Hans-Peter Königs

# IT-Risiko-Management mit System

## Von den Grundlagen bis zur Realisierung - Ein praxisorientierter Leitfaden

Mit 77 Abbildungen

2., korrigierte Auflage

vieweg

# Inhaltsverzeichnis

**1 Einführung ... 1**

1.1 Warum beschäftigen wir uns mit Risiken? ... 1

1.2 Risiken bei unternehmerischen Tätigkeiten ... 2

1.3 Inhalt und Aufbau dieses Buchs ... 3

**Teil A: Grundlagen erarbeiten ... 5**

**2 Elemente für die Durchführung eines Risiko-Managements ... 7**

2.1 Fokus und Kontext Risiko-Management ... 8

2.2 Definition des Begriffs „Risiko" ... 9

2.3 Anwendung der Risiko-Formel ... 12

2.4 Subjektivität bei der Risiko-Einschätzung ... 13

2.5 Hilfsmittel zur Risiko-Einschätzung ... 13

2.5.1 Risiko-Matrix ... 13

2.5.2 Schadenseinstufung ... 15

2.5.3 Risiko-Karte und Risiko-Portfolio ... 17

2.5.4 Risiko-Katalog ... 18

2.5.5 Risiko-Aggregierung ... 19

2.6 Risiko-Kategorien, Risiko-Arten und Top-Down-Vorgehen ... 20

2.6.1 Bedrohungslisten ... 21

2.6.2 Beispiele von Risiko-Arten ... 22

2.7 Zusammenfassung ... 24

2.8 Kontrollfragen und Aufgaben ... 25

**3 Risiko-Management als Prozess ... 27**

3.1 Festlegung Risiko-Management-Kontext ... 29

32 Durchführung der Risiko-Analyse ... 30

3.2.1 Analyse-Arten ... 30

3.2.2 Durchführung der Risiko-Analyse in einem RM-Prozess ... 32

3.2.3 Value at Risk-Methode ... 34

3.2.4 Analyse-Methoden ... 36

3.2.5 Such-Methoden ... 38

3.2.6 Szenarien-Analyse ... 39
33 Durchführung von Teil-Analysen ... 39
3.3.1 Schwächen-Analyse ... 39
3.3.2 Impact-Analyse ... 40
3.4 Risiko-Bewertung ... 41
3.5 Risiko-Bewältigung ... 42
3.6 Risiko-Kontrolle und -Reporting ... 44
3.7 Risiko-Kommunikation ... 45
3.8 Anwendungen eines Risiko-Management-Prozesses ... 45
3.9 Zusammenfassung ... 46
3.10 Kontrollfragen und Aufgaben ... 47
**Teil B: Anforderungen berücksichtigen ... 49**
**4 Risiko-Management, ein Pflichtfach der Unternehmensführung ... 51**
4.1 Corporate Governance ... 52
4.2 Anforderungen von Gesetzgebern und Regulatoren ... 54
4.2.1 Gesetz KonTraG in Deutschland ... 54
4.2.2 Obligationenrecht in der Schweiz ... 55
4.2.3 Swiss Code of best Practice for Corporate Governance ... 56
4.2.4 Basel Capital Accord (Basel II) ... 57
4.2.5 Sarbanes-Oxley Act (SOX) der USA ... 60
4.3 Risiko-Management: Anliegen der Kunden und Öffentlichkeit ... 62
4.4 Hauptakteure im untemehmensweiten Risiko-Management ... 63
4.5 Zusammenfassung ... 66
4.6 Kontrollfragen und Aufgaben ... 67
**5 Risiko-Management integriert in das Management-System ... 69**
5.1 Integrativer Risiko-Management-Prozess ... 70
5.2 Normatives Management ... 72
5.2.1 Unternehmenspolitik ... 72
5.2.2 Unternehmensverfassung ... 72
5.2.3 Unternehmenskultur ... 73
5.2.4 Mission und Strategische Ziele ... 73
5.2.5 Vision als Input des Strategischen Managements ... 74

