen wieder.

*Höchste Impact-
Stufe*

Bei verschiedenen Impact-Arten wird nach dem Majoritätsprinzip jeweils die höchste Impact-Stufe als Geschäfts-Impact registriert.

Schutzobjekt (Asset)	Impact-Art	Einstufung *) Geschäfts-Impact: 0-4 0: kein Impact			Bemerkung
		Verfügbarkeit	Vertraulichkeit	Integrität	
Kursverwaltung	Firmenreputations- und Goodwill-Schaden	4	0	2	Die Kursdaten besitzen keinen Vertraulichkeitswert, müssen aber integer und „realtime-verfügbar“ sein.
	Kundenvertrauensverlust	3	0	2	
	Missbrauch geheime Daten (z.B. Passwörter und Berechtigungsprofile)	0	0	0	
	Lieferkontinuitätsverluste von Services	3	0	0	
	Verletzung regulatorische und legale Verpflichtungen	3	0	2	
	Migrations-Hindernis für Provider-Wechsel	0	0	0	
	Klagen und Schadensersatz	3	0	2	
	Majoritäts-Einstufung	4	0	2	
Vertrags- und Berechtigungs-Mgmt.	Firmenreputations- und Goodwill-Schaden	3	4	4	Die Vertrags- und Berechtigungsdaten müssen „integer“ sein; die Berechtigungsdaten sind zudem „streng vertraulich“.
	Kundenvertrauensverlust	3	4	4	
	Missbrauch geheime Daten (z.B. Passwörter und Berechtigungsprofile)	3	4	4	
	Lieferkontinuitätsverluste von Services	3	0	0	
	Verletzung regulatorische und legale Verpflichtungen	3	4	4	Möglicher Lizenzentzug
	Migrations-Hindernis für Provider-Wechsel	3	0	0	
	Klagen und Schadensersatz	3	3	3	
	Majoritäts-Einstufung	3	4	4	

*) Maximale im Worst-Case-Szenario auftretende Geschäfts-Impacts

Abbildung 16.8: Beispiel der Geschäfts-Impact-Einstufung

Risiko-Bewertung in der Evaluationsphase (Phase 2)

*Akzeptanz-
kriterien*

In der Evaluationsphase muss bereits darauf geachtet werden, dass in einer ausgewählten Realisierung die Akzeptanzkriterien (s. Abbildung 16.5) erfüllt werden können.

Risiko-Analyse im Sicherheitskonzept mit ausgewähltem Provider (Phase 3)

*Risiko-Analyse
und Risiko-
Bewertung für
Betriebsfassung*

Mit den aus der Evaluationsphase resultierenden Ergebnissen beim ausgewählten Provider für die Bewertung der Schwachstellen, die durch Bedrohungen ausgenutzt werden können, ist es nun möglich, die Risiko-Analyse und die Risiko-Bewertung für das definitive Sicherheitskonzept in seiner Betriebsfassung durchzuführen.

Die Abbildung 16.9 zeigt beispielhaft, wie die in der Evaluationsphase ermittelten Werte für das Risiko-Assessment in die Betriebsfassung des Sicherheitskonzepts einfließen.

*End-to-end-
Risikobetrachtung*

An dieser Stelle gilt zu erwähnen, dass die Betriebsfassung des Sicherheitskonzepts nicht nur die Risiken auf der Provider-Seite, sondern im Sinne einer End-to-end-Risikobetrachtung auch die Risiken auf der Kundenseite enthalten muss. So kommen die Risiko-Ursachen infolge der Bedrohungen und Schwachstellen auf der Kundenseite und der Kommunikationsverbindungen bis zum-Cloud-Provider dazu. Auch können bezüglich der Risiko-Auswirkungen für den Kunden weitere Schutzobjekte (Assets) auf der Kundenseite dazukommen, wie beispielsweise die über Schnittstellen verbundenen Datenbanken oder andere verknüpfte Endbenutzer-Services.

Risiko-Bewertung im Sicherheitskonzept mit ausgewähltem Provider (Phase 3)

Bei der Risiko-Bewertung in der Vertragsphase (Phase 3) mit dem ausgewählten Provider muss das Gesamtrisiko sowohl auf der Provider-Seite als auch auf der Kundenseite mit den Akzeptanzanforderungen in Einklang gebracht werden.

*Anforderungen
für Massnahmen
im Vertrag*

Daraus ergeben sich Anforderungen bezüglich der vertraglich zu vereinbarenden Massnahmen auf der Providerseite sowie auf der Kundenseite. Beispielsweise könnten die Anforderungen und Risiken bezüglich Verfügbarkeit des Endbenutzer-Services dringende Massnahmen für Back-up erforderlich machen, um die Risikoakzeptanzkriterien erfüllen zu können.

Risiko-Assessment														
Schutzobjekt (Asset)	Identifikation							Analyse					Bewertung	
	Risiko- bezeichnung	Bedrohungen und Schwachstellen, die von Bedrohungen ausgenutzt werden (Ursachen)	Impact-Arten für Cloud-Kunde (Schadensauswirkungen)							Impact-Höhe sehr gross: 4 gross: 3 mittel: 2 klein: 1 sehr klein: 0			Häufigkeit mehrmals pro Jahr: 4 1-3 Jahre: 3 3-10 Jahre: 2 10-30 Jahre: 1 >30 Jahre: 0	Akzeptanz (s. Abb. 16.5): 6,7,8: grosses Risiko, nicht akzeptabel; 3,4,5: mittleres Risiko, nicht akzeptabel; 2,1,0: unter Beobachtung tragbar. Bemerkungen
			Firmenreputations- und Goodwill-Schaden	Kundenvertrauensverlust	Missbrauch geheimer Daten	Lieferkontinuitätsverluste von Services	Verletzung regulatorische und legale Verpflichtungen	Migrations-Hindernis für Provider-Wechsel	Klagen und Schadensersatz	Verfügbarkeitsverlust	Vertraulichkeitsverlust	Integritätsverlust		
Kursverwaltung in PaaS	Daten-Lokalisierung	• Dislokation und Speicherung von Daten in Regionen mit nicht den Anforderungen entsprechender Jurisdiktion; • Intransparente Rechtsituation;	x	x		x	x		x	4	0	2	3	7 Gegenmassnahmen vertraglich absichern
Vertrags- und Berechtigungs-Mgmt. in PaaS		• Unvorhersehbare gesetzliche Rahmenbedingungen und Rechtdurchsetzung.	x	x	x	x	x		x	3	4	4	4	8 Gegenmassnahmen vertraglich absichern
Kursverwaltung in PaaS	Langfristige Überlebensfähigkeit (Lock-in)	• Mangelnde Daten- und Service-Portabilität (z.B. infolge unterschiedlicher „APIs“); • Mangelnde Transparenz in Benutzungsbestimmungen; • Mangel an standardisierten Technologien und Lösungen.	x	x		x	x	x	x	4	0	2	3	7
Vertrags- und Berechtigungs-Mgmt. in PaaS				x	x	x	x	x		x	3	4	4	3
Kursverwaltung in PaaS	Privilegierte Zugriffsrechte Provider	• Unautorisierte Zugriffe durch Mitarbeiter und Dritte; • Mangelhafte Zuteilung und Überwachung von Rollen und Verantwortlichkeiten; • Ungenügende Mitarbeiterkompetenz; • Ungenügendes Mitarbeiter-Screening;	x	x		x	x		x	4	0	2	2	6
Vertrags- und Berechtigungs-Mgmt. in PaaS		• „Vieraugen-“ und „Need-to-know-Prinzip“ nicht umgesetzt; • Keine oder schwache Datenchiffrierungsverfahren; • Schwachstellen in Komponenten und OS (z.B. kein Hardening).	x	x	x	x	x		x	3	4	4	2	6

Abbildung 16.9: Risiko-Assessment-Beispiel von Cloud-Computing-Risiken

Risikobehandlung im Sicherheitskonzept mit dem ausgewählten Provider (Phase 3)

Massnahmen auf Kundenseite und Provider-Seite

Die Massnahmen, die sowohl auf der Kundenseite als auch der Provider-Seite zur Behandlung der Risiken zu ergreifen sind, müssen in dieser Phase konkret ausgearbeitet, vertraglich abgesichert und im Sicherheitskonzept für die spätere Betriebsphase festgehalten werden. Auf der Providerseite könnte eine solche Massnahme eine zu vereinbarende Back-up Policy sein (z.B. Back-up-Methoden und -Formate, Versions-Kontrollen, Integritäts-Verifikation, Restore-Verfahren). Auf der Kundenseite besteht die Massnahme darin, eine Backup-Policy aus Anwendersicht zu erstellen, welche die Anleitung und die Parameter für das Back-up und Restore-Verfahren enthält.

Risikobewältigung, -überwachung und Optimierung während der Betriebsphase (Phase 4)

Sowohl das Servicemanagement als auch das Risikomanagement im Cloud-Computing sollte im Sinne eines PDCA-Zyklus die Überwachung und Kontrolle der Risiken und Prozesse sowie die daraus resultierende ständige Optimierung der Prozesse erlauben.

Abgestimmtes Incident-Management und Access-Management

Die dafür notwendigen Massnahmen und Aktivitäten waren bei der Vertragsgestaltung in der Cloud-Sourcing-Phase 3 bereits entsprechend vorzukehren und sind nun auch im Sicherheitskonzept für die Betriebsphase (Phase 4) entsprechend zu berücksichtigen. So erfordert beispielsweise das Service-Management ein zwischen Provider und Kunde abgestimmtes Incident-Management sowie ein abgestimmtes Access-Management. Auch ist die Funktion eines Service-Desk aufeinander abzustimmen.

Koordination der Anforderungen auf Kundenseite

Die Funktion des Betriebs erfordert insbesondere auch auf der Kundenseite Rollen und Verantwortlichkeiten zur Überwachung und zur Koordination der Anforderungen im Sinne eines Change-Managements.

16.5

Cloud-Sourcing-Lifecycle auf der Provider-Seite

Aus den Ausführungen über den „Cloud-Sourcing-Lifecycle“ auf Konsumentenseite werden die komplementären Anforderungen auf der Provider-Seite offensichtlich.

Provider-Strategie

Selbstverständlich verfolgt der Provider eine seinem Geschäftsmodell angemessene Strategie. Die für jeden Kunden verschiedenen individuellen Anforderungen, wird der Provider mit möglichst allgemeinen Lösungen abzudecken versuchen, um den

<i>Skaleneffekt</i>	Skaleneffekt des Cloud-Computings und das Serviceangebot als „Commodity“, ohne grossen Administrationsaufwand, beibehalten zu können. Den von den Kunden bezüglich Compliance, Informationssicherheit, Datenschutz und Geschäftskontinuität individuellen Anforderungen (s. Abschnitt 16.3) wird der Provider gleichwohl in geeigneter Form Rechnung tragen müssen.
<i>Individuelle Kunden-Anforderungen</i>	Inwiefern sogenannte „Elastic Compute Clouds“ gerade die unabdingbaren „Compliance-Anforderungen“ hinsichtlich Datenschutz (EU-Richtlinie) oder Bankenvorschriften (z.B. FINMA-Outsourcing-Vorschriften) erfüllen kann, bleibt abzuwarten. Die diesbezüglichen Lösungen müssen weniger von den Gesetzgebern und Regulatoren als von den Providern selber erwartet werden. Für den Provider kann es, wie für den Kunden, nützlich sein, seine Sicherheitsanforderungen und -massnahmen anhand eines eigenen, gegebenenfalls auf bestimmte Kundenanforderungen abgestimmten, IT-Sicherheitskonzepts auszuarbeiten und zu dokumentieren.
<i>Zertifizierungen ISO/IEC 27001 in Verbindung mit ISO/IEC 27017</i>	Sicherlich können auf bestimmte Kundenanforderungen fallweise notwendige Einschränkungen (z.B. Einschränkungen bei geographischen Dislokationen) sowie Zertifizierungen, basierend auf noch in Bearbeitung befindlichen Standards (z.B. ISO/IEC 27001 in Verbindung mit dem in Entwicklung befindlichen Standard ISO/IEC 27017 [Isoc12]) helfen, angemessen sichere Lösungen für gehobene Kundenanforderungen herbeizuführen

16.6

Zusammenfassung

Die Virtualisierung von IT-Komponenten und die Inanspruchnahme von IT-Leistungen in der Form von „Services aus der Steckdose“ erfordert eine neue Art der Risiko-Ermittlung und Massnahmenbestimmung, um für Cloud-Computing sowohl auf der Anbieterseite als auch auf der Kundenseite akzeptable Restriktionen erreichen zu können. Generell nimmt beim Cloud-Computing ein Konsument bzw. Abonnent mit als „Clients“ bezeichneten Zugriffseinrichtungen über ein Netzwerk und entsprechenden Interfaces die Computer-Dienstleistung eines Anbieters (Provider) in Anspruch. Dabei bleibt dem Konsumenten jedoch verborgen, welche physikalischen Ressourcen des Cloud-Anbieters zum Einsatz gelangen und wo sich die Ressourcen und Daten im Einzelnen befinden. Die Systeme, auf die zugegriffen wird, sind aus Flexibilitäts- und Wirtschaftlichkeitsgründen mit „virtualisierten“ Ressourcen aufgebaut. Die Risiken und damit das Sicherheitskonzept sind deshalb nicht alleine von

den Akteuren (Cloud-Provider oder Kunden) sondern insbesondere auch von der eingesetzten **„Charakteristik“** sowie dem **„Service-Modell“** und dem verwendeten **„Deployment-Modell“** der Cloud-Bereitstellung abhängig.

Das Informations-Risikomanagement auf der Kundenseite wird vorteilhaft im Rahmen eines „Cloud-Sourcing-Prozesses“ abgewickelt. Dieser hat die Phasen

- „Cloud-Sourcing-Strategie“,
- „Evaluation und Auswahl“,
- „Vertragsentwicklung“ und
- „Cloud-Sourcing-Management“,

die idealerweise in einen „IT-Service-Lifecycle“ nach ITIL V3 oder ISO/IEC 2000 eingebettet werden.

