

Inhaltsverzeichnis

Übersichtsverzeichnis	11
Abkürzungsverzeichnis	14
Vorwort	17
1 Einführung	19
1.1 Für eine bessere Welt	19
1.2 Warum gehen Unternehmen unter?	19
1.3 Warum misslingen Projekte?	22
1.4 Warum treffen Menschen Fehlentscheidungen?	24
1.5 Was dürfen wir vom Risikomanagement erwarten?	25
2 Grundlagen des Risikomanagements	27
2.1 Risikomanagement im Kontext	27
2.1.1 Management und Risiko	27
2.1.2 Grundverständnis von Risiko	28
2.1.3 Quellen des Risikomanagements	29
2.2 Risiko definiert	32
2.2.1 Unsicherheit bzw. Ungewissheit	33
2.2.2 Kombination von Eintrittswahrscheinlichkeit und Auswirkung	33
2.2.3 Auswirkungen positiv oder negativ	34
2.2.4 Ungewissheit als Eintrittswahrscheinlichkeit	34
2.2.5 Ziele, Tätigkeiten und Anforderungen	36
2.2.6 Entwicklungen und Ereignisse	36
2.3 Risikomanagement als Führungsaufgabe	37
2.3.1 Management	37
2.3.2 Strategisches Management	38
2.3.3 Operatives Management	39
2.3.4 Strategisches und operatives Risikomanagement	40
2.3.5 Ziele des Risikomanagements	40
2.4 Corporate Governance	41
2.4.1 Corporate Governance als Grundlage für das Risikomanagement ..	41
2.4.2 Internationale Vereinbarung der G20 / OECD	42
2.4.3 Deutschland	43
2.4.4 Österreich	45
2.4.5 Schweiz	46

2.4.6	England	46
2.4.7	Vereinigte Staaten von Amerika	48
2.5	Normative Grundlagen	50
2.5.1	Allgemeines	50
2.5.2	COSO Enterprise Risk Management Framework	51
2.5.3	ISO 31000 Risk management – Principles and guidelines	55
2.5.4	Regulatorisches Risikomanagement in der Finanzindustrie	62
2.5.5	Risikomanagement-Konzepte in der Gesamtübersicht	66
3	Anwendungen des Risikomanagements	69
3.1	Vielfältige Anwendungen und Sichtweisen	69
3.1.1	Top-down und Bottom-up-Ansatz	69
3.1.2	Integrativer Ansatz	70
3.2	Unternehmens-Risikomanagement	72
3.2.1	Strategisches Risikomanagement und Entscheidungsfindung	72
3.2.2	Operatives Risikomanagement: Fehler und Schadenereignisse	75
3.3	Sicherheit von Produkten und Dienstleistungen	77
3.3.1	Produktsicherheit und Produkthaftung	77
3.3.2	Klinisches Risiko- und Qualitätsmanagement	94
3.4	HSE – Health, Safety, Environment	102
3.4.1	Gesundheitsschutz	102
3.4.2	Umweltschutz	107
3.5	Interne Kontrollsysteme	110
3.5.1	Vorgaben aus Gesetz und Normen	110
3.5.2	Prozessorientierte Umsetzung	111
3.6	Sicherheit der Informationstechnologie	114
3.6.1	Risiken von vernetzten IT-Systemen	114
3.6.2	IT-Sicherheits-Standards	115
3.7	Notfall-, Krisen-, Kontinuitätsmanagement	116
3.7.1	Betriebliches Notfall-, Krisen- und Kontinuitätsmanagement	116
3.7.2	Öffentliches Notfall-, Krisen- und Kontinuitätsmanagement	117
3.7.3	Risikomanagement bei kritischen Infrastrukturen	119
3.8	Risikobasierter Ansatz	119
3.8.1	Risikobasiertes Denken	119
3.8.2	Risikobasierter Ansatz	120
3.8.3	Das wirkliche Potential des Risikomanagements	123
4	Der Risikomanagement-Prozess	125
4.1	Allgemeines	125
4.2	Kommunikation und Konsultation	125
4.2.1	Risikowahrnehmung und Risikoeinstellung	125
4.2.2	Informationsbeschaffung und -Verbreitung	127
4.3	Rahmenbedingungen	128
4.3.1	Auslöser des Risikomanagement-Prozesses	128
4.3.2	Externe Rahmenbedingungen	128