5.3 Strategisches Management ... 74
5.3.1 Strategische Ziele ... 76
5.3.2 Strategien ... 80
5.4 Strategie-Umsetzung ... 80
5.4.1 Strategieumsetzung mittels Balanced Scorecards (BSC) ... 80
5.4.2 Unternehmensübergreifende BSC ... 85
5.4.3 Balanced Scorecard und CobiT für die IT-Strategie ... 85
5.4.4 IT-Indikatoren in der Balanced Score Card ... 87
5.4.5 Operatives Management (Gewinn-Management) ... 91
5.4.6 Policies und Pläne ... 91
5.4.7 Risikopolitische Grundsätze ... 93
5.5 Zusammenfassung ... 94
5.6 Kontrollfragen und Aufgaben ... 95

**Teil C: IT-Risiken erkennen und bewältigen ... 97**

**6 Informations- und IT-Risiken ... 99**

6.1 Veranschaulichung der Risikozusammenhänge am Modell ... 99
6.2 Informationen - die risikoträchtigen Güter ... 101
6.3 Systemziele für den Schutz von Informationen ... 103
6.4 Informations-Sicherheit versus IT-Sicherheit ... 105
6.5 IT-Risikomanagement, IT-Sicherheit und Grundschutz ... 106
6.6 Zusammenfassung ... 107
6.7 Kontrollfragen und Aufgaben ... 108

**7 Informations-Sicherheit und Corporate Governance ... 109**

7.1 Management von IT-Risiken und Informations-Sicherheit ... 109
7.1.1 IT-Governance und Informations-Sicherheit-Governance ... 110
7.1.2 Leitfaden für Informations-Sicherheit-Governance ... 111
7.2 Organisatorische Funktionen für Informations-Risiken ... 115
7.2.1 Chief Information Officer (CIO) ... 116
7.2.2 Chief (Information) Security Officer ... 116
7.2.3 Checks and Balances durch Organisations-Struktur ... 118
7.3 Zusammenfassung ... 120
7.4 Kontrollfragen und Aufgaben ... 121

**8 IT-Risiko-Management in der Führungs-Pyramide ..... 123**
8.1 Ebenen der IT-Risiko-Management-Führungspyramide ..... 124
8.1.1 Risiko- und Sicherheitspolitik auf der Unternehmens-Ebene ..... 124
8.1.2 Informations-Sicherheitspolitik ..... 125
8.1.3 IT-Sicherheitsweisungen und Ausführungsbestimmungen ..... 127
8.1.4 IT-Sicherheitsarchitektur und -Standards ..... 129
8.1.5 IT-Sicherheitskonzepte ..... 132
8.2 Zusammenfassung ..... 133
8.3 Kontrollfragen und Aufgaben ..... 134
**9 IT-Risiko-Management mit Standard-Regelwerken ..... 135**
9.1 Bedeutung der Standard-Regelwerke ..... 135
9.2 Wichtige Regelwerke der Informations-Sicherheit ..... 137
9.2.1 IT-Risiko-Bewältigung mit ISO/IEC 17799 und ISO/IEC 27001 ..... 141
9.2.2 IT-Risiko-Bewältigung mit CobiT ..... 144
9.3 Zusammenfassung ..... 149
9.4 Kontrollfragen und Aufgaben ..... 150
**10 Methoden und Werkzeuge zum IT-Risiko-Management ..... 151**
10.1 IT-Risikomanagement mit Sicherheitskonzepten ..... 151
10.1.1 Ausgangslage ..... 155
10.1.2 Systembeschreibung und Schutzobjekte ..... 156
10.1.3 Risiko-Analyse ..... 158
10.1.4 Schwachstellen-Analyse anstelle einer Risiko-Analyse ..... 161
10.1.5 Anforderungen an die Sicherheitsmassnahmen ..... 162
10.1.6 Beschreibung der Sicherheitsmassnahmen ..... 164
10.1.7 Umsetzung der Sicherheitsmassnahmen ..... 164
10.1.8 Iterative und kooperative Ausarbeitung der Kapitel ..... 166
10.2 Die CRAMM-Methode ..... 167
10.3 Fehlermöglichkeits- und Einflussanalyse ..... 173
10.4 Fehlerbaumanalyse ..... 176
10.5 Ereignisbaum-Analyse ..... 180
10.6 Zusammenfassung ..... 182
10.7 Kontrollfragen und Aufgaben ..... 184