Das in allen Phasen des Cloud-Sourcing notwendige Risikomanagement wird anhand eines IT-Sicherheitskonzepts vorgenommen. Ein solches Sicherheitskonzept bezieht sich auf die mit dem Cloud-Computing realisierten Services und enthält in einer groben Fassung ein Risiko-Assessment, das die Sicherheitsanforderungen für die Provider-Evaluation aufzeigt. In einer zweiten, für den Betrieb der Services massgeblichen Fassung werden sodann die Risiken, Massnahmen, sowie der Massnahmen-Umsetzungsplan und die Restrisiken mit dem ausgewählten Provider dokumentiert. Aufgrund der Dokumentation der Aktionen mit ihren Ergebnissen eignet sich das IT-Sicherheitskonzept nicht nur für die Abstimmung der SLAs mit dem Cloud-Provider, sondern auch als „Prüfspur“ und als Kontrollwerkzeug zur Überwachung und für die fallweise durchzuführenden Sicherheits-Audits der mit Cloud-Computing realisierten Services.

Somit ist das IT-Sicherheitskonzept in der Evaluationsphase (Phase 2) eine wichtige Anforderungsbasis für den „Request for Proposal“ an die potentiellen Anbieter.

Bei der Vertragsentwicklung (Phase 3) mit dem ausgewählten Provider sollten möglichst viele Prozesse in Anlehnung an ein Servicemanagement (ITIL oder ISO/IEC 2000) festgelegt werden. Das Servicemanagement soll durchgängig sein und betrifft auch Prozesse auf der Kundenseite. So sind beispielsweise die wichtigen Festlegungen zu treffen für die Prozesse:

- „Incident Management“,
- „Availability Management“,

- „IT Service Continuity Management“,
- „Information Security Management“ und
- „Service Desk“.

In der Betriebsphase des Cloud-Sourcing (Phase 4) wird das auf einem soliden Vertrag aufgebaute Servicemanagement mit seinen Subprozessen sowie dem auf der Grundlage des IT-Sicherheitskonzepts definierten „IT Service Continuity Management“ und „IT Security Management“ betrieben.

Im „Risiko-Kontext“ des Sicherheitskonzepts werden vor allem die strategischen Festlegungen aus dem Sourcing-Lifecycle aufgeführt, welche für die Sicherheit massgeblich sind: Z.B. Angaben über das Geschäftsmodell und die involvierten Geschäftsprozesse sowie deren Ziele und Anforderungen. Zum Kontext gehört auch eine Systembeschreibung über die vom Kunden vorgesehenen Service-Prozesse und die angestrebte Cloud-Computing-Variante. Weiter werden darin die technischen und organisatorischen Systemkomponenten in ihrem Verbund sowie die allenfalls auf der Kundenseite bereits vorhandenen Sicherheitsmassnahmen (z.B. Firewalls, Zugriffskontrollsysteme) beschrieben. Im Weiteren enthält das IT-Sicherheitskonzept in der Abfolge eines Risikomanagement-Prozesses alle für das Risikomanagement notwendigen Voraussetzungen, Aktivitäten und Ergebnisse.

Aus den Ausführungen über den Cloud-Sourcing-Lifecycle auf Kundenseite werden auch die komplementären Anforderungen auf der Provider-Seite offensichtlich. Dabei verfolgt der Provider eine seinem Geschäftsmodell angemessene Strategie und wird versuchen, die für jeden Kunden individuellen Anforderungen mit möglichst allgemeinen Lösungen abzudecken, um den Skaleneffekt und das Serviceangebot als „Commodity“ nicht zu verlieren. Für den Provider kann es dennoch nützlich sein, seine Sicherheitsanforderungen und -massnahmen ebenfalls mittels eines auf bestimmte Kundenanforderungen abgestimmten IT-Sicherheitskonzepts auszuarbeiten und zu dokumentieren. Mit einer Zertifizierung, basierend auf den noch in Bearbeitung befindlichen Sicherheitsstandards Standards (z.B. ISO/IEC 27001 in Verbindung mit dem in Entwicklung befindlichen Standard ISO/IEC 27017) kann vom Provider überdies ein Gütesiegel für die Bereitstellung und das Management sicherer Lösungen erworben werden.

16.7

Kontrollfragen und Aufgaben

1. Der NIST-Standard 800-145 beschreibt u.a. drei Service-Modelle für Cloud-Computing.

Benennen Sie diese mit ihren Abkürzungen und beschreiben Sie kurz, was unter den einzelnen Service-Modellen zu verstehen ist.

2. Das Risikomanagement beim Cloud-Computing enthält ein Risiko-Assessment, das in den einzelnen Cloud-Sourcing-Phasen sukzessive verfeinert wird.

Nennen Sie sieben der für Cloud-Computing aus Kundensicht typischen Sicherheitsprobleme, die im Rahmen des Risiko-Assessments näher untersucht werden müssen?

3. Warum ist eine der Auswahl eines Anbieters vorgezogene Schwachstellenanalyse so wichtig?

Wie und mit welchen Hilfsmitteln kann diese vorgenommen werden?

4. In der Evaluations-Phase (Phase 2) eines Cloud-Computing-Angebots wollen Sie eine Impact-Analyse für ein IT-Sicherheitskonzept durchführen. Als Informations-Quellen können Sie folgende Stellen beanspruchen:

- a) Aussichtsreichster Anbieter;
- b) Chef interne IT-Abteilung;
- c) Interner Administrator für Zugriffsberechtigungen;
- d) Owner des Geschäftsprozesses, den es mit Cloud-Computing zu unterstützen gilt.

Welche Stelle konsultieren Sie für die Ermittlung der Impacts?

Begründen Sie:

5. In der Evaluations-Phase (Phase 2) wird die Grobfassung eines Sicherheitskonzepts erstellt.

Enthält dieses Sicherheitskonzept nebst der Impact-Analyse auch bereits Massnahmen?

Wenn ja, welche Kategorie von Massnahmen?

6. Bei der Vertragsentwicklung (Phase 3) sollten mit dem ausgewählten Provider wichtige Prozesse in Anlehnung an ein Servicemanagement gemäss ITIL V3 festgelegt werden.

Benennen Sie fünf solcher Servicemanagement-Prozesse auf der Kundenseite und deren wesentlichen Aktivitäten.

7. Eine in einer „Cloud“ durch mehrere Benutzer eines Kunden benutzte Applikation mit individuellen Zugriffsberechtigungen bedarf der Verwaltung und Zuteilung der verschiedenen Zugriffsberechtigungen auf die Benutzer.

Auf welcher Seite (Provider oder Kunde) und unter welchen Bedingungen soll die Verwaltung und Zuteilung der Zugriffsberechtigungen vorgenommen werden?

Anhang

A.1 Beispiele von Risiko-Arten

Marktrisiken

Abweichungen von System-Zielen	Bedrohungsliste
• Verlust von Abnehmern • Verlust der Marktposition • Probleme mit Partnern • Probleme mit Lieferanten • Schädigung des Unternehmensimage	• Wettbewerber im gleichen Markt • Abhängigkeit von Lieferanten • Schwierige Kunden und Kundenansprüche • Substitutions- und Ersatzprodukte • Veränderungen der Markt- und Branchenkonstellation • Währungsschwankungen

Finanzrisiken

Abweichungen von System-Zielen	Bedrohungslisten
• Gewinneinbussen/Verluste • Schwacher Cash Flow • Geringer Deckungsbeitrag • Schwierigkeiten bei der Finanzmittelaufnahme	• Zinsänderung • Bonitätsverschlechterung einer Gegenpartei • Eigene Bonitätseinbusse • Kursrisiken

Rechtliche Risiken

Abweichungen von System-Zielen	Bedrohungslisten
• Abgeschlossene Geschäfte nicht durchsetzbar • Verlust von Lizenzen • Haftung • Entschädigung • Strafe	• Rechte, Pflichten und Konditionen nicht klar und vollständig dokumentiert • Ungenügende Haftungsausschlüsse • Neue gesetzliche Auflagen • Gesetzesverletzung

Sachrisiken

Abweichungen von System-Zielen	Bedrohungslisten
• Betriebsbehinderungen • Produktionsausfälle • Sachbeschädigungen • Ressourcenschwund	• Brand • Terror • Betrug • Unterschlagung • Sabotage • Vandalismus • Technische Fehler • Wassereinbruch • Versorgungsengpässe (Wasser, Strom, Energie)

Projektrisiken

Abweichungen von System-Zielen	Bedrohungslisten
• Kostenabweichungen • Terminabweichungen • Funktionalitätsabweichungen • Qualitätsabweichungen	• Personalrisiken • Managementschwächen • Kommunikationsprobleme • Planungsdefizite • Lieferverzögerungen • Mängel bei Entwicklungs- und Einführungswerkzeugen

Informations- und IT-Risiken

Abweichungen von System-Zielen	Bedrohungslisten
• Verlust Integrität (Authentizität) • Verlust Verfügbarkeit • Verlust Vertraulichkeit	• Terroristische Attacken • Mangel notwendiger Fachkräfte • Manipulation / Betrug • Maskerade einer Benutzer- oder System-Identität • Infiltrierung Kommunikation • Abhörung Kommunikation • Einschleusen schädlicher „Codes“ • Missbrauch / Lahmlegen von Systemressourcen • Diebstahl von Informationen / Spionage • Absichtliche Beschädigung • Benutzerfehler • Betriebsfehler • Fehlfunktionen Hardware • Fehlfunktionen Software • Naturkatastrophen / Höhere Gewalt

Organisations- / Betriebsrisiken

Abweichungen von System-Zielen	Bedrohungslisten
• Qualitätsmängel • Fehlverarbeitungen / Ausschuss • Abweichungen von Produktspezifikationen • Ineffiziente Prozesse / Abläufe • Mittelabflüsse durch Diebstahl • Unterbrechungen der Leistungserstellung • Kostenexplosion	• Inkompetentes Personal • Schlechte Führung • Schlechte Arbeitsanweisungen, Kompetenzregelungen • Schlechte oder fehlende Kontrollen • Ausfall von Produktionseinrichtungen und IT-Systemen

Personalrisiken

Abweichungen von System-Zielen	Bedrohungslisten
• Personalengpässe • Fachpersonalmangel • Ausbildungsdefizite • Personalmangel	• Krankheit/Verletzung • Abwerbung • Ausgetrockneter Arbeitsmarkt • Abwanderung von Führungskräften • Fehlende Ausbildungsmöglichkeiten

A.2 Beispiele von „Cyber Threats“

Als „Cyber Threats“ werden die Bedrohungen rund um das Internet mit seinen Kommunikationsmöglichkeiten und seinen umgebenden Funktionen und Einrichtungen (Hompepages, E-Mail, Soziale Netzwerke, Systemplattformen usw.) bezeichnet.

Aufgrund der globalen Vernetzung, Virtualität der Gegenstände, Geschwindigkeit und Anonymität der Aktionen im „Cyber Space“ sowie der meist hohen betrieblichen Abhängigkeiten führen diese Bedrohungen mittlerweile zu einem hohen Risikopotential.

Mittel zur Schadensauslösung	Bedrohungsabsicht	Angriffsziele und Schadensausprägung
Soziale Netzwerke (Social Media)	• Imageschädigende Kampagnen • Vandalismus	Rufschädigung aufgrund der hohen Vernetzungsdichte bei Millionen von potentiellen Kunden innert wenigen Stunden. „Bestrafende“ wie „werbende“ Aktionen sind für das Publikum gut sichtbar und medienwirksam.
Hacking	• Kriminalität • Spionage • Sabotage	Der Angreifer dringt über bekannte oder zum Zweck des Angriffs analysierte Schwachstellen in ein System ein, um geheime Informationen ausspionieren, zu sabotieren oder anderweitige kriminelle Handlungen vorzunehmen. Er bedient sich dabei Angriffsmittel wie Trojanische Pferde, Spyware, Botnetze, Phishing und „Social Engineering“. Neben dem Ausnützen der typischen möglichen Schwachstellen an Systemen wie „Cross-Site-Scripting“ oder „Buffer overflow“ bedient sich ein Angreifer auch aus dem Arsenal einer Vielzahl von neuen und teilweise unveröffentlichten Schwachstellen und Angriffsmethoden.
Malware dazu gehören: • Trojanische Pferde • Viren • Würmer • Spyware • (mit Einschränkungen auch Adware und Cookies)	• Vandalismus • Kriminalität • Spionage • Sabotage	Mit den Trojanischen Pferden wird durch den Angreifer meist die Kontrolle über Funktionen des Zielsystems übernommen, was sämtlichen Bedrohungsabsichten dienen kann. Viren und Würmer nehmen bestimmte ungezielte Aktionen vor, z.B. Vandalismus und Sabotage. Mit Spyware (z.B. sog. Keylogger) werden vertrauliche Informationen gesammelt und missbräuchlich an den Angreifer abgeführt. Mit Adware wird unerwünschte Werbung betrieben. Die Cookies werden oft zur unerlaubten Erstellung von Benutzerprofilen zu Werbezwecken missbraucht.

Mittel zur Schadensauslösung	Bedrohungsabsicht	Angriffsziele und Schadensausprägung
Denial of Service Angriffe	• Vandalismus • Sabotage	Überlastung und Lahmlegung Internet-Portal durch Bombardierung der Internet-Eingänge mit Datenverkehr. Der massive Datenverkehr wird meist mittels sog. Botnetze generiert.
Botnetze	• Vandalismus • Kriminalität • Spionage • Sabotage	Der Angreifer sendet beispielsweise mittels Wurm ein spezielles Trojanisches Pferd an für diese Attacke ungeschützte Rechner (PC oder Server). Die solchermassen in hoher Anzahl infizierten Rechner werden nun, gesteuert durch das Trojanische Pferd, von Opfern zu Tätern gemacht und schicken an eine ausgewählte Portal-Adresse gleichzeitig Anfragen und verursacht somit eine „Denial of Service“-Attacke. Eine weitere Verwendung solcher Botnetze dient dem Abführen von gestohlenen Daten der Zielsysteme an den Angreifer.
Phishing	• Kriminalität • Spionage • Sabotage	Durch Überlistung von Benutzern durch gefälschte Aufrufe (z.B. mittels E-Mail) zur Preisgabe ihrer geheimen Benutzerdaten erbeutet der Angreifer vorwiegend Passwörter, PINs oder anderweitige geheime Zugriffsdaten. Solche Zugriffsdaten werden manchmal verkauft oder benutzt, um mittels unrechtmäßiger Zugriffe zu sabotieren, Informationen auszuspionieren oder anderweitige Aktionen wie betrügerische E-Commerce-Transaktionen oder den Weiterverkauf von Kreditkartennummern vorzunehmen.