4.3.3	Interne Rahmenbedingungen	132
4.3.4	Rahmenbedingungen des Risikomanagements	135
4.3.5	Festlegen der Risikokriterien	136
4.4	Risikoidentifikation	142
4.4.1	Erkennbarkeit von Risiken	142
4.4.2	Nicht bzw. schwer erkennbare Risiken	145
4.4.3	Neue Risiken durch Veränderung der Risikowahrnehmung	145
4.4.4	Systematik der Risikoidentifikation	147
4.4.5	Früherkennung von Risiken	148
4.5	Risikoanalyse	150
4.5.1	Risiken verstehen	150
4.5.2	Risikoszenario als Credible-Worst-Case	152
4.5.3	Zeitfaktor im Risikoszenario	155
4.5.4	Korrelation von Risiken	156
4.5.5	Kombination von Risiken	156
4.5.6	Einschätzung der Wahrscheinlichkeit	158
4.5.7	Einschätzung der Auswirkungen	158
4.6	Risikobewertung	159
4.6.1	Akzeptierbare, tolerierbare Risiken	159
4.6.2	Chancenabwägung im Geschäftsbereich	159
4.6.3	Rendite-Risiko-Abwägung im Finanzbereich	161
4.6.4	Güterabwägung im Sicherheitsbereich	162
4.6.5	Vorsorgeprinzip	164
4.7	Risikobewältigung	165
4.7.1	Konzepte der Risikobewältigung	165
4.7.2	Präventives Risikomanagement	166
4.7.3	Schadenmanagement	172
4.7.4	Risikofinanzierung / Versicherungsmanagement	173
4.7.5	Restrisiko akzeptieren	174
4.8	Risikoüberwachung und Risikoüberprüfung	174
4.8.1	Risikomanagement als iterativer Prozess	174
4.8.2	Risikoüberwachung	175
4.8.3	Risikoüberprüfung	175
5	Methoden der Risikobeurteilung	177
5.1	Überblick	177
5.2	Kreativitätstechniken	180
5.2.1	Brainstorming	180
5.2.2	World Café	181
5.2.3	Delphi-Studie als Befragungstechnik	182
5.2.4	Citizens Conference / Bürgerkonferenz	183
5.3	Szenarioanalysen i.w.S.	184
5.3.1	Allgemeines	184
5.3.2	Ursache-Wirkungs-Analyse / Ishikawa Diagramm	184
5.3.3	Anwendungen	185

5.3.4	Schadenfallanalyse	185
5.3.5	Szenarioanalysen i.e.S.	187
5.3.6	Fehlerbaum- und Ablaufanalyse	190
5.4	Indikatorenanalysen	195
5.4.1	Fehlermeldesysteme (Critical Incidents Reporting Systems)	195
5.4.2	Risk Based Change Management (RBCM)	200
5.5	Funktionsanalysen, Gefährdungsanalysen	203
5.5.1	Allgemeines.	203
5.5.2	FMEA – Failure Mode and Effects Analysis	203
5.5.3	Gefährdungsanalysen	207
5.5.4	HAZOP	208
5.5.5	Anwendung	210
5.6	Statistische Methoden	211
5.6.1	Allgemeines.	211
5.6.2	Abbildung des Risikos mit einer Verteilungsfunktion	212
5.6.3	Value at Risk als Maß für das Risiko	216
5.6.4	Monte Carlo Simulation zur Risikoaggregation.	217
5.7	Zusammenfassung: Methodeneinsatz	221
6	Risikomanagement-System	223
6.1	Einführung des Risikomanagements	223
6.1.1	Projekt der Unternehmensentwicklung	223
6.1.2	Auftretende Widerstände	224
6.1.3	Handlungsspielraum und Entscheidungsfreiheit	225
6.1.4	Organisationspezifische Gegebenheiten	226
6.2	Steuerung des Risikomanagements	228
6.2.1	Risikomanagement-System	228
6.2.2	Auftrag und Verpflichtung der Leitung	229
6.2.3	Planung des Risikomanagements	230
6.2.4	Umsetzung des Risikomanagements	241
6.2.5	Leistungsbewertung des Risikomanagements.	259
6.2.6	Verbesserung des Risikomanagements	265
6.3	Risikomanagement in komplexen Organisationen	267
6.3.1	Komplexe Organisationen	267
6.3.2	Vertikale Integration von Risiken.	268
6.3.3	Horizontale Integration von Risiken	269
	Schlusswort	271
	Verzeichnis der Begriffe	273
	Literaturverzeichnis	277
	Verzeichnis der Internetquellen	287

