

Hans-Peter Königs

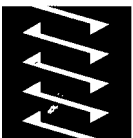
# IT-Risiko-Management mit System

Von den Grundlagen bis zur Realisierung -  
Ein praxisorientierter Leitfaden

3., überarbeitete und erweiterte Auflage

Mit 88 Abbildungen

PRAXIS



**VIEWEG +  
TEUBNER**

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>1</b>
1.1	Warum beschäftigen wir uns mit Risiken?	1
1.2	Risiken bei unternehmerischen Tätigkeiten	2
1.3	Inhalt und Aufbau dieses Buchs	3
<b>Teil A: Grundlagen erarbeiten</b>		<b>5</b>
<b>2</b>	<b>Elemente für die Durchführung eines Risiko-Managements</b>	<b>7</b>
2.1	Fokus und Kontext Risiko-Management	8
2.2	Definition des Begriffs „Risiko“	9
2.3	Anwendung Risiko-Formeln	13
2.4	Subjektivität bei Einschätzung und Bewertung der Risiken	14
2.5	Hilfsmittel zur Einschätzung und Bewertung der Risiken	15
2.5.1	Risiko-Bewertungs-Matrix	15
2.5.2	Kriterien zur Schadenseinstufung	16
2.5.3	Risiko-Landkarte, Akzeptanz-Kriterien und Risiko-Portfolio	20
2.5.4	Risiko-Katalog	21
2.5.5	Risiko-Aggregation	22
2.6	Risiko-Organisation, Kategorien und Arten von Risiken	24
2.6.1	Bedrohungslisten	27
2.6.2	Beispiele von Risiko-Arten	27
2.7	Zusammenfassung	29
2.8	Kontrollfragen und Aufgaben	30
<b>3</b>	<b>Risiko-Management als Prozess</b>	<b>31</b>
3.1	Festlegung Risiko-Management-Kontext	33
3.2	Durchführung der Risiko-Analyse	34
3.2.1	Analyse-Arten	34
3.2.2	Durchführung der Risiko-Analyse in einem RM-Prozess	37
3.2.3	"Value at Risk" als Risiko-Masszahl	39
3.2.4	Analyse-Methoden	42

## *Inhaltsverzeichnis*

3.2.5	Such-Methoden.....	44
3.2.6	Szenario-Analyse.....	45
3.3	Durchführung von Teil-Analysen.....	46
3.3.1	Schwächen-Analyse.....	46
3.3.2	Impact-Analyse.....	47
3.4	Risiko-Bewertung.....	48
3ö	Risiko-Bewältigung.....	49
3.6	Risiko-Überwachung, Überprüfung und Reporting.....	51
3.7	Risiko-Kommunikation.....	52
3.8	Kriterien für Prozesswiederholungen.....	53
3.9	Anwendungen eines Risiko-Management-Prozesses.....	53
3.10	Zusammenfassung.....	54
3.11	Kontrollfragen und Aufgaben.....	55
<b>Teil B: Anforderungen berücksichtigen.....</b>		<b>57</b>
<b>4</b>	<b>Risiko-Management, ein Pflichtfach der Unternehmensführung.....</b>	<b>59</b>
4.1	Risiko-Management integriert in das Führungssystem.....	59
4.2	Corporate Governance.....	62
4.3	Anforderungen von Gesetzgebern und Regulatoren.....	64
4.3.1	Gesetz KonTraG in Deutschland.....	64
4.3.2	Obligationenrecht in der Schweiz.....	65
4.3.3	Swiss Code of best Practice for Corporate Governance.....	67
4.3.4	Basel Capital Accord (Basel II).....	68
4.3.5	Sarbanes-Oxley Act (SOX) der USA.....	76
4.3.6	EuroSOX.....	79
4.4	Risiko-Management: Anliegen der Kunden und der Öffentlichkeit ...	80
4.5	Hauptakteure im unternehmensweiten Risiko-Management.....	81
4.6	Zusammenfassung.....	84
4.7	Kontrollfragen und Aufgaben.....	85
<b>5</b>	<b>Risiko-Management integriert in das Management-System.....</b>	<b>87</b>
5.1	Integrierter Unternehmens weiter Risiko-Management-Prozess.....	88
5.2	Normatives Management.....	90