**Teil D: Unternehmensprozesse meistern ..... 189**

**11 Risiko-Management-Prozesse im Unternehmen ..... 191**

11.1 Verzahnung der RM-Prozesse im Unternehmen ..... 191

11.1.1 Risiko-Konsolidierung ..... 193

11.1.2 Subsidiäre RM-Prozesse ..... 194

11.1.3 IT-RM imGesamt-RM ..... 195

11.2 Risiko-Management im Strategie-Prozess ..... 197

11.2.1 Risiko-Management und IT-Strategie im Strategie-Prozess ..... 198

11.2.2 Periodisches Risiko-Reporting ..... 201

11.3 Zusammenfassung ..... 201

11.4 Kontrollfragen und Aufgaben ..... 202

**12 Geschäftskontinuitäts-Planung und IT-Notfall-Planung ..... 205**

12.1 Einzelpläne zur Unterstützung der Geschäft-Kontinuität ..... 206

12.1.1 Geschäftskontiuitäts-Plan (Business Continuity Plan) ..... 206

12.1.2 Geschäftswiedererlangungs-Plan (Business Recovery Plan) ..... 207

12.1.3 Betriebskontinuitäts-Plan (Continuity of Operations Plan) ..... 207

12.1.4 Notfall-Plan (Disaster Recovery Plan) ..... 207

12.1.5 IT-Notfall-Plan (IT Contingency Plan) ..... 208

12.1.6 Vulnerability- und Incident Response Plan ..... 208

12.2 Geschäftskontinuitäts-Planung ..... 209

12.2.1 Start Geschäftskontinuitäts-Plan ..... 210

12.2.2 Bedrohungs- und Verletzlichkeits-Analyse ..... 211

12.2.3 Geschäfts-Impact-Analyse ..... 211

12.2.4 Problemerfassung und Lagebeurteilung ..... 212

12.2.5 Kriterien für Plan-Aktivierungen ..... 213

12.2.6 Ressourcen und externe Abhängigkeiten ..... 215

12.2.7 Zusammenstellung Kontinuitäts-Plan ..... 215

12.2.8 Kommunikationskonzept ..... 217

12.2.9 Tests, Übungen und Plan-Unterhalt ..... 218

12.3 IT-Notfall-Plan, Vulnerability- und Incident-Management ..... 220

12.3.1 Organisation eines Vulnerability- und Incident-Managements ..... 222

12.3.2 Behandlung von plötzlichen Ereignissen als RM-Prozess ..... 225

12.4 Zusammenfassung ... 226
12.5 Kontrollfragen und Aufgaben ... 228
**13 Risiko-Management im Lifecycle von Informationen und Systemen ... 229**
13.1 Schutz von Informationen im Lifecycle ... 229
13.1.1 Einstufung der Informations-Risiken ... 229
13.1.2 Massnahmen für die einzelnen Schutzphasen ... 230
13.2 Risiko-Management im Lifecycle von IT-Systemen ... 231
13.3 Synchronisation RM mit System-Lifecycle ... 233
13.4 Zusammenfassung ... 235
13.5 Kontrollfragen und Aufgaben ... 236
**14 Sourcing-Prozesse ... 239**
14.1 IT-Risiko-Management im Outsourcing-Vertrag ... 240
14.1.1 Sicherheitskonzept im Outsourcing-Lifecycle ... 242
14.1.2 Sicherheitskonzept im Insourcing-Lifecycle ... 245
14.2 Zusammenfassung ... 247
14.3 Kontrollfragen ... 248
**Anhang ... 249**
A.1 Beispiele von Risiko-Arten ... 251
A.2 Muster Ausführungsbestimmung für Informationsschutz ... 255
A.3 Formulare zur Einschätzung von IT-Risiken ... 259
**Literatur ... 263**
**Abkürzungsverzeichnis ... 267**
**Stichwortverzeichnis ... 269**