Übersichtenverzeichnis

Übersicht 1: Muster der Selbstüberschätzung	21
Übersicht 2: Muster der Unterschätzung von Komplexität	23
Übersicht 3: COSO Internal Control – Integrated Framework	52
Übersicht 4: COSO Enterprise Risk Management Framework	53
Übersicht 5: Prozess Risikomanagement nach AS/NZS 4360	57
Übersicht 6: Das Risikomanagement-System	58
Übersicht 7: Struktur der ONR 49000 Serie	62
Übersicht 8: Eigenmittelanforderungen Basel I + II	65
Übersicht 9: Eigenmittelanforderungen Solvency I + II	66
Übersicht 10: Unterschiedliche Risikomanagement-Konzepte	67
Übersicht 11: Top-down- und Bottom-up-Ansatz	70
Übersicht 12: Anwendungsbereiche des Risikomanagements	72
Übersicht 13: Risikomanagement in Strategie	73
Übersicht 14: Strategisches Risikomanagement	75
Übersicht 15: New Legislative Framework	79
Übersicht 16: CE-Kennzeichen	79
Übersicht 17: Richtlinien des New Legislative Frameworks	84
Übersicht 18: Module der Konformitätsbewertung	85
Übersicht 19: Konformitätsbewertungs-Verfahren	85
Übersicht 20: Die Umsetzung der Maschinenrichtlinie	86
Übersicht 21: Risikoprofil eines Krankenhauses der Grundversorgung	96
Übersicht 22: Das Schweizer-Käse-Modell	99
Übersicht 23: Never Events des NHS 2013-2014	101
Übersicht 24: IKS-Kontroll-Matrix	111
Übersicht 25: Notfall-, Krisen- und Kontinuitätsmanagement	117
Übersicht 26: Der Risikomanagement-Prozess	125
Übersicht 27: Überschätzte und unterschätzte Risiken	127
Übersicht 28: Allgemeine Risikokriterien	138
Übersicht 29: Risikokriterien für die Patientensicherheit	138
Übersicht 30: Definition Wahrscheinlichkeit in Organisationen	139
Übersicht 31: Definition Wahrscheinlichkeit in Systemen	140
Übersicht 32: Risikotoleranz und Risikoakzeptanz	142
Übersicht 33: Das Risikoszenario	151
Übersicht 34: Beispiel für ein Risikoszenario	152
Übersicht 35: Das Eisbergprinzip	153
Übersicht 36: Darstellung des Risikos als Linie	155
Übersicht 37: Gegenseitige Abhängigkeit von Risiken	157
Übersicht 38: Gegenseitige Abhängigkeit von Risiken	157
Übersicht 39: Stufen für Bedrohungen und Chancen	160

Übersicht 40: Chancen- und Bedrohungsprofil	160
Übersicht 41: Risiken mit Chancen und Bedrohungen	161
Übersicht 42: Capital Asset Pricing Model	162
Übersicht 43: Menschliche Fehlerarten	167
Übersicht 44: Die Risikoquellen im Team	168
Übersicht 45: Das Drei-Stufen-Modell	170
Übersicht 46: Methoden der Risikobeurteilung im Überblick.....	177
Übersicht 47: Das Fischgräte- bzw. Ishikawa-Diagramm	184
Übersicht 48: Systemanalyse nach dem London-Protokoll.....	186
Übersicht 49: Vorgehen für die Abklärung eines schweren Unfalls.....	187
Übersicht 50: Das Zielsystem nach Balanced Scorecard	188
Übersicht 51: Risikolandschaft im Ist- und Soll-Zustand	189
Übersicht 53: Fehlerbaum- und Ablaufanalyse.....	191
Übersicht 54: Beispiel Erdgasleitung	192
Übersicht 55: Das Störfall-Risikomatrix	194
Übersicht 56: Critical Incidents als Teil des Eisbergs.....	195
Übersicht 57: Bewertung der Veränderung.....	200
Übersicht 58: Eskalationsprozess	201
Übersicht 59: Frühe Voraussicht der Subprime-Krise in 2007	202
Übersicht 60: Original FMEA-Arbeitsblatt	206
Übersicht 61: Risikokriterien bei der Gefährdungsanalyse	207
Übersicht 62: HAZOP Anwendung in der chemischen Industrie	209
Übersicht 63: Definition der Auswirkungen	210
Übersicht 64: Normalverteilung mit Standardabweichung	212
Übersicht 65: Standardabweichung als Maß für das Risiko	213
Übersicht 66: Statistische Merkmale eines Risikos.....	214
Übersicht 67: Verteilungsfunktionen aus Crystall Ball.....	215
Übersicht 68: Value at Risk als Maß für das Risiko	216
Übersicht 69: Risiko von Aktien und Anleihen	218
Übersicht 70: Risiko einer Versicherung	219
Übersicht 71: Aggregation eines Risikoprofils	220
Übersicht 72: Vergleich des Value at Risk IST- und SOLL.....	220
Übersicht 73: Übersicht über die Methoden	222
Übersicht 74: Das Risikomanagement-System	228
Übersicht 75: Planung des Risikomanagements	231
Übersicht 76: Beispiel Risikomanagement-Politik	232
Übersicht 77: Die drei Verteidigungslinien	238
Übersicht 78: Risikomanagement in ISO 9001	239
Übersicht 79: Risikomanagement als vernetzter Führungsprozess	240
Übersicht 80: Umsetzung des Risikomanagements	242
Übersicht 81: Risikomanagement im Strategieprozess	243
Übersicht 82: Risikofelder Strategische Führung	245
Übersicht 83: Produkt-Risikomanagement.....	246
Übersicht 84: Risikofelder Produktrisiken.....	248
Übersicht 85: Projekt-Risikomanagement	249