5.2.1	Unternehmens-Politik.....	90
5.2.2	Unternehmens-Verfassung.....	91
5.2.3	Unternehmens-Kultur.....	91
5.2.4	Mission und Strategische Ziele.....	91
5.2.5	Vision als Input des Strategischen Managements.....	92
5.3	Strategisches Management.....	92
5.3.1	Strategische Ziele.....	94
5.3.2	Strategien.....	98
5.4	Strategie-Umsetzung.....	98
5.4.1	Strategieumsetzung mittels Balanced Scorecards (BSC).....	98
5.4.2	Unternehmensübergreifende BSC.....	103
5.4.3	Balanced Scorecard und CobIT für die IT-Strategie.....	103
5.4.4	IT-Indikatoren in der Balanced Scorecard.....	105
5.4.5	Operatives Management (Gewinn-Management).....	109
5.4.6	Policies und Pläne.....	109
5.4.7	Risikopolitische Grundsätze.....	111
5.5	Zusammenfassung.....	112
5.6	Kontrollfragen und Aufgaben.....	113
Teil C: IT-Risiken erkennen und bewältigen.....		115
6	Informations-und IT-Risiken.....	117
6.1	Veranschaulichung der Risikozusammenhänge am Modell.....	117
6.2	Informationen - die risikoträchtigen Güter.....	119
6.3	System-Ziele für den Schutz von Informationen.....	121
6.4	Informations-Sicherheit versus IT-Sicherheit.....	124
6.5	IT-Risiko-Management, Informations-Sicherheit und Grundschutz.....	125
6.6	Zusammenfassung.....	126
6.7	Kontrollfragen und Aufgaben.....	126
7	Informations-Sicherheit und Corporate Governance.....	127
7.1	Management von IT-Risiken und Informations-Sicherheit.....	127
7.1.1	IT-Governance und Informations-Sicherheit-Governance.....	128
* 7.1.2	Informations-Sicherheit-Governance.....	130

*Inhaltsverzeichnis*

7.2	Organisatorische Funktionen für Informations-Risiken.....	134
7.2.1	Chief Information Officer (CIO).....	135
7.2.2	Chief (Information) Security Officer.....	135
7.2.3	IT-Owner und IT-Administratoren.....	137
7.2.4	• Information Security Steering Committee.....	138
7.2.5	Checks and Balances durch Organisations-Struktur.....	138
7.3	Zusammenfassung.....	141
7.4	Kontrollfragen und Aufgaben.....	142
8	IT-Risiko-Management in der Führungs-Pyramide.....	143
8.1	Ebenen der IT-Risiko-Management-Führungspyramide.....	144
8.1.1	Risiko- und Sicherheits-Politik auf der Unternehmens-Ebene.....	144
8.1.2	Informations-Sicherheits-Politik und ISMS-Politik.....	145
8.1.3	IT-Sicherheitsweisungen und Ausführungsbestimmungen.....	147
8.1.4	IT-Sicherheits-Architekturincl -Standards.....	149
8.1.5	IT-Sicherheitskonzepte.....	152
8.2	Zusammenfassung.....	153
8.3	Kontrollfragen und Aufgaben.....	155
9	IT-Risiko-Management mit Standard-Regelwerken.....	157
9.1	Bedeutung der Standard-Regelwerke.....	157
9.2	Übersicht über wichtige Regelwerke.....	159
9.3	Risiko-Management mit der Standard-Reihe ISO/IEC 2700x.....	164
9.3-1	Informations-Sicherheits-Management nach ISO/IEC 27001.....	165
9.3-2	Code of Practice ISO/IEC 27002.....	172
9.3.3	Informations-Risiko-Management mit ISO/IEC 27005.....	176
9.4	IT-Risiko-Management mit CobiT.....	179
9.5	BSI-Standards und Grundschutzkataloge.....	186
9.6	Zusammenfassung.....	189
9.7	Kontrollfragen und Aufgaben.....	190
10	Methoden und Werkzeuge zum IT-Risiko-Management.....	191
10.1	IT-Risiko-Management mit Sicherheitskonzepten.....	191
10.1.1	Kapitel „Ausgangslage“.....	195
*	10.1.2 Kapitel „Systembeschreibung und Schutzobjekte“.....	196