A.3 Muster Ausführungsbestimmung für Informationsschutz

Tabelle A.3.1: Informations-Einstufungskriterien

Die Stufe der Vertraulichkeit wird umso höher gewählt, je höher der mögliche Schaden eines Missbrauchs ist	
Stufe 1	Schutzwürdige Informationen mit <u>internem</u> Charakter; Beispiele: - Interne Notizen und Mitteilungen, Konzepte, neutrale Kunden-Informationen (ohne weiteren Aufschluss über die Beziehungen des Kunden oder seine Transaktionen) - Personen-Informationen ohne besonderen Schutzbedarf (z.B. Adressangaben, sofern sie neutral sind und nicht in einem sensiblen Zusammenhang stehen)
Stufe 2	Nur einem bestimmtem Personenkreis anvertraute Informationen mit <u>vertraulichem</u> Charakter; Beispiele: - Konzepte oder Computer-Programme mit strategischem Charakter - Informationen von Kunden, welche die Beziehungen oder Transaktionen der Kunden wiedergeben - Besonders schützenswerte Personen-Informationen und Persönlichkeitsprofile
Stufe 3	Nur den namentlich bezeichneten Personen anvertraute Informationen mit <u>streng vertraulichem</u> Charakter; Beispiele: - Kryptographische Schlüssel oder Passwörter - Personen-Informationen, welche den Betroffenen schwerwiegend gefährden oder schädigen könnten
Die Stufe der Integrität wird umso höher gewählt, je höher der mögliche Schaden einer Integritätsverletzung ist	
Stufe 1	Informationen mit <u>niedrigen</u> Verfälschungs-/Verlustauswirkungen; Beispiele: - Informationen, die bei Integritätsverletzungen ohne grossen Aufwand berichtigt, rekonstruiert oder wiederholt werden können - Informationen, die bei Integritätsverletzungen zu <u>Verlusten unter € 10'000</u> führen
Stufe 2	Informationen mit <u>mittleren</u> Verfälschungs-/Verlustauswirkungen; Beispiele: - Informationen, die im Schadensfalle zu <u>bedeutenden Vertrauensverlusten</u> führen - Informationen, die im Schadensfalle zu <u>Verlusten von € 10'000 bis € 100'000</u> führen
Stufe 3	Informationen mit <u>hohen</u> Verfälschungs-/Verlustauswirkungen; Beispiele: - Informationen, die im Schadensfalle zu <u>sehr grossen Verlusten</u> führen - Informationen, die im Schadensfalle zu <u>Verlusten von über € 100'000</u> führen

Tabelle A.3.2: Allgemeiner Grundschutz für Informationen im Arbeitsumfeld

Für alle Stufen (1, 2 und 3) gültige Grundschutz-Massnahmen
☐ Arbeitsplatzeinrichtungen und mobile Geräte vor unberechtigtem Zugriff schützen; ☐ Arbeitsplatz nach Arbeitsschluss aufräumen, Informationen einschliessen und die persönlichen Arbeitsplatzeinrichtungen kontrolliert abschalten; ☐ Informationen vor unberechtigter Einsichtnahme, Diebstahl oder Manipulation schützen; ☐ Originalinformation sicherstellen (Informationen-Backup); ☐ Für jede Anwendung separates Passwort mit genügender Länge und Komplexität verwenden; ☐ Passwörter (Chiffrierschlüssel) getrennt von den chiffrierten Informationen aufbewahren und versenden; ☐ Systeme, Arbeitsstationen, Geräte, Datenträger und Applikationen stets vor Malware (Trojaner, Viren etc.) schützen (z.B. Firewall, Internet-Sicherheit, Virenschutz aktualisieren und keine fremden oder ungeprüften Datenträger einsetzen); ☐ Informationen und Datenträger geordnet sowie gemäss Aufbewahrungsfristen ablegen, archivieren und sicherstellen; ☐ Mobile Systeme und Datenträger zur eindeutigen Identifikation beschriften und gegen Diebstahl sichern (z.B. einschliessen); ☐ Informationen auf Informations- und Datenträger kontrolliert vernichten; ☐ Keine Systeme und Datenträger mit unvernichteten Informationen an unberechtigte Personen abgeben; ☐ Datenträger gegen Verluste und äussere Einwirkungen schützen (z.B. Liegenlassen, Schmutz, Kratzer, Knicken, Brechen, Wärme, Feuchtigkeit, magnetische Felder). ☐ Abhandengekommene Geräte, Informationsträger und Dokumente unverzüglich an Vorgesetzten, Informations-Owner und CISO melden;

Tabelle A.3.3: Massnahmen für Informationen der Stufen 2 und 3 in den einzelnen Schutzphasen

Phase	Besondere Massnahmen für Stufe 2	
	Vertraulichkeit	Integrität
Erstellung (Entwerfen, Schreiben, Erfassen oder Bearbeiten)	(1) Berechtigte festlegen; (2) Meldepflicht Datenschutzgesetz für Personendaten prüfen und befolgen; (3) Klassifikationsvermerk für Dokumente 'VERTRAULICH'.	(1) Berechtigte festlegen; (4) Sicherstellung .
Elektronische Übermittlung (z.B. File Transfer und E-Mail)	(7) Daten-Chiffrierung mit Chiffrier-Werkzeug in der Verantwortlichkeit des Absenders.	(8) Digitale Unterschrift.
Transport (Versand oder Mitnahme)	(9) Versand geschützt oder (11) Transport, begleitet und geschützt.	(9) Versand geschützt oder (11) Transport, begleitet und geschützt.
Aufbewahrung (Speicherung und Ablage)	(5) Zugriff geschützt.	(5) Zugriff geschützt; (12) Ablage geschützt.
Löschung / Entsorgung	(14) Daten-Löschung; (16) Informationsträger-Entsorgung	-

Phase	Besondere Massnahmen für Stufe 3	
	Vertraulichkeit	Integrität
Erstellung (Entwerfen, Schreiben, Erfassen oder Bearbeiten)	(1) Berechtigte namentlich festlegen; (2) Meldepflicht Datenschutzgesetz für Personendaten prüfen und befolgen; (3) Klassifikationsvermerk für Dokumente 'STRENG VERTRAULICH'.	(1) Berechtigte namentlich festlegen; (6) Zugriff streng geschützt; (4) Sicherstellung am selben Tag vornehmen.
Elektronische Übermittlung (z.B. File Transfer und E-Mail)	(7) Daten-Chiffrierung mit Chiffrier-Werkzeug in der Verantwortlichkeit des Absenders.	(8) Digitale Unterschrift.
Transport (Versand oder Mitnahme)	(10) Versand streng geschützt oder (11) Transport, begleitet und geschützt.	(10) Versand streng geschützt oder (11) Transport, begleitet und geschützt.
Aufbewahrung (Speicherung und Ablage)	(5) Zugriff geschützt; (7) Daten-Chiffrierung;	(6) Zugriff streng geschützt; (12) Ablage geschützt; (13) Daten-Auslagerung.
Löschung / Entsorgung	(15) Strenge Datenlöschung (17) Strenge Informationsträger-Entsorgung;	-

Anm.: Nachfolgende Tabelle A.3.4 zeigt die Erläuterungen der Massnahmen pro Ziffer

Tabelle A.3.4: Erläuterung der Massnahmen für Informationen der Stufen 2 und 3 in den einzelnen Schutzphasen

- (1) **Berechtigte:** Einzelpersonen oder Personengruppen (z.B. organisatorische Einheit), die Kenntnis oder Zugriff auf bestimmte Daten erhalten, werden durch den Owner festgelegt. Owner ist, wenn nicht speziell bestimmt, der Ersteller der Daten oder des Dokuments.
- (2) **Meldepflicht Datenschutzgesetz:** Personendaten auf Meldepflicht des Datenschutzgesetzes (DSG) prüfen und, wenn erforderlich, an den zuständigen Datenschutzbeauftragten der Gesellschaft melden.
- (3) **Klassifikationsvermerk:** Vorderste Seite des höchstklassierten Einzeldokuments mit Vermerk 'VERTRAULICH' oder 'STRENG VERTRAULICH' versehen. Klassifikation kann auch zeitlich beschränkt werden, z.B.: 'VERTRAULICH bis 1. August 2005, 12.00 Uhr'.
- (4) **Sicherstellung:** Originaldaten reproduktionsfähig kopieren (Daten-Backup) und getrennt vom Original aufbewahren oder transportieren.
- (5) **Zugriff geschützt:** Zugriff auf Daten nur mittels Schlüssel (Passwort, Schlüssel etc.).
- (6) **Zugriff streng geschützt:** Zugriff geschützt, zusätzlich lückenlose Beweissicherung der erfolgten Zugriffe.
- (7) **Daten-Chiffrierung:** Kryptographische Verschlüsselung der Daten bei der Abspeicherung oder Uebertragung, die nur durch den Besitzer des geheimen Schlüssels (resp. Passworts) rückgängig gemacht werden kann.
- (8) **Digitale Unterschrift:** Kryptographisches Beweisverfahren für die Richtigkeit von Absender und Dateninhalt einer Meldung.
- (9) **Versand geschützt:** Post oder Interner Kurier: Verschlissenes Behältnis und persönlich adressiert.
- (10) **Versand streng geschützt:** Post oder Interner Kurier: Persönlich adressiertes verschlossenes Behältnis mit Klassifikationsvermerk versehen und zusätzlicher äusserer Verpackung mit Vermerken 'EINSCHREIBEN', 'PERSÖNLICH'.
- (11) **Transport, begleitetet und geschützt:** Zugriff geschützt und unter persönlicher Aufsicht eines Berechtigten oder einer Vertrauensperson.
- (12) **Ablage geschützt:** Originalfähige Daten vor Elementarereignissen geschützt, d.h. Aufbewahrung in feuersicherem Behältnis, Datensafe, etc. oder in separatem Brandabschnitt.
- (13) **Daten-Auslagerung:** Originalfähige Daten zusätzlich zur Ablage in einem separaten Gebäude aufbewahren (z.B. externes Archiv).
- (14) **Daten-Löschung:** Löschen gemäss Löschi-Standard. Protokollierung des Löschi-Vorgangs.
- (15) **Strenge Datenlöschung:** Löschung gemäss Standard. Lückenlose Beweissicherung.
- (16) **Informations-Datenträger-Entsorgung:** Abholung durch Entsorgungsdienst. Protokollierung des Entsorgungsvorgangs.
- (17) **Strenge Informations-Datenträger-Entsorgung:** Vernichten (z.B. Shreddern) durch Informations-Owner selbst oder durch ihn selbst beauftragte Person. Lückenlose Beweissicherung des Vorgangs.

A.4 Formulare zur Einschätzung von IT-Risiken

Tabelle A.4.1: Formular zur Durchführung des „First Cut“

Formblatt First Cut					
Abteilung / Projektname / Systembezeichnung:					
Kontext und Kurzbeschreibung: Fortsetzung auf Zusatzblätter ☐					
Geschäftsprozess, Geschäftsanforderungen, Auftraggeber, Verantwortlichkeiten, verwendete Infrastruktur, Technologie, Anwendungsumfeld, Anzahl Benutzer, Art der Benutzer, Verbindung zu anderen Systemen, Bedeutung für Geschäft, spezifische Sicherheitsanforderungen, Systemabgrenzungen usw.					
Kernfragen zur Informations-Sicherheit					
1. Sind Grundschutz-Massnahmen eingerichtet? Nein ☐ Ja ☐ Wenn ja, welche?					
2. Welche Informationen werden mit dem System behandelt?					
3. Welche Schutzwürdigkeit besitzen die mit dem System verwendeten Informationen?					
	keine	Stufe 1	Stufe 2	Stufe 3	
Vertraulichkeit	☐	☐	☐	☐	
Integrität	☐	☐	☐	☐	
4. Ist das System mit Datennetzen verbunden? Nein ☐ Ja ☐ Wenn ja, mit welchen?					
5. Kann das System andere Systeme gefährden? Nein ☐ Ja ☐ Wenn ja, welche?					
6. Ist das System mit Systemen von Dritten verbunden? Nein ☐ Ja ☐ Wenn ja, mit welchen?					
7. Sind Informationen oder IT-Prozesse and Dritte ausgelagert (z.B. durch Outsourcing)? Nein ☐ Ja ☐ Wenn ja, an wen?					
Zusammenfassung der Ergebnisse der Risikoanalyse					
Füllen Sie diese Tabelle nach der Beantwortung der angefügten Formulare aus					
	sehr klein	klein	mittel	gross	sehr gross
Vertraulichkeit	☐	☐	☐	☐	☐
Integrität	☐	☐	☐	☐	☐
Verfügbarkeit (höchstes bewertetes Ausfallrisiko)	☐	☐	☐	☐	☐
Einverständnis und Genehmigung First Cut					
Vorbehalte / Auflagen:					
Rolle	Datum	Name	Unterschrift		
Projektleiter					
Business Owner (Auftraggeber)					
Chief Information Security Officer					

Tabelle A.4.2: Einstufung der Häufigkeiten aufgrund der Bedrohung

Bezeichnung System / Prozess:.....			
Wie häufig tritt aufgrund einer Bedrohung ein Schaden in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit auf?	Vertraulichkeit a b c d e	Integrität a b c d e	Verfügbarkeit a b c d e
Maskerade einer User- oder System-Identität	□□□□□	□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Abhören der Kommunikation	□□□□□		
Infiltrierung der Kommunikation	□□□□□	□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Einschleusen von schädlicher Software	□□□□□	□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Lahmlegen von Systemressourcen			□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Diebstahl	□□□□□		□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Absichtliche Beschädigung / Terrorismus		□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Benutzerfehler	□□□□□	□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ 15 Min.
Betriebsfehler	□□□□□	□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ 15 Min.
HW & SW - Wartungsfehler	□□□□□	□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Fehlfunktion / Versagen der Applikations-Software	□□□□□	□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Fehlfunktion / Versagen der infrastrukturnahen Software	□□□□□	□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Fehlfunktion / Versagen der Hardware		□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Naturkatastrophen		□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Arbeitskräftemangel	□□□□□	□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche
Andere (bitte spezifizieren)	□□□□□	□□□□□	□□□□□ 15 Min. □□□□□ 1 Std. □□□□□ 1 Tag □□□□□ 1Woche □□□□□ >1Woche

Hinweis: Metrik zur Einstufung der Häufigkeiten s. Tabelle A.4.3

Tabelle A.4.3: Metrik zur Einstufung der Häufigkeit

Häufigkeit der Fälle				
a	b	c	d	e
sehr oft	oft	selten	sehr selten	unwahrscheinlich
mehrere mal pro Jahr	1 mal in 1 bis 3 Jahren	1 mal in 3 bis 10 Jahren	1 mal 10 bis 30 Jahren	1 mal in > 30 Jahren

Tabelle A.4.4 : Bestimmung von Schadensausmass und Risiko

Bezeichnung System / Prozess:.....				
Schadensausmass (Impact) (Einstufungen entsprechend Schadens-Metrik Tabelle A.3.5)	Aufgrund Vertraulich- keitsverlust	Aufgrund Integritäts- verlust	Aufgrund Verfügbarkeits- verlust	Monetarisierter Schaden
	A B C D E	A B C D E	A B C D E	(€)
Finanzieller Verlust (z.B. Direkter Geschäftsverlust, Betrug, Wiederherstellungskosten)	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ 15 Min. ☐ ☐ ☐ ☐ ☐ 1 Std. ☐ ☐ ☐ ☐ ☐ 1 Tag ☐ ☐ ☐ ☐ ☐ 1Woche ☐ ☐ ☐ ☐ ☐ >1Woche	
Schädigung der geschäftlichen und wirtschaftlichen Interessen (z.B. Verwertbarkeit von Informationen wie Methoden, Konzepten, Verträgen, Störungen von Vertriebskanälen)	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ 15 Min. ☐ ☐ ☐ ☐ ☐ 1 Std. ☐ ☐ ☐ ☐ ☐ 1 Tag ☐ ☐ ☐ ☐ ☐ 1Woche ☐ ☐ ☐ ☐ ☐ >1Woche	
Beeinträchtigung der Management- und Geschäftsvorgänge (z.B. Falsche Führungsentscheide, Ineffizienter Betrieb, Schwache Verhandlungen)	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ 15 Min. ☐ ☐ ☐ ☐ ☐ 1 Std. ☐ ☐ ☐ ☐ ☐ 1 Tag ☐ ☐ ☐ ☐ ☐ 1Woche ☐ ☐ ☐ ☐ ☐ >1Woche	
Verlust an Goodwill (z.B. schlechtes öffentliches Image, Verlust an Glaubwürdigkeit/Ranking, Fallen des Aktienpreises)	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ 15 Min. ☐ ☐ ☐ ☐ ☐ 1 Std. ☐ ☐ ☐ ☐ ☐ 1 Tag ☐ ☐ ☐ ☐ ☐ 1Woche ☐ ☐ ☐ ☐ ☐ >1Woche	
Nichteinhaltung von gesetzlichen und regulativen Verpflichtungen (z.B. keine ordnungsgemässe Geschäftsführung, Verletzung Sorgfaltspflicht, Geldwäscherei, Computerkriminalität, Sittenwidrigkeit)	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ 15 Min. ☐ ☐ ☐ ☐ ☐ 1 Std. ☐ ☐ ☐ ☐ ☐ 1 Tag ☐ ☐ ☐ ☐ ☐ 1Woche ☐ ☐ ☐ ☐ ☐ >1Woche	
Beeinträchtigung von Informationen anderer Personen (z.B. Verletzung Geschäftsgeheimnis, Verletzung Datenschutzgesetz)	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ 15 Min. ☐ ☐ ☐ ☐ ☐ 1 Std. ☐ ☐ ☐ ☐ ☐ 1 Tag ☐ ☐ ☐ ☐ ☐ 1Woche ☐ ☐ ☐ ☐ ☐ >1Woche	

Anm.: Bei Verwendung der „First Cut“-Formulare erfolgt die Risikobestimmung mit den aus der Einschätzung resultierenden Höchstwerten für „Häufigkeit“ und „Schadensausmass“.

Bestimmung des Risikos					
Schadenshöhe pro Fall [Mio. €]	E klein < 0.3	D mittel 0.3 - 1	C gross 1-3	B sehr gross 3 - 10	A katastrophal > 10
Häufigkeit der Fälle					
sehr oft (mehrere mal pro Jahr)	mittel	gross	sehr gross	katastrophal	irreal
oft (1 mal in 1 bis 3 Jahren)	klein	mittel	gross	sehr gross	katastrophal
selten (1 mal in 3 bis 10 Jahren)	sehr klein	klein	mittel	gross	katastrophal
sehr selten (1 mal in 10 bis 30 Jahren)	sehr klein	klein	klein	mittel	katastrophal
unwahrscheinlich (1 mal in > 30 Jahren)	-	sehr klein	klein	mittel	katastrophal

Tabelle A.4.5 : Beispiel einer Schadensmetrik für IT-Risiken

Impacts	Direkter finanzieller Verlust (Barwert der Ersatzkosten+ Opportunitäts-kosten) [in Mio. €]	Sonstige firmentypische Schadensauswirkungen		
		Schädigung der geschäftlichen und wirtschaftlichen Interessen Beeinträchtigung der Management- und Geschäftsvorgänge Verlust an Reputation	Nichteinhaltung gesetzlicher und regulativer Verpflichtungen (*)	Beeinträchtigung Informationen anderer Personen (*)
		Beispiele		
katastrophal A	> 10 z.B. aufgrund umfassender Zerstörungen und/oder zeit- und ressourcen-aufwändiger Wiederherstellungs-Aktivitäten	Massiver Umsatzrückgang aufgrund eines Ereignisses mit sehr grosser Marktbeeinflussung	Endgültiger Lizenzentzug oder Höchst-Strafen bei aufgetretenen Schadensfällen	-
sehr gross B	3 - 10 z.B. aufgrund langanhaltender Ausfälle	Kunden stellen infolge preisgegebener Produktionsgeheimnisse oder irreparabler Imageschäden auf Alternativprodukte um	Vorübergehender Lizenzentzug oder Strafen bei aufgetretenen Schadensfällen	Klagen wegen Abhören und gezieltem Missbrauch von Personal- und/oder Kundendaten in grossem Umfang
gross C	1 - 3 z.B. aufgrund Zerstörung von Produktionssystemen und entsprechenden Produktionsausfällen	Abnehmer drücken Preis aufgrund abgeflossener Geschäftsinformationen	Sanktionen/ Strafen wegen grober Sorgfaltspflicht-verletzung	Klage und Schadensersatz wegen Verletzung des Geschäftsgeheimnisses von Kunden oder Partnern
mittel D	0.3 - 1 z.B. aufgrund Schadensersatzforderungen bei fehlerhaften Produkt- und/oder Service-Lieferungen	Erhöhte Werbeaufwendungen infolge angeschlagener Reputation	Verfahren wegen Mängel der ordnungsgemässen Geschäftsführung	Klagen wegen indiskreter Behandlung von Personaldaten
E klein	< 0.3 z.B. aufgrund kleinerer Störungen und daraus entstandener Rückvergütungen	-	-	Schadensersatz wegen vereinzelter Verletzung des Datenschutzes

* z.T. persönliche Haftung verantwortlicher leitender Personen

A.5 Beispiele zur Aggregation von operationellen Risiken

A.5.1 Beispiel der Bildung eines VAR durch Vollenumeration

Sollen zwei Verteilungen von Zufallszahlen zu einer Gesamtverteilung aggregiert werden, dann kann dies, - vorausgesetzt die Verteilungen sind voneinander statistisch unabhängig -, durch Faltung der beiden Wahrscheinlichkeitsdichtefunktionen und numerisch mit der Vollenumeration erfolgen:

$$h(x) = \int_{i=1}^n f(x | k) \times p(k) dk$$

Im Folgenden wird die Aggregation der Daten einer „Verlustanzahl“-Verteilung mit einer „Verlusthöhen“-Verteilung zu einer Gesamtverlust-Verteilung mittels Vollenumeration gezeigt. Die Gesamtverlustverteilung dient sodann der Ermittlung eines „Operational Value at Risk“:

Verlustanzahl-Verteilung p(k)		x	Verlusthöhen-Verteilung f(x k)		
Verlustanzahl pro Jahr	Wkt. *)		Verlusthöhe [Mio. €]	Wkt.	
0	0.3	0.9	1	0.4	1.8
1	0.5		2	0.5	
2	0.2		4	0.1	
					1.62 Mio. € (erwarteter Gesamtverlust)

*) Wkt: Wahrscheinlichkeit als rel. Häufigkeit erfasst

Verlust- anzahl	Wkt. Verlust- anzahl	1. Verlust- höhe [Mio. €]	Wkt. 1. Ver- lusthöhe [Mio. €]	2. Ver- lusthöhe [Mio. €]	Wkt. 2. Ver- lusthöhe [Mio. €]	Gesamt- verlust [Mio. €]	Gesamt- Wkt.
0	0.3	-				0	0.3
1	0.5	1	0.4			1	0.2
1	0.5	2	0.5			2	0.25
1	0.5	4	0.1			4	0.05
2	0.2	1	0.4	1	0.4	2	0.032
2	0.2	1	0.4	2	0.5	3	0.04
2	0.2	1	0.4	4	0.1	5	0.008
2	0.2	2	0.5	1	0.4	3	0.04
2	0.2	2	0.5	2	0.5	4	0.05
2	0.2	2	0.5	4	0.1	6	0.01
2	0.2	4	0.1	1	0.4	5	0.008
2	0.2	4	0.1	2	0.5	6	0.01
2	0.2	4	0.1	4	0.1	8	0.002

Der **Operational Value at Risk (OpVAR)** ergibt sich aus dem „Value at Risk für ein x-prozentiges Konfidenz-Niveau“ minus dem „erwarteten Verlust“.

Gesamtverlust [Mio. €]	Gesamt- Wkt.	Kumulierte Gesamt-Wkt. *)	Beispiele von OpVAR bei unterschiedlichen Konfidenz-Intervallen
0	0,3	0.3	
1	0,2	0.5	
2	0.282	0.782	
3	0.08	0.862	
4	0.1	0.962	OpVAR = 2.38 Mio. € bei Konfidenz-Niveau 96.2 %
5	0.016	0.978	
6	0.02	0.998	OpVAR = 4.38 Mio. € bei Konfidenz-Niveau 99.8 %
8	0.002	1.0	

*) Zur Berechnung eines VAR bei einem genau definierten Konfidenzintervall kann zwischen zwei Gesamt-Wahrscheinlichkeiten linear interpoliert werden.

Das für die Erläuterung der Aggregation anschauliche Verfahren der Vollenumeration zeigt gleichzeitig, dass bei vielen Datenwerten das Verfahren schnell sehr umfangreich und aufwändig wird. Im praktischen Einsatz ist deshalb eine Monte Carlo Simulation, wie sie unter A.5.3 grob skizziert wird, vorteilhafter einzusetzen.

A.5.2 Beispiele für Verteilung von Verlusthöhen und Verlustanzahl

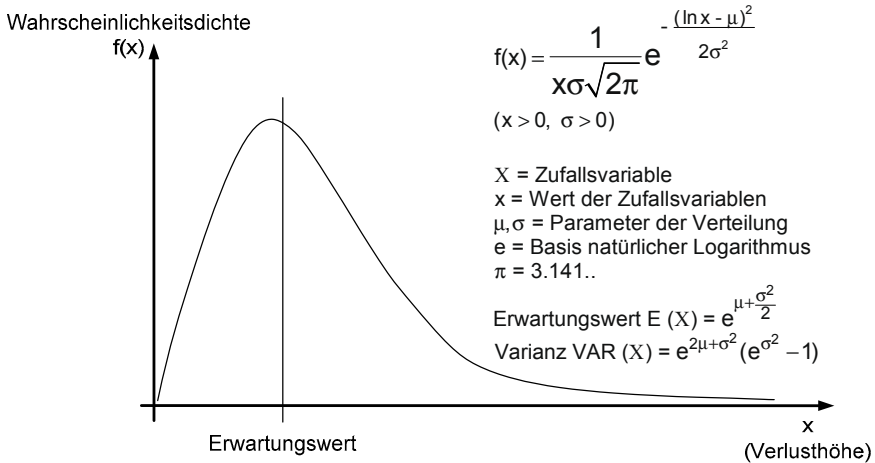


Abbildung A.5.1: Verteilung der „Verlusthöhe“ mit Log-Normal-Verteilung

Für die statistische Verteilung der „Verlusthäufigkeiten“ bietet sich beispielsweise die Poisson-Verteilung an.

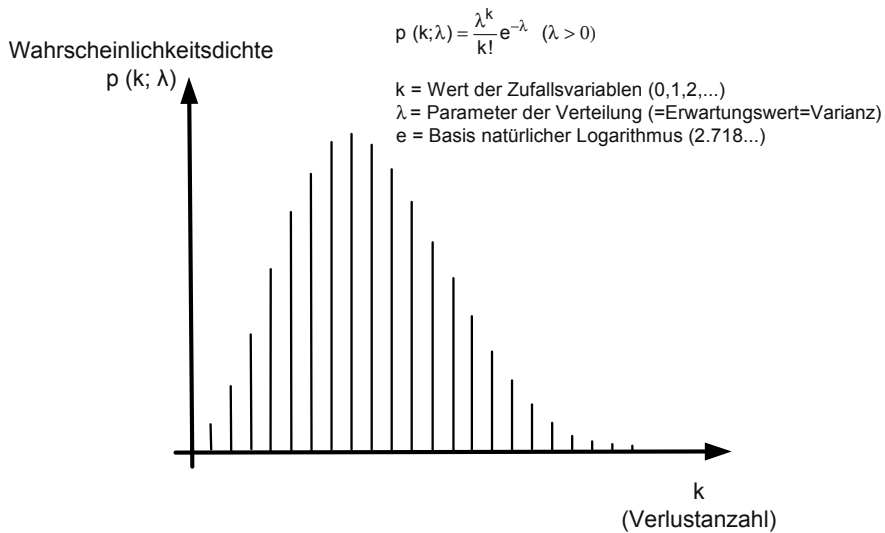


Abbildung A.5.2: Verteilung der „Verlustanzahl“ (Häufigkeit) mit Poisson-Verteilung

Die Kombination der Verlusthöhen-Verteilung und der Verlustanzahl-Verteilung zu einer Gesamtverlust-Verteilung kann, statistische Unabhängigkeit vorausgesetzt, mit der „Faltung“ der beiden Verteilungsdichtefunktionen durchgeführt werden (s. A.5.1).

A.5.3 Aggregation mittels Monte-Carlo-Methode

Monte-Carlo-Methode

Aus verschiedenen Gründen können sich rein analytische Berechnungen als unlösbar darstellen. Solche Fälle liegen dann vor, wenn beispielsweise zu wenig und ungenaues statistisches Datenmaterial vorliegt oder die den Risiken zugrundeliegenden Zufallsvariablen statistische Abhängigkeiten besitzen.

Eine Methode, die auch in diesen Situationen sinnvolle quantitative Ergebnisse liefert, ist die Monte-Carlo-Simulation. (Der Name kommt von der berühmten Spielbank in Monte-Carlo.)

Die Methode ist am Beispiel der Kombination einer Verlustanzahl-Verteilung mit einer Verlusthöhen-Verteilung zu einer Gesamtverlust-Verteilung, anhand von drei groben Prozessschritten gezeigt (statistische Unabhängigkeit vorausgesetzt):

Schritt 1:

Als Input-Daten werden vorhandene Zufallsdaten eingegeben, die mit fehlenden und für die Zukunft relevanten Zahlen und Parametern ergänzt werden können. Sollen theoretische Verteilungsfunktionen approximiert werden, dann kann dies mit entsprechenden Tests erfolgen (z.B. Chi-Quadrat-Anpassungstest). In unseren Beispielen sind die Verlusthöhen auf eine Log-Normal-Verteilung und die Verlust-Anzahl auf eine Poisson-Verteilung zu approximieren.

Schritt 2:

Der Monte-Carlo-Algorithmus wählt nun aus der Verlustanzahl-Verteilung nach dem Zufallsprinzip eine Anzahl von Verlusten und wählt entsprechend dieser Anzahl zufällige Verlustwerte aus der Verlusthöhen-Verteilung aus. Diese Anzahl von Verlusthöhen werden nun aufsummiert und bilden mit ihrer Wahrscheinlichkeit (Häufigkeit) einen Punkt in der Gesamtverlustverteilung.

Schritt 3:

Der Schritt 2 wird so oft wiederholt, bis sich eine genügend genaue Kurve für die Gesamtverlust-Verteilung ergibt.

Literatur

- [Alex03] Alexander, Carol: Operational Risk. Ed. Carol Alexander. London: Pearson Education Ltd., 2003.
- [Anhb04] Standards Australia / New Zealand: HB 221:2004, Handbook Business Continuity Management. Sydney: Standards Australia International, 2004.
- [Asnz04] Australian / New Zealand Standard: Risk Management, AS/NZS 4360:2004. Sydney: Standards Australia International Ltd, 2004.
- [Bein03] Beinert, Claudia: „Bestandesaufnahme Risikomanagement“. In Risiko-management und Rating. Hrsg. Peter Reichling. Wiesbaden: Gabler, 2003, 32-41.
- [Bisf04] Bank for International Settlements: International Convergence of Capital Measurement and Capital Standards – A Revised Framework. Basel: Bank für Internationalen Zahlungsausgleich, 2004.
- [Bisr06] Bank for International Settlements: International Convergence of Capital Measurement and Capital Standards – A Revised Framework Comprehensive Version. Basel: Bank für Internationalen Zahlungsausgleich, 2006.
- [Biss03] Bank for International Settlements: Sound Practices for the Management and Supervision of Operational Risk. Basel: Bank für Internationalen Zahlungsausgleich, 2003.
- [Bisw01] Bank for International Settlements: Working Paper on Regulatory Treatment of Operational Risk. Basel: Bank für Internationalen Zahlungsausgleich, 2001.
- [Bitr04] Biri, Kurt und Giampaolo M. Trenta: Corporate Information Security Governance im schweizerischen Privatbankgeschäft. Diplomarbeit Executive MBA. Universität Zürich, 2004.
- [Bleic92] Bleicher, Knut: Das Konzept Integriertes Management. Frankfurt: Campus, 1992.
- [Böck04] Böckli, Peter: Schweizerisches Aktienrecht. Zürich: Schulthess, 2004.
- [Brod08] Brodtkin, Jon: Gartner: Seven cloud-computing security risks. www.infoworld.com, 2008.

- [Brüh01] Brühwiler, Bruno: Unternehmensweites Risk Management als Frühwarnsystem. Bern: Haupt, 2001.
- [Brüh03] Brühwiler, Bruno: Risk Management als Führungsaufgabe. Bern: Haupt, 2003.
- [Brüh11] Brühwiler, Bruno: Risk Management als Führungsaufgabe. ISO 31000 mit ONR 49000 wirksam umsetzen. Bern: Haupt, 2011.
- [Bsig08] BSI: BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Version 2.0. Bonn: BSI, 2008.
- [Bsim08] BSI: BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.5. Bonn: BSI, 2008.
- [Bsir08] BSI: BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5. Bonn: BSI, 2008.
- [Buch04] Buchta, Dirk, Marcus Eul und Helmut Schulte-Croonenberg: Strategisches IT-Management. Wiesbaden: Gabler, 2004.
- [Buco06] BS 25999-1:2006: Business continuity management – Part 1: Code of practice. British Standards Institution, 2006.
- [Busp07] BS 25999-2:2007: Business continuity management – Part 2: Specification. British Standards Institution, 2007.
- [Cobc00] ISACF: CobiT – Detailed Control Objectives. 3rd ed. Rolling Meadows: Information Systems Audit and Control Foundation IT Governance Institute, 2000.
- [Cobf00] ISACF: CobiT – Framework. 3rd ed. Rolling Meadows: Information Systems Audit and Control Foundation IT Governance Institute, 2000.
- [Cobm00] ISACF: CobiT – Management Guidelines. 3rd ed. Rolling Meadows: Information Systems Audit and Control Foundation IT Governance Institute, 2000.
- [Cosa02] Committee of Sponsoring Organizations of Treadway Commission (COSO): Internal Control - Integrated Framework. New York: AICPA, 2002.
- [Cose04] COSO: Enterprise Risk Management – Integrated Framework, Framework. New York: AICPA, 2004.
- [Delt03] Deloitte Touche Tohmatsu: 2003 Global Security Survey. www.deloitte.com, 2003.

- [Foll07] Follmann, David: Basel II und Solvency II. Saarbrücken: VDM Verlag Dr. Müller, 2007.
- [Dölk06] Dölker, Annette: Das operationelle Risiko in Versicherungsunternehmen. Karlsruhe: Verlag Versicherungswirtschaft GmbH, 2006.
- [Dübe04] Dübendorfer, Thomas, Arno Wagner und Bernhard Plattner: „An Economic Damage Model for Large-Scale Internet Attacks“, in Proceedings of 13th IEEE International Workshops on Enabling Technologies (WET ICE 2004); Enterprise Security (ES), IEEE, 2004.
- [Dübe05] Dübendorfer, Thomas: Impact Analysis, Early Detection and Mitigation of Large-Scale Internet Attacks. Dissertation Swiss Federal Institut of Technology Zürich, Zürich: ETH, 2005.
- [Dunn04] Dunn, Myriam und Isabelle Wigert: International CIIP Handbook 2004. Hrsg. Andreas Wenger und Jan Metzger. Zürich: Center for Security Studies at ETH Zurich, 2004.
- [Eber03] Eberhardt, Otto: Gefährdungsanalyse mit FMEA. Renningen: Expert Verlag, 2003.
- [Encr09] ENISA: Cloud Computing - Benefits, risks and recommendations for information Security. European Network and Information Security Agency (ENISA), 2009.
- [Erns04] Ernst & Young: Global Information Security Survey 2004. www.ey.com, 2004.
- [Gaul10] Gaulke, Markus: Praxiswissen COBIT Val-IT – Risk-IT, 1. Auflage. Heidelberg: dpunkt.Verlag, 2010.
- [Glei05] Gleissner, Werner und Frank Romeike: Risikomanagement. München: Haufe, 2005.
- [Glei08] Gleissner, Werner: Grundlagen des Risikomanagements im Unternehmen. München: Verlag Franz Vahlen, 2008.
- [Grue04] Grütter, Matthias: IT-Risikomanagement in Kombination mit IT-Sicherheitsstandards. Diplomarbeit Nachdiplom Informatik-Sicherheit. Hochschule für Wirtschaft Luzern, 2004.
- [Hamm93] Hammer, Michael and James Champy: Reengineering the Corporation. New York: HarperCollins Publishers, 1993.
- [Isoa09] ISO/IEC 31010:2009: Risk management – Risk assessment techniques. International Organization for Standardization, 2009.

- [Isob12] ISO 22301:2012: Societal security – Business •continuity management systems – Requirements. International Organization for Standardization, 2012.
- [Isoc12] ISO/IEC 2nd WD 27017: Guidelines on Information security controls fort he use of cloud computing services based on ISO/IEC 27002. International Organization for Standardization, 2012.
- [Isod08] ISO/IEC 24762:2008: Guidelines for information and communications technology disaster recovery services. International Organization for Standardization, 2009.
- [Isog08] ISO/IEC 38500:2008: Corporate governance of information technology. International Organization for Standardization, 2008.
- [Isog12] ISO DIS 22313: 2012: Societal security – Business continuity management systems – Guidance. International Organization for Standardization, 2012.
- [Isoh11] ISO/IEC DIS 27014:2011: Governance of information security. International Organization for Standardization, 2011.
- [Isoi03] ISO/IEC 1st CD 13335-1: 2003. Information technology – Management of ICT security – Part 1: Concept and models for ICT security management. International Organization for Standardization, 2003.
- [Isom05] ISO/IEC 27001:2005: Information Security Management System-Requirements. International Organization for Standardization, 2005.
- [Isoo09] ISO/IEC 27000:2009: Information security management systems-Overview and vocabulary. International Organization for Standardization, 2009.
- [Isop07] ISO/PAS 22399:2007: Societal security – Guidelines for incident preparedness and operational •continuity management. International Organization for Standardization, 2007.
- [Isor09] ISO 31000:2009: Risk management – Principles and guidelines. International Organization for Standardization, 2009.
- [Isov09] ISO/IEC Guide 73:2009: Risk management – Vocabulary. International Organization for Standardization, 2009.
- [Itgb03] IT Governance Institute: Board Briefing on IT Governance, 2nd Edition. Rolling Meadows: IT Governance Institute, 2003.

- [Itgf07] IT Governance Institute: CobiT 4.1, Framework, Control Objectives, Management Guidelines, Maturity Models. Rolling Meadows: IT Governance Institute, 2007.
- [Itgi06] IT Governance Institute: CobiT Mapping, Overview of International IT Guidance, 2nd Edition. Rolling Meadows: IT Governance Institute, 2004.
- [Itgr09] IT Governance Institute: The Risk IT Framework, Exposure Draft. Rolling Meadows: IT Governance Institute, 2009.
- [Itgs06] IT Governance Institute: IT Control Objective for Sarbanes-Oxley, 2nd Edition. Rolling Meadows: IT Governance Institute, 2006.
- [Itgv08] IT Governance Institute: The Val IT Framework 2.0. Rolling Meadows: IT Governance Institute, 2008.
- [Itse03] Macfarlane, Ivor and Collin Rudd: IT Service Management. Ein Begleitband zur IT INFRASTRUCTURE LIBRARY. Earley Reading: itSMF Ltd., 2003.
- [Itss08] Meijer, Machteld, Mark Smalley and Sharon Taylor: ITIL V3 and ASL _ Sound Guidance for Application Management and Application Development. Norwich, Norfolk: Office of Government Commerce, 2009.
- [Jauc88] Jauch, Lawrence R. and William F. Glück: Business Policy and Strategic Management, Fifth Edition. New York: McGraw Hill, 1988.
- [Jori07] Jorion, Philippe: VALUE AT RISK, 3rd Edition. New York: McGraw-Hill, 2007.
- [Kapl01] Kaplan, Robert S. and David P. Norton: The Strategy Focused Organization. Boston: Harvard Business School Press, 2001.
- [Lehm02] Lehmann Beat: Verantwortung und Haftung für die IT-Sicherheit. Luzern: FHZ-IWI, 2002.
- [Leve95] Leveson, Nancy G.: Safeware, System Safety and Computers. New York: Addison-Wesley, 1995.
- [Mose02] Moser, Ulrich: Der IT-Ernstfall - Katastrophenvorsorge. Rheinfelden/Schweiz: BPX, 2002.
- [Nisc02] NIST: Contingency Planning Guide for Information Technology Systems. Washington DC: U.S. Department of Commerce, 2002.

- [Nisc10] NIST: Contingency Planning Guide for Federal Information Technology Systems, NIST Special Publication 800-34 Rev. 1. Washington DC: U.S. Department of Commerce, 2010.
- [Nide11] NIST: The NIST Definition of Cloud Computing. Washington DC: U.S. Department of Commerce, 2011.
- [Nicc11] NIST: Draft Cloud Computing Synopsis and Recommendation. Washington DC: U.S. Department of Commerce, 2011.
- [Obli10] OR: Schweizerisches Obligationenrecht. Zürich: Orell Füssli, 2010.
- [Oenb05] Oesterreichische Nationalbank: Management des operationellen Risikos. Wien: QeNB, 2005.
- [Oecd04] OECD: OECD Principles of Corporate Governance. Paris: OECD Publications, 2004.
- [Onno08] ONR 49002-3:2008: Risikomanagement für Organisationen und Systeme; Teil 3: Leitfaden für das Notfall-, Krisen- und Kontinuitätsmanagement. Wien: Österreichisches Normungsinstitut, 2008.
- [Onri08] ONR 49001:2008: Risikomanagement für Organisationen und Systeme - Risikomanagement. Wien: Österreichisches Normungsinstitut, 2008.
- [Piaz02] Piaz, Jean-Marc: Operational Risk Management bei Banken. Zürich: Versus Verlags AG, 2002.
- [Prok08] Prokein, Oliver: IT-Risikomanagement. Wiesbaden: Gabler, 2008.
- [Röss05] Rössing von, Rolf: Betriebliches Kontinuitätsmanagement. Bonn: mitp-Verlag, 2005.
- [Romi03] Romeike, Frank: „Risikoidentifikation und Risikokategorien.“ In Erfolgsfaktor Risikomanagement. Hrsg. Frank Romeike und Robert B. Finke. Wiesbaden: Gabler, 2003, S. 165 ff.
- [Rome03] Romeike, Frank: „Bewertung und Aggregation von Risiken.“ In Erfolgsfaktor Risikomanagement. Hrsg. Frank Romeike und Robert B. Finke. Wiesbaden: Gabler, 2003, S. 183 ff.
- [Roml04] Romeike, Frank: Lexikon Risikomanagement. Köln: Wiley-VCH Verlag GmbH & Co. KGaA, 2004.
- [Rome09] Romeike, Frank und Peter Hager: Erfolgsfaktor Risikomanagement 2.0. Wiesbaden: Gabler, 2009.

- [Rüeg02] Rüegg-Stürm, Johannes: Das neue St. Galler Management-Modell. Bern: Haupt, 2002.
- [Scod02] Swiss code of best practice for corporate governance. Zürich: economicsuisse, 2002.
- [Sonn06] Sonnenreich, Wes, Jason Albanese and Brouce Stout: "Return On Security Investment (ROSI) – A Practical Quantitative Model." Journal of Research and Practice in Information Technology, Vol. 38, February 2006, 55-66.
- [Stor96] Storey, Neil: Safety Critical Computer Systems. London: Prentice Hall, 1996.
- [Swan96] Swanson, Marianne und Marianne Gutmann: NIST 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems. Washington DC: U.S. Department of Commerce, 1996.
- [Ulri01] Ulrich, Hans und Gilbert J. B. Probst: Anleitung zum ganzheitlichen Denken und Handeln. 3. erw. Auflage, Bern: Haupt, 2001.
- [Vese81] Vesely, W.E. und Andere: Systems and Reliability Research Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission: Fault Tree Handbook. Washington, D.C.: U.S. Government Printing Office, 1981.
- [Witt10] Wittmann, Edgar:, „Organisation des Risikomanagements im Siemens Konzern“, in Risk Controlling in der Praxis. Hrsg. Henner Schienbeck. Zürich: Verlag Neue Zürcher Zeitung, 1999.
- [Wolk07] Wolke, Thomas: Risikomanagement. München: Oldenburg Wissenschaftsverlag, 2007.
- [Witb06] Witt, Bernhard C.: IT-Sicherheit kompakt und verständlich. Edition <kes>, Wiesbaden: Vieweg, 2006.
- [Witb10] Witt, Bernhard C.: Datenschutz kompakt und verständlich, 2. Auflage. Edition <kes>, Wiesbaden: Vieweg, 2010.

Abkürzungsverzeichnis

AktG	Aktiengesetz
BS	British Standard
BSC	Balanced Scorecard
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
BSI	British Standards Institution (UK)
CC	Common Criteria
CEO	Chief Executive Officer
CERT®	Computer Emergency Response Team (Carnegie Mellon University)
CERT®/CC	Computer Emergency Response Team / Coordination Center (Carnegie Mellon University)
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CISO	Chief Information Security Officer
CLO	Chief Legal Officer
CobiT	Control Objectives for Information and related Technology (Information Systems Audit and Control Association)
COBIT®	
COO	Chief Operation Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRAMM	Centre for Information Systems Risk Analysis und Management Method
CRO	Chief Risk Officer
CSF	Critical Success Factor
CSO	Chief Security Officer
EBK	Eidgenössische Bankenkommission (Schweiz)
ETA	Event Tree Analysis (Ereignisbaum-Analyse)
FINMA	Eidg. Finanzmarktaufsicht
FMEA	Failure Modes and Effects Analysis (Fehler-Effekt- und Ausfall-Analyse)
FMECA	Failure Modes, Effects and Criticality Analysis

FTA	Failure Tree Ananlysis (Fehlerbaum-Analyse)
GL	Geschäftsleitung
HGB	Handelsgesetzbuch (Deutschland)
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
ISACA®	Information Systems Audit and Control Association®
ISMS	Informationssicherheits-Management-System
ISO	International Standards Organisation
IT	Informations-Technologie (Information Technology)
ITGI	IT Governance Institute®
ITIL®	IT Infrastructure Library (Office of Commerce)
ITSEC	Information Technology Security Evaluation Criteria
KCI	Key Control Indicator
KGI	Key Goal Indicator
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPI	Key Performance Indicator
KRI	Key Risik Indicator
MAO	Maximum Acceptable Outage
MTPD	Maximum Tolerable Period of Disruption
Mil Std	Military Standards (USA)
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failures
MTTR	Mean Time To Repair
OR	Schweizerisches Obligationenrecht
PDCA	Plan Do Check Act
PCCIP	President's Commission on Critical Infrastructure Protection
RM	Risikomanagement
ROSI	Return on Security Investments
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SOX	Sarbanes-Oxley Act (USA)
SWOT	Strength, Weaknesses, Oportunities, and Threats
SSL	Secure Socket Layer
VR	Verwaltungsrat

Stichwortverzeichnis

A

Abschlussprüfer-Richtlinie 78, 79, 94
Aggregation.. 27-29, 297, 425
Akkreditierung..... 347
Akteure..... 329
AktG, Aktienrecht..... 79
Akzeptanz 62, 118, 179, 234, 249, 319
Akzeptanz Restrisiko 64
Akzeptanz-Aussagen 244
Akzeptanz-Entscheide.... 250
Akzeptanz-Kriterien.. 47, 242
Alarmierung 335, 336
Analyse
 Bottom-up 57
 Impact 54
 qualitativ 57
 quantitativ 57
 Schwächen 52
 Schwachstellen 52
 Top-down 57
Analysegebiet 52
Anforderungsanalyse..... 363
Angebot Dienstleister..... 376
Angriffsbaum-Analyse 263
Angriffsmittel 39
Annual Loss Exposure.... 276
Anspruchsgruppe .. 3, 56, 75, 76, 109, 117, 321, 323
Anwendungsbereich 233
Applikations-Server 181
Assessment-Methode..... 232
Asset 9, 46, 143
Asset-Liste 235
Asset-Register..... 397
Attacke 355
Audit-Komitee..... 82, 170

Auditoren 65
Aufsichtsrat 77
Ausbildung..... 321
Ausfallzeit-Verlust 280
Ausführungsbestimmung 132, 175, 177
Ausweich-Plan 311
Ausweichstandorte . 333, 339
Auswirkung..... 10
Authentisierungs-Methode 180

B

Backtracking 256
Balanced Scorecard 120, 282, 297
 Corporate Scorecard... 124
 Dimension..... 121
 Grundsätze 122
 Konzept..... 121
 Perspektiven 120
Bankgeheimnis 98, 104
Basel II 78, 83
Baseler Ausschuss 84
Baseline Security Control 187
Baseline Security Standard 183, 241
Basisindikatoransatz 85
Basisschutz..... 188
Basis-Sicherheitschecks.. 223
BCM-Leistung..... 323
BCMS-Anforderungen 319
BCM-Standard
 BS259999-1:2006..... 309
 BS259999-2:2007..... 309
Bedrohung..... 11, 25, 39, 52, 143
Bedrohungsanalyse 51

Bedrohungsauswirkung . 235	BSI 225
Bedrohungsliste 39, 52	BSI IT-Grundschutz-
Bedrohungsabsicht 39	Kataloge 183
Bedrohungsumfeld 53	BSI Standards 221
Eskalations-Begriffe	Bundes-Datenschutzgesetz
Katastrophe 349	(BDSG) 96
Krise 349	Business Case 284
Notfall 349	Business Continuity
Behandlungs-Option 62	Management 309
Berichterstattung 91	Business Continuity Plan
Best Practices 53, 78, 162,	309
188, 206	Business Model for
Betriebsgewinn 23	Information Security ... 212
Betriebskontinuitäts-Plan	Business-Impact-Analyse
311	(BIA) 326
Betriebskosten 277	
Betriebs-Owner 301	
Betroffene 9	
Betrugs-Risiko 24	
Beurteilung der Lage 337	
Bewältigungs-Optionen ... 61	
Bewältigungs-Prioritäten 244	
Bewertung	
kardinal 21	
ordinal 21	
Bewertungskriterien 47, 210,	
232	
Bewertungsmetriken 288	
Bewilligungs- und	
Anordnungsbefugnis... 166	
Bewusstseinsbildung 322	
BIA 326	
BMIS 212	
Board of Directors 77	
Bonitätsprüfung 97	
Boolesche Algebra 260	
Börsenkotierung 91	
Bottom-up-Analyse 57	
Bottom-up-Suche 59	
Bottom-up-Verfahren 239	
Branche ... 21, 37, 38, 39, 188	
Brandrisiko 18	
BS 7799-2 199	
	C
	Chance .. 2, 3, 10, 12, 36, 55,
	61, 68, 73, 102, 107, 117,
	119, 123, 124, 138, 242
	Checks and Balances 102
	Chief-Revisor 170
	Chief Executive Officer . 101,
	170
	Chief Financial Officer .. 101,
	170
	Chief Information Officer
	 101, 164, 165, 170
	Chief Information Security
	Officer (CISO) 101, 164,
	165, 168, 170, 301
	Chief Legal Officer 170
	Chief Operation Officer 101,
	170
	Chief Risk Officer ... 101, 170
	Cloud Computing Interface
	 181
	Cloud Sourcing 384, 386
	Cloud Sourcing Lifecycle
	 387
	Cloud-Computing
	Anwendungsbereich... 394

Assets.....	397	Cloud-Sourcing-Lifecycle	403
Backup-Policy	403	Cloud-Sourcing-Vertrag..	386
Benutzungspolicy	384	CobIT.....	92, 183, 212
Betriebsphase	403	Framework	124
Cloud Sourcing Strategie		IT-Werte-Management	218
.....	388	Prozessbereiche	213
Cloud-Sourcing		Rahmenwerk	282
Management.....	392	Risiko-Beurteilung	220
Commodity	404	Version 4.1.	215
Compliance	404	Wasserfall-Modell	216
Compliance-Risiken....	384	Würfel.....	215
Deployment-Modelle..	383	CobIT 4.1.....	213
Evaluationsphase	396, 399	Cobit 5 – Framework	212
Geschäfts-Impact	401	CobIT-Regelwerk	224
Informationssicherheits-		Code of best Practice	82
Risiken.....	384	Code of Practice for	
IT-Sicherheitskonzept.	387	Information Security	
Kontext.....	394	Management	205
Kunde.....	381, 384	Committee of Sponsoring	
Risiko-Analyse	401	Organizations of the	
Risiko-Assessment	396,	Treadway Commission	
400		(COSO).....	8
Risiko-Auswirkungen .	401	Common Criteria (CC) ...	190
Risikomanagement	393	Compliance.....	150, 154, 160
Schwachstellenliste.....	399	Compliance-Risiken....	11, 98
Serviceabkommen	385	Computer Emergency	
Skaleneffekt	404	Response Team (CERT)	
Systembeschreibung...	395		350
Vertragsentwicklung...	391	Conditional Value-at-Risk	30
Vertragsphase	401	Content-Filter	183
Zertifizierung	403	Continuity of Operations	
Zugriffsrechte.....	386	Plan.....	311
Cloud-Computing.....	97	Control Objectives for	
Charakteristik	382	Information and related	
Service Modell	382	Technology (CobIT)	92
Provider.....	381	Corporate Governance....	76,
Virtualisierung.....	380	82, 91, 111, 155	
Prinzip und Definitionen		COSO	
.....	379	Komponenten	92
Konsumenten.....	381	Standard	91
Cloud-Provider	381		
Cloud-Service-Provider ..	385		

COSO Internal Control- Integrated Framework	194
CRAMM	49, 250
Asset Model	253
Asset Types	251
Asset Valuation	252
Backtracking	256
Bedrohungs-Arten	251
Enduser Service	253
Impact Type	256
Massnahmenkatalog ...	251
Profil	251
Review	256
Risiko-Management- Report	256
Risiko-Matrix	251, 252
Schutzobjekt-Gruppe..	255
What-if-Funktion	256
Critical Infrastructure Protection (CIP)	147
Critical Success Factors (CSF)	126
Cyber Space	39

D

Dashboard	65
Datenmaterial	34
Datenschutz	96
Datenschutzbeauftragter ..	98
Datenschutzgesetze ..	97, 104
Datenschutzkommission ..	98
Datenschutzrichtlinie der EU (95/46/EG)	96
Datenschutzvorschriften ..	97
De-facto-Standards	187
Dienstleister	375
Dienstleistungs-Ausfall	55
Disaster Recovery Plan ..	313
Divisions-Kalkulation	281
Dokumentierte Informationen	324, 325

Dringlichkeit	36
Drittländer	97
Due Diligence	371

E

Effektivität	149, 290, 300, 348
Effizienz ..	149, 150, 290, 348
Eidg. Bankenkommission (EBK)	370
Eigenkapital	83, 85
Eigenkapitalrendite	102
Eigenkapitalunterlegung .	35, 87
Eigenkapitalvereinbarung	83
Einführungs- und Inbetriebnahmekosten	277
Einstufung Häufigkeiten	422
Einstufungs-Kriterien	21
Eintrittshäufigkeit	14
Eintrittswahrscheinlichkeit	13, 24
Elastic Compute Cloud...	404
Endbenutzer-Service	253
Endbenutzer-Services	398
End-to-end-Paradigma ...	385
End-to-end- Risikobetrachtung	401
Entwicklung oder Beschaffung	363
Ereignisbaum-Analyse	264
Auslösenden Ereignis .	264
Brandschutz	265
Folgeereignis	264
Wahrscheinlichkeit Folgeereignis	265
Ereignisfall	332
Ereignis-Szenarien	349
Erklärung zur Anwendbarkeit	204

Erlaubnisvorbehalt 97
 Erwartet
 Schadenshöhe, Verlust. 14
 Erwartungswert..... 276, 290
 Eskalations-Ebenen 351
 Eskalations-Kriterium 341
 Eskalations-Stufen 354
 Europäische Richtlinie
 Datenschutz 96
 EuroSOX 78, 94
 Evakuationsanordnung .. 336
 Event Tree Analysis (ETA)
 264
 Ex ante 19, 50
 Ex post 19, 50
 Executive Management 77
 Expected Shortfall 28
 Experten-Befragung 239
 Exploit 53, 66
 Exponential-Verteilung 32
 Extremwert-Theorie 34

F

Fabrikations- und
 Geschäftsgeheimnis..... 99
 Failure Mode and Effects
 Analysis (FMEA) 257
 Failure Mode Effect and
 Criticality Analysis
 (FMCEA)..... 257
 Fault Tree Analysis (FTA)
 259
 Fehlerbaum-Analyse..... 259
 Ausfallkategorien 263
 Basis-Ereignis..... 260
 Cut Set 260
 Minimal Cut Set 260
 Single Point of Failures
 263
 Top-Ereignis..... 259
 Wahrscheinlichkeit 261

Fehlermöglichkeits- und
 Einflussanalyse..... 257
 Fernmeldegeheimnis 98,
 104
 Finanzrisiken..... 409
 FINMA 84, 370
 Firewall-System..... 183
 Firmenspezifischer Standard
 188
 First Cut..... 363, 421
 Risiko-Analyse..... 363
 Folgen 11
 Formular für First Cut.... 421,
 420
 Fortgeschrittene
 Messansätze 85
 Frameworks und
 Managementsysteme .. 133
 Frühwarnsystem 66, 78
 Führung..... 317
 Führungs- und
 Kontrollinstanz..... 173
 Führungsaspekte 107
 Führungsinstrument 173,
 175
 Führungspyramide 173,
 174
 Führungsrhythmus 335
 Führungssystem..... 110
 Funktionen..... 340

G

Gartner Group 371
 Gegenstand..... 46
 Geographische Standorte
 321
 Gesamtrisiko 27
 Gesamt-RM-Prozess 296,
 296, 298
 Gesamtschadensverteilung
 32
 Gesamtverlustverteilung... 28

I

- Imageschädigende
 - Kampagnen..... 39
- Image-Verlust..... 100
- Impact 12, 54
 - durchschnittlich 55
 - maximal..... 54
 - statistisch 55
- Impact-Analyse .. 51, 54, 189, 240
- Impact-Arten 238
- Impact-Einschätzung 359
- Impact-Höhen..... 238
- Impact-Kriterien..... 210
- Impact-Stufen..... 360
- Incident 334, 350
 - Management-Prozess.. 335
- Incident-Informations-System 353, 354, 355
- Incident-Management ... 181, 348
- Information Security
 - Maturity Model..... 162
- Information Technology
 - Assurance Framework 212
- Informationen 144
- Informations-Asymmetrie 168
- Informations-Einstufung 360
- Informations-
 - Einstufungskriterien.... 417
- Informations-Klassierung 359
- Informationskriterien..... 213, 221, 293
- Informationskriterien-Profil 125
- Informations-Risiken 154, 298, 299
- Informations-Risiko 152, 154
- Informations-
 - Risikomanagement 155, 293, 298
- Informations-RM-Prozess 295
- Informations-Sicherheit . 150, 151, 152, 154, 156
 - Governance..... 160
 - Maturity-Modell..... 164
- Informationssicherheits-Architektur .. 179, 180, 182
- Informationssicherheits-Ausführungsbestimmungen 177
- Informationssicherheits-Governance. 155-157, 159, 160, 293
- Informationssicherheits-Politik 175
- Informationssicherheits-Risiken..... 175, 227, 295
- Informationssicherheits-Standards..... 179
- Informationssicherheits-Weisungen 177
- Infrastruktur 326
- Sourcing Management.... 377
- Integriertes
 - Managementsystem ... 135, 136
- Integrität..... 11, 41, 100, 125, 144, 148, 149, 153, 166, 181, 359, 360
- Interaktionen 74, 341
- Interne Kontrolle 81, 91
- Internen Kontrollsystem... 94
- Interner Bemessungs-Ansatz 86
- Internes Audit 170
- Internes Datennetz 181
- Internes Kontroll-System.. 66
- Intrusion Detection 181, 183
- Investitionskosten..... 277

Investitions-Management	284	IT-Grundschutz-Kataloge	221
ISMS		ITIL V3	191, 387
Phase "act"	203	ITIL-Applikations-Management-Prozess..	361
Phase "check"	203	ITIL-Servicemanagement-Prozess	361
Phase "do"	202	IT-Infrastruktur	350
Phase "plan"	201	IT-Investitionen	283
ISMS-Politik.....	175, 177	IT-Kontinuität.....	310
ISMS-Standard.....	197	IT-Notfall-Plan	314, 338, 347, 349
ISO 31000:2009.....	8	Eskalations-Ebene.....	351
ISO Guide 73:2009	8	Funktionsstellen.....	352
ISO Guide 83	136, 315	Kommunikations-System	352
ISO/IEC	196	Vulnerability und Incident-Management	352
17799:2005	196	IT-Outsourcing	369
27001:2005 ..	196, 198, 199	IT-Owner	167
27002:2005 ..	196, 205, 206, 207, 209	IT-Prozess	218
27005:2008	196	IT-Prozessdomänen.....	214
TR 13335-3	198	IT-Prozesse.....	75, 167, 213
ISO/IEC 15408 (CC / ITSEC)	190	IT-Ressourcen	213
ISO/IEC 17799	183, 205	IT-Risiken 154, 227, 293, 413	
ISO/IEC 17799:2000	153, 205, 209	Schadensmetrik.....	424
ISO/IEC 20000	192	IT-Risiko.....	39
ISO/IEC 27001		Modellvorstellung	143
Zertifizierungen	199	IT-Risikomanagement 2, 143	
ISO/IEC 27005:2011	209	293	
ISO/IEC 31010	47	IT-RM-Prozess.....	166
ISO/IEC2700x-Familie	197	IT-Sicherheit.....	154
IT Contingency Plan.....	314	IT-Sicherheits-Administratoren	164
IT Governance Institut	92	IT-Sicherheitskonzept.....	300
IT Infrastructure Library .	191	detaillierte Betriebsfassung	393
IT Infrastructure Library (ITIL) ...	191, 192, 199, 361	Grobfassung.....	393
IT-Administratoren .	164, 167	IT-Sicherheitskosten	280, 289
ITAF.....	212	IT-Sicherheits-Politik	133
IT-Architektur	188	IT-Sicherheits-Prozess	222
IT-Betriebs-Risiko	24		
IT-Governance 155-159, 225, 293			
IT-Governance Institut ...	158		

IT-Strategie 159, 303
 IT-Strukturanalyse 222
 IT-Support-Funktionen... 312
 IT-System 167
 Definition 227
 IT-System Owner..... 101
 IT-System Ownership..... 300

K

Kapitalgeber..... 3
 Kapitalmarkt 76
 Katastrophe 311, 334, 343,
 351
 Katastrophenstab 334
 Kategorien (Risiken) 37
 Kennzahlen..... 35, 348
 Key Goal Indicator (KGI)
 126
 Key Performance Indicator
 (KPI) 126
 Key-Risk-Indikatoren..... 35
 Klassierung
 Einstufungskriterien.... 360
 Klassifizierung Regelwerke
 194
 Kommitment 321
 Kommunikation 45, 249,
 321, 322
 Kommunikationseinrichtung
 en..... 324
 Kommunikationskonzept. 45
 Kommunikations-Matrix
 233, 234
 Kommunikations-System . 45
 Kompatibilität RM-Prozesse
 296
 Konfidenz-Niveau..... 31
 Konfigurations-Management
 367
 Konsequenz 10, 12, 18
 Konstruktions-FMEA 258
 Konsultation..... 45, 249

Kontaktlisten 339
 Kontext....9, 46, 47, 233, 318
 Kontextbeschreibung 231
 Kontext-Elemente 47
 Kontinuierliche
 Verbesserungen 320
 Kontinuität
 Analyse..... 317, 356
 Pläne..... 310
 Reporting..... 317, 356
 Risiken 316
 Überprüfung 317, 356
 Überwachung 317, 356
 Ziele..... 331
 Kontinuitäts-Anforderungen
 329
 Kontinuitäts-Kultur 342
 Kontinuitäts-Management
 318
 Kontinuitäts-Prozess 317
 Kontinuitäts-Risiken 319
 Kontinuitäts-Sicherung ... 311
 Kontinuitäts-Ziele 322
 KonTraG 78
 Kontrollen 168
 Kontrollfunktion 100
 Kontrollsystem..... 82
 Kontroll-Ziel..... 216
 Korrelation 27, 58, 297
 Korrelationskoeffizient 27
 Kosten
 Arten..... 278
 Risikobewältigung 273
 Unternehmensrisiken . 273
 Kosten-/Nutzen..... 62
 Kosten-/Nutzen-Abwägung
 247
 Kosten-/Nutzen-Nachweise
 273
 Kostenabwägung..... 229
 Kostengruppen 278
 Kostenrechnung 278
 KPI..... 65

KPMG 199
 Kreditkarten 99
 Kreditzinssatz 83
 KRI 65
 Krise 334, 351
 Krisenbewältigung 344
 Krisenmanagement 334
 Krisensitzungs-Räume 341
 Krisenstab 334, 353
 Kritische Geschäftsfunktion
 331
 Kritische Geschäftsprozesse
 339
 Kritische Infrastruktur 147
 Kritischer Zustand 334
 Kryptographie 181

L

Lagebericht 79
 Lebenszyklus .. 228, 359, 361
 Leistungs-Messung 161
 Lieferobjekt 364
 Lifecycle 359
 Lifecycle-Modell 361
 Lifecycle-Phase 233
 Linien-Manager 101
 Log-Normal-Verteilung 32

M

Management
 Ansatz 73
 Bericht 88
 Konzept 107
 Prozesse 73, 74
 System 73, 87
 Management-Konzept 108
 Management-Prozesse 75,
 135, 188
 Management-System. 73, 134
 Marktdisziplin 84

Marktrisiken 24, 411
 Marquer 343
 Massnahmen 1, 9, 144
 Entscheide 13, 24
 Informationsschutz 419
 Kosten 61, 277
 Nutzen 281
 Rezept 360
 Strategien 317, 356
 Massnahmenbibliothek .. 256
 Massnahmen-Kosten 62
 Massnahmenkosten-Metrik
 298
 Maximum Acceptable
 Outage (MAO) 327
 Maximum Tolerable Period
 of Disruption (MTPD) 327
 Mechanismus 179
 Medien 99
 Meldedienste 322
 Messgrösse 115
 Mindestkapitalanforderung
 84
 Mission 112
 Modell
 Systemisches Modell 2
 Monitoring-Prozess 160
 Monte-Carlo
 Methode 28, 298
 Simulation 428

N

Nachlaufende Indikatoren 36
 Nachweispflicht 342
 Nebeneffekte
 von Massnahmen 274
 Netto-Verlustreduktion... 275
 NIST 379
 NIST 800-14 193
 NIST Special Publication
 800-18 227
 Non-Konformitäten 320

Normalbetrieb..... 330
 Normalverteilung..... 32
 Normatives Management
 107, 110
 Normen 46
 Notarbeitsplätze..... 339
 Notbetrieb..... 327
 Notbetriebsdauer 327
 Notfall..... 311, 334, 338, 339
 Notfalldokumentation 341
 Notfall-Informationen-System
 354
 Notfall-Instanz 355
 Notfall-Kommunikations-
 System 353
 Notfallorganisation . 339, 340
 Notfall-Plan 54
 Notfall-Reaktion..... 311, 317,
 336, 354
 Notfallstab..... 334
 Notfallszenario..... 343

O

Oberaufsicht 80
 Objekt (Risiko) 52, 143
 Obligationenrecht..... 79
 Offshore Outsourcing 371
 ONR 49000:2008 ff 8
 Operational Level
 Agreement..... 385
 Operational Service
 Lifecycle 392
 Operational Value-at-Risk 31
 Operationalisierung..... 119
 Operationelles Risiko 85
 Operative Ebene..... 109
 Operatives Management
 107, 130
 OR
 Artikel 663b..... 80
 Artikel 716a 80
 Artikel 728a/b 81

Ordinalskala..... 21, 50
 Ordnungsgemässe
 Geschäftsführung..... 370
 Organhaftung..... 80
 Organisation 79
 Organisations- /
 Betriebsrisiko 414
 Organisations-Einheit 37
 Organisations-Konzept... 112
 Organisatorische
 Massnahmen . 98, 105, 245
 Outsourcing 369
 Audit-Mechanismen.... 370
 Dienstleister 370
 Evaluation und Auswahl
 374
 Gartner-Empfehlung... 371
 IT-RM-Prozess 371
 Lifecycle 371
 Sicherheitskonzept 372
 Sicherheits-Management
 371
 Sourcing-Management 375
 Strategie..... 373
 Vertrag..... 370
 Vertragsentwicklung... 374
 Outsourcing-Partner 370
 Ownership 101, 270
 Ownership-Prinzip 167

P

Parametrisierungen..... 135
 Partnerschaft 375
 Passwort-Authentisierung
 180
 Patch..... 355
 Patch-Verteilung 181
 Payment Card Industries 188
 PDCA-Zyklus . 196, 309, 325,
 349, 403
 Performance Management
 212

Performance-Indikatoren
 65, 282
 Personal 326
 Personalrisiko 416
 Personenbezogene Daten 98
 Persönlichkeitsrechte 96
 Plan-Aktivierung 338
 Plan-Do-Study-Act-
 Lernzyklus..... 198
 Pläne 132, 305, 334
 Planung 321
 Plattform-Owner..... 301
 Policies 114
 Policy..... 131, 182, 305
 Portfolio-Management.... 284
 Postgeheimnis..... 98, 104
 President's Commission on
 Critical Infrastructure
 Protection (PCCIP). 147
 Principal/Agent-Situation 168
 Prinzip der Wesentlichkeit
 300
 Privatsphäre 96
 Problembehandlung..... 352
 Problemerkfassung... 335, 336
 Problemerkennung..... 355
 Problemlösung..... 355
 Problemlösungs-Phasen. 354
 Problemlösungs-Prozess ... 2,
 67, 48, 352
 Problemsituation..... 353
 Projekt-Risiko..... 165, 413
 Projekt-Vorgehen..... 364
 Projekt-Vorgehens-Methode
 363
 Proxy-Infrastruktur 180
 Prozess-FMEA 258
 Prozess-Owner 351
 Prüfungsausschuss 82, 94
 Prüfungsergebnis..... 79

Q

Qualitätsanforderungen . 228
 Qualitätsmanagement.... 112,
 257, 258
 Qualitätsmangel 55
 Qualitätsmerkmal 375
 Qualitätssicherung.. 263, 367
 Qualitätssystem (ISO
 9001:2000)..... 109, 110
 Quantitative
 Aussagen 273
 Kostendarstellung 273
 Quantitative Indikatoren.. 36

R

Rechtliche Risiken 412
 Rechtsrisiko..... 85
 Recovery Point Objective
 (RPO)..... 329
 Recovery Time Objective
 (RTO) 327
 Regelwerke 187, 195
 Regulativ 111
 Regulator 3, 75, 78, 103, 169,
 324, 339
 Reifegrad (Maturity Level)
 216
 Reporting 66
 Reputation..... 23
 Reputationsrisiken 85, 98
 Request for Proposal..... 390
 Resource Management... 212
 Ressourcen..... 62, 323, 330
 Ressourcen-Gruppen..... 332,
 333
 Ressourcen-Management 161
 Ressourcen-Optimierung 212
 Ressourcen-Sharing 181
 Restrisiken.... 7, 63, 250, 231,
 296
 Akzeptanz 248

- Restwahrscheinlichkeit..... 31
- Return on Security
 - Investments 275
- Richtlinien 98
- Risiken und Chancen 322
- Risiko..... 1, 55
 - Arten..... 38, 411
 - Behandlungs-Optionen
 - 332
 - Bewältigung..... 37, 66
 - Bewertung..... 55, 66, 285
 - Chance 303
 - Einschätzung..... 66
 - Erkennung 66
 - Governance..... 285
 - IT-Risiko 1
 - Konsolidierung 297
 - Reaktion 286
 - Risiko-Definition..... 10
- Risiko- und
 - Sicherheitsorganisation174
- Risiko- und Sicherheits-
 - Politik 132, 174
- Risiko-Affinität 19
- Risiko-Aggregation 27
- Risiko-Akzeptanz..... 118
- Risiko-Akzeptanz-Kriterien
 - 210
- Risiko-Akzeptanz-Linie..... 24
- Risiko-Analyse 43, 48, 50,
 - 189, 238
- Risiko-Analyse
 - Methode 58
 - qualitativ..... 50
 - quantitativ 50
 - semi-quantitativ 50
- Risiko-Appetit 101
- Risiko-Art 25, 37, 40
- Risiko-Assessment 24, 47,
 - 235, 328, 393
- Risiko-Assessment-Methode
 - 47
- Risiko-Assessment-Prozess
 - 330
- Risiko-Aversion..... 19, 133
- Risiko-Behandlung 36, 62
- Risiko-Berechnung 18
- Risiko-Bereitschaft... 19, 101,
 - 133
- Risiko-Bericht..... 66, 88
- Risiko-Bewältigung.... 24, 55,
 - 61, 62
- Risiko-Bewertung 13, 61,
 - 242, 243, 244
- Risiko-Bewertungs-Matrix
 - 18, 19
- Risiko-Bewusstsein..... 45
- Risiko-Ereignisse..... 99
- Risiko-Gebiet 175
- Risiko-Höhen 238
- Risiko-Identifikation .. 25, 48,
 - 235, 237
- Risiko-Indikator 65, 116
- Risiko-Inventar..... 26
- Risiko-Karte..... 24
- Risiko-Katalog.... 25, 53, 305,
 - 304
- Risiko-Kontrolle 102
- Risiko-Kosten 369
- Risiko-Kriterien 319
- Risiko-Kultur 45
- Risiko-Lage..... 56, 374
- Risiko-Management 2, 7, 161
 - Absicht..... 46
 - Prozess ... 37, 43, 108, 229,
 - 297, 355
 - Standard 8
 - Ziel..... 46
 - Zweck..... 46
- Risiko-Matrix 20, 234, 395
- Risiko-Metrik..... 298
- Risiko-Modell 241
- Risiko-Objekt .. 21, 25, 30, 48
- Risiko-Optimierung 212
- Risiko-Organisation 36
- Risiko-Owner 300
- Risiko-Politik..... 47

Risikopolitische Grundsätze	132	Schadensdatenbank.....	26
Risiko-Portfolio	24, 33, 37	Schadens-Einstufungstabelle	21, 23
Risiko-Position	306	Schadens-Ereignis	13, 14, 18, 54, 66, 275, 355
Risikoprioritätenzahl.....	260	Schadens-Folgen.....	334
Risiko-Profil	82	Schadens- Häufigkeitsverteilung ...	33
Risiko-Register	26	Schadens-Höhenverteilung	32
Risiko-Reporting	305	Schadens-Metrik ..	21-23, 298
Risiko-Toleranz.....	25, 115	Schadens-Potential	53
Risiko-Wahrnehmung.	21, 56	Schnittstellen.....	326
Risiko-Ziel	13, 116, 174	Schnittstellen-Definition .	182
Risk Driver	29	Schutzbedarf	223
Risk IT	212, 283, 285	Schutzobjekt	143
Risk Management	212	Schutz-Phase	360
Risk Manager	101	Bearbeitung.....	359
Risk Map	24	Entsorgung	359
Risk Owner.....	101, 300	Entstehung	359
Risk-Indikator	130	Speicherung	359
Risk-Owner	167	Übertragung	359
Risk-Register	25, 240, 246	Schwäche	11, 145, 305
RM-Prozess.....	174	Schwachstelle....	11, 52-54, 145, 154, 241, 242, 252
RM-Prozesse		Verletzlichkeit	11, 53, 145, 255
Schnittstellen.....	298	Schwächen-Analyse....	51, 52
Rollen	321, 340	Schwachstellen	53, 144
Rollenbasiertes Zugriffs- Kontrollsystem	181	Schwachstellen-Analyse ..	52, 208, 240
ROSI	275	Schwachstellen-Katalog....	53
Ansatz.....	289	Schwachstellen-Liste.....	398
Berechnung.....	289	Schweizerisches Obligationenrecht	80
		Scorecard-Ansatz	86
S		Scorecard-Daten	21
Sachrisiken	412	Scores	298
Sarbanes-Oxley Act	90	Scout.....	352
Schaden.....	12, 18	Securities and Exchange Commission	91
Schadendenseintritt	13	Selfassessment	344
Schaden-Einstufungstabelle	22	Service Desk ...	353, 354, 393
Schadens-Ausmass	55		
Schadens-Ausmass, Häufigkeit und Risiko	423, 422		
Schadensauswirkung.....	21		

Service Level Agreement (SLA).....	244, 383
Service-Qualität	334
Shareholder-Value	76
Shewhart	135
Sicherheits-Administratoren	167
Sicherheitsanforderungen	375
Sicherheits-Architektur ...	179
Sicherheits-Bedürfnis.....	181
Sicherheits-Dienste .	180, 183
Sicherheits-Dispositiv	370
Sicherheits-Funktionen...	278
Sicherheits-Infrastruktur ..	183
Sicherheitskonzept .	184, 228
Abnahme.....	166
Aufbau.....	230, 380, 386
Coaching	249
Umsetzung	246
Umsetzungsplan	247
Sicherheits-Niveau	371
Sicherheits-Policy	182
Sicherheits-Politik	133
Sicherheits-Strategie des Dienstleisters.....	375
Sicherheits-Vorschriften .	177
Sicherheits-Zonen.....	181
Sicherheits-Infrastruktur	179
Signatur	181
Single Point of Failure....	260
SLA	301
Sofortmassnahmen	336
Soft-Zertifikat	180
Solvency II	78
Sourcing-Lifecycle	393
Sourcing-Vertrag	372
SOX Section 302.....	92
Section 404.....	91
Spieltheorie	30
SQS.....	199
St. Galler Management Modell	73, 107
Stakeholder ...	3, 75, 109, 117
Standardansatz.....	85, 87
Standard-Regelwerke	187
Stärke.....	305
Statement of Applicability	202, 204
Steering Committee	168
Storage Area Network (SAN)	181
Strategic Alignment	212
Strategie.....	119
Chance	305, 307
Risiko.....	305, 307
Risiko-Position	307
Strategiefindung.....	119
Strategiefindungs-Prozesses	44
Strategien	114, 332
Strategie-Prozess	74, 302, 317
Strategie-Risiken	165
Strategie-Themen.....	333
Strategieumsetzung.....	119
Strategische Aktionen.....	114, 119
Ausrichtung.....	161
Ebene	109
Management	113
Pläne.....	114
Rahmen	113
Stossrichtung.....	305
Ziele.....	114-116
Strategische Aktion.....	305
Strategisches Management	107
Strategy Map ...	120, 121, 305
Sub-Prozesse.....	43, 58
Suche Bottom-up	59
Top-down	59
Support-Prozesse	330

Swiss Code 82
 Swiss TS 199
 SWOT-Analyse. 51, 118, 119,
 303
 System-Architektur 179
 Systemausfall-at-Risk 149
 System-Ausfall-Risiko 299
 Systembeschreibung..... 233
 System-FMEA 258
 System-Lifecycle 359
 System-Modell 280
 System-Optimierung..... 365
 System-Owner 164
 System-Ziel..... 11, 12, 293
 Szenario-Analyse 60, 87, 239

T

Taskforce 353
 Taskforce-Leiter 352, 353
 Taskforce-Mitglied 352
 Technische Massnahme . 245
 Technische und
 organisatorische
 Massnahmen 98
 Technologie-Risiko..... 165
 Tests 320, 343
 Ticket 354
 Top-down-Analyse 58
 Top-down-Suche 60
 Top-Management 319
 Total Cost of Ownership 279
 Tragweite 13, 18, 275
 Training..... 323

U

Überprüfung..... 65
 Übergeordnete Risiko-Art
 299
 Überprüfung 250
 Überprüfungsprozess 84

Übertragungs-Chiffrierung
 375, 269, 360
 Überwachung 62, 65, 250
 Überwachungssystem..... 79
 Übungen 320
 Umsetzungsplan 62, 63, 231,
 247
 Umsetzungssteuerung / -
 Überwachung 337
 Underpinning contracts.. 385
 Unsicherheit..... 9
 Unternehmen
 Modellvorstellung 74
 Oberleitung..... 76, 79
 Unternehmens-Kultur..... 75,
 136, 179
 Unternehmens-Politik. 3, 111
 Unternehmens-Risiken 78
 Unternehmensspezifische
 Standards..... 183
 Unternehmens-Strategie 3,
 301, 306
 Unternehmens-Verfassung
 111
 Unternehmens-Vision..... 111
 unternehmensweiter RM-
 Prozess 108
 Unternehmens-Wert 221
 Unternehmens-Zweck 112
 Unterstützungs-Prozesse . 52,
 74, 75, 303
 US Securities and Exchange
 Commission 91

V

Val IT..... 283
 Val IT 2.0 212
 Value-at-Risk 28, 30, 31
 VAR 31, 298, 425
 Verantwortlichkeiten 247,
 319
 Verbindlichkeit 149

Verbotsprinzip	97
Verfügbarkeit ... 11, 144, 148- 150, 153, 166, 181, 305, 359	
Verletzlichkeiten.....	53
Verlust	13, 275
katastrophale	312
unerwartete	312
Verlust aktueller und potentieller Kunden ...	280
Verluste	
erwartete	34, 299, 312
katastrophale	34, 299
unerwartete	34, 299
Verlustereignis-Typen	89
Verlustverteilungs-Ansatz.	86
Verordnungen.....	98
Versorgungseinrichtungen	326
Versorgungs-Infrastruktur	339
Verteilung	
Gesamtverlust	425
Log-Normal	427
Poisson	427
Verlustranzahl	425
Verluthöhen.....	425
Verteilungsdichtefunktion	32
Vertragspartner	376
Vertraulichkeit . 11, 116, 144, 148, 149, 153, 166, 181, 359, 360	
Verwaltungsrat... 77, 79, 100, 170	
Viren-Schutz.....	181
V-Modell	361, 365
Vollenumeration.....	425
Vollkosten	279
Vorgehens-Modell	365
Vorlaufenden Indikatoren	36
Vulnerability	355
Vulnerability- und Incident Management	352
Vulnerability- und Incident Response Plan.....	314 348
Vulnerability-Management	350
W	
Wahrscheinlichkeit 10, 11, 13, 14, 18, 275	
Webentry-System.....	183
Weibull-Verteilung	32
Weisung	132, 175, 177
Weisungskonzept	178
Wertbeitrag (Value Delivery)	161
Werte-Governance	284
Wertschöpfung	212, 224
Wiederanlauf	327, 329
Wiederanlaufs-Ziel	331
Wiederanlaufzeit.....	328
Wiederherstellung . 311, 314, 327, 328, 329	
Wiederherstellungskosten	280
Wirksamkeit	228
Wirtschaftsprüfung	90
Worst Case Szenario... 30, 54	
Worst-case.....	31, 400
Z	
Zeitprioritäten	243
Zero-Day-Exploit	54
Zielobjekte	224
Zugriffs-Kontrollsystem . 181, 183	
Zuverlässigkeit	150
Zyklischer Prozess	64