Übersicht 86: Risikofelder Projektmanagement.....	251
Übersicht 87: Risikomanagement im Zeitablauf	251
Übersicht 88: Beispiele für Notfälle und Krisen	253
Übersicht 89: Ablauf von Notfällen und Krisen	253
Übersicht 90: Führungsprozess Krisenmanagement.....	255
Übersicht 91: Kontinuitätsmanagement	257
Übersicht 92: Risikokriterien für das Kontinuitätsmanagement	257
Übersicht 93: Leistungsbewertung im Risikomanagement	260
Übersicht 94: Veränderungen der Risikolandschaft.....	261
Übersicht 95: Langzeitergebnisse eines Risikomanagement-Programms.....	262
Übersicht 96: Die wichtigsten Audit-Punkte	265
Übersicht 97: Das Reifegradmodell des Risikomanagements.....	266
Übersicht 98: Konsolidierung von Risiken	269
Übersicht 99: Querschnittsrisiken	270

Abkürzungsverzeichnis

AKW	Atomkraftwerk
AIA	Automatischer Informations-Ausgleich
ALARP	As low as reasonably practicable
AS/NZS	Australian/New Zealand
ATC	Air Traffic Control
ATIR	Air Traffic Incident Report
ATM	Air Traffic Management
BAV	Bundesamt für Verkehr (Schweiz)
BCM	Business Continuity Management
BMI	Bundesministerium des Innern (Deutschland)
BSI	British Standard Institute
CAPM	Capital Asset Pricing Model
CEN	European Committee for Standardization / Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Electrotechnique / European Committee for Electrotechnical Standardization
CGMPS	Current Good Manufacturing Practices
CIRS	Critical Incidents Reporting System
CobiT	Control Objectives Information Technology
COSO	Committee of Sponsoring Organizations of the Teadway Commission
CSR	Corporate Social Responsibility
DIIR	Deutsches Institut für Interne Revision
DIN	Deutsches Institut für Normung
DoD	Department of Defence (USA)
EBIT	Earnings Before Interest and Tax
EFQM	European Foundation for Quality Management
EG	Europäische Gemeinschaft
EN	Europäische Norm
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
ERM	Enterprise Risk Management
F.A.Z.	Frankfurter Allgemeine Zeitung
FERMA	Federation of European Risk Management Associations
FMEA	Failure Mode and Effects Analysis / Fehler-Möglichkeiten und Einfluss-Analyse
GRS	Gesellschaft für Reaktorsicherheit
GRC	Governance, Risk and Compliance
HSE	Health, Safety and Environment

IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISO	International Standard Organization
ITIL	Information Technology Infrastructure Library
KonTraG	Deutsches Gesetz über die Kontrolle und Transparenz im Unternehmensbereich vom 30. April 1998
MAS	Master of Advanced Studies (Hochschulabschluss)
MIL-STD	Military Standard
NHS	National Health Service (UK)
NPA	Non Prosecution Agreement (Schweizer Banken)
NZZ	Neue Zürcher Zeitung
OEM	Original Equipment Manufacturer
ON	Österreichisches Normungsinstitut
ONR	Regelwerk des Österreichischen Normungsinstituts (ON)
OR	Schweizerisches Obligationenrecht
Q	Quality
QRM	Qualitäts- und Risikomanagement
REACH	Registration, Evaluation, Authorization of Chemicals
RLCG	Richtlinie Corporate Governance (Schweiz)
RPZ	Risikoprioritätszahl
PRA	Probabilistic Risk Assessment
PrSG	Produktsicherheits-Gesetz (Schweiz) vom 1. Juli 2010
PSA	Persönliche Schutzausrüstung
SA	Social Accountability
SE	Systems Engineering
SEC	Securities Exchange Commission
SNV	Schweizerische Normenvereinigung
SOP	Start of Production / Standard Operation Procedure
SOX	Sarbanes-Oxley Act (USA)
STEG	Bundesgesetz über die Sicherheit von technischen Einrichtungen und Geräten
STEV	Verordnung über die Sicherheit von technischen Einrichtungen und Geräten
StGB	Schweizerisches Strafgesetzbuch
SUVA	Schweizerische Unfallversicherungs-Anstalt
UN	United Nations
UNCED	UN Commission on Environment and Development
USV	Unterbrechungsfreie Stromversorgung
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation (Schweiz)
VaR	Value at Risk
VSZV	Verordnung über die Sicherheitsuntersuchung von Zwischenfällen im Verkehrswesen (VSZV) vom 17. Dezember 2014 (Stand am 1. Februar 2015)
WEF	World Economic Forum

Vorwort

Seit der Veröffentlichung der 3. Auflage dieses Buches sind fünf Jahre vergangen. Seinerzeit dominierte die Finanzkrise die Diskussionen im Risikomanagement. Warum war diese trotz der umfangreichen regulatorischen Vorgaben im Risikomanagement möglich? Die aufwendigen internen Kontrollsysteme waren offenbar nicht ausreichend wirksam, um dieses weltweite Desaster zu verhindern.

Im März 2011 ereignete sich die Nuklearkatastrophe von Fukushima. Ausgerechnet im führenden Technologieland Japan, wo zudem weltweit die größte Erfahrung mit Erdbeben und Tsunamis vorhanden ist, hat die Katastrophe stattgefunden. Wenn man Fukushima eingehend analysiert, hat die Technik trotz des Erdbebens funktioniert. Aber ein überflutetes Kernkraftwerk kann seine Funktion nicht mehr wahrnehmen. Frühere Fehlentscheidungen betreffend die Wahl des Standortes sowie die Missachtung von Sicherheitsempfehlungen der IAEA betreffend Naturkatastrophen und Tsunamis führten zum verhängnisvollen Verlauf.

Im Januar 2012 lief die Costa Concordia in Giglio / Italien auf Grund. 100 Jahre nach der Titanic spielte wenigstens das Glück mit, indem das havarierte Schiff an die Küstennähe getrieben wurde und dort liegen blieb. Unvorstellbar wären die Folgen gewesen, wenn das Schiff mit 4200 Menschen an Bord nachts auf offenem Meer gesunken wäre. Der Kapitän hat schwere Fehler begangen. Ende Juli 2012 hat die Reederei das Arbeitsverhältnis mit Schettino gekündigt. Sie hat sich von ihm öffentlich distanziert. Die Kreuzfahrtgesellschaft einigte sich im April 2013 mit der italienischen Justiz auf einen strafrechtlichen Vergleich; gegen die Zahlung von einer Million Euro – die Höchstsumme im italienischen Recht – wurden die Ermittlungen gegen das Unternehmen eingestellt. Nach Abschluss des Vergleichs wurde die Reederei auf ihr Verlangen im Prozess gegen ihren Kapitän als Nebenklägerin zugelassen. Schettino wurde am 11. Februar 2015 erstinstanzlich zu 16 Jahren und einem Monat Freiheitsstrafe verurteilt. Dieses Gerichtsverfahren hat allerdings mit Risikomanagement nichts mehr zu tun.

Am 15. November 2009 wurde der Internationale Standard ISO 31000 Risk management – Principles and guidelines veröffentlicht. Es wäre vermessen zu behaupten, dass dieser globale Ansatz die vergangenen Krisen und Katastrophen hätte verhindern können. Aber die Tatsache, dass eine solche globale Norm entstanden ist, weist auf die großen Erwartungen an das Risikomanagement hin.

Inzwischen darf ich als Vorsitzender der Arbeitsgruppe ISO TC 262 WG «Core risk management standards» die Weiterentwicklung der ISO 31000 auf globaler Ebene leiten. Eine anspruchsvolle und herausfordernde Aufgabe. Auch die ONR 49000-Serie wurde inzwischen überarbeitet. Mit der Version 2014 entstand ein Regelwerk, das insbesondere in Europa hohe Anerkennung errungen hat.

Inzwischen