10.1.3	Kapitel „Risiko-Analyse“.....	198
10.1.4	Schwachstellen-Analyse anstelle einer Risiko-Analyse.....	201
10.1.5	Kapitel „Anforderungen an die Sicherheitsmassnahmen“.....	203
10.1.6	Kapitel „Beschreibung der Sicherheitsmassnahmen“.....	204
10.1.7	Kapitel „Umsetzung der Sicherheitsmassnahmen“.....	205
10.1.8	Iterative und kooperative Ausarbeitung der Kapitel.....	207
10.2	Die CRAMM-Methode.....	208
10.3	Fehlermöglichkeits- und Einfluss-Analyse.....	214
10.4	Fehlerbaum-Analyse.....	216
10.5	Ereignisbaum-Analyse.....	221
10.6	Zusammenfassung.....	222
10.7	Kontrollfragen und Aufgaben.....	225
<b>11</b>	<b>Kosten/Nutzen-Relationen der Risikobewältigung.....</b>	<b>229</b>
11.1	Formel für Return on Security Investments (ROSI).....	231
11.2	Ermittlung der Kosten für die Sicherheitsmassnahmen.....	233
11.3	Ermittlung der Kosten der bewältigten Risiken.....	236
11.4	Massnahmen-Nutzen ausgerichtet an Unternehmenszielen.....	237
11.4.1	Grundzüge von Val IT.....	239
11.4.2	Grundzüge von Risk IT.....	241
11.5	Fazit zu Ansätzen der Sicherheits-Nutzen-Bestimmung.....	244
11.6	Zusammenfassung.....	244
11.7	Kontrollfragen und Aufgaben.....	247
<b>Teil D: Unternehmens-Prozesse meistern.....</b>		<b>249</b>
<b>12</b>	<b>Risiko-Management-Prozesse im Unternehmen.....</b>	<b>251</b>
12.1	Verzahnung der RM-Prozesse im Unternehmen.....	251
12.1.1	Risiko-Konsolidierung.....	253
12.1.2	Subsidiäre RM-Prozesse.....	254
12.1.3	IT-RM und Rollenkonzepte im Gesamt-RM.....	256
12.2	Risiko-Management im Strategie-Prozess.....	258
12.2.1	Risiko-Management und IT-Strategie im Strategie-Prozess.....	259
12.2.2	Periodisches Risiko-Reporting.....	262

## *Inhaltsverzeichnis*

12.3	Zusammenfassung.....	262
12.4	Kontrollfragen und Aufgaben.....	263
13	<b>Geschäftskontinuitäts-Management und IT-Notfall-Planung.....</b>	<b>265</b>
13.1	Einzelpläne zur Unterstützung der Geschäftskontinuität.....	266
13-1-1	Geschäftskontinuitäts-Plan (Business Continuity Plan).....	267
13-1-2	Betriebskontinuitäts-Plan (Continuity of Operations Plan).....	269
13-1-3	Ausweichplan (Disaster Recovery Plan).....	269
13-1-4	IT-Notfall-Plan (IT Contingency Plan).....	270
13-1-5	Vulnerability- und Incident Response Plan.....	270
13-2	Business Continuity Mangement im Risk Management.....	271
13-2J	Start Gechäftskontinuitäts-Prozess.....	273
13-2.2	Kontinuitäts-Analyse.....	274
13.2.3	Massnahmen-Strategien.....	277
13-2.4	Notfall-Reaktionen und Pläne.....	279
13-2.5	Tests, Übungen und Plan-Unterhalt.....	287
13.2.6	Kontinuitäts-Überwachung, -Überprüfung und -Reporting.....	290
13-3	IT-Notfall-Plan, Vulnerability- und Incident-Management.....	291
13-3-1	Organisation eines Vulnerability- und Incident-Managements.....	294
13-3-2	Behandlung von plötzlichen Ereignissen als RM-Prozess.....	296
13-4	Zusammenfassung.....	297
13-5	Kontrollfragen und Aufgaben.....	299
14	<b>Risiko-Management im Lifecycle von Informationen und Systemen.....</b>	<b>301</b>
14.1	Schutz von Informationen im Lifecycle.....	301
14.1.1	Einstufung der Informations-Risiken.....	301
14.1.2	Massnahmen für die einzelnen Schutzphasen.....	302
14.2	Risiko-Management im Lifecycle von IT-Systemen.....	303
14.3	Synchronisation RM mit System-Lifecycle.....	305
14.4	Zusammenfassung.....	307
14.5	Kontrollfragen und Aufgaben.....	308
15	<b>Risiko-Management in Outsourcing-Prozessen.....</b>	<b>311</b>
15.1	IT-Risiko-Management im Outsourcing-Vertrag.....	312
15-1-1	Sicherheitskonzept im Sourcing-Lifecycle.....	313

15-1.2	Sicherheitskonzept beim Dienstleister.....	317
15.2	Zusammenfassung.....	319
15.3	Kontrollfragen.....	320
Anhang.....		321
A.1	Beispiele von Risiko-Arten.....	323
A.2	Muster Ausführungsbestimmung für Informationsschutz.....	327
A.3	Formulare zur Einschätzung von IT-Risiken.....	331
A.4	Beispiele zur Aggregation von Operationellen Risiken.....	335
Literatur.....		339
Abkürzungsverzeichnis.....		345
Stichwortverzeichnis.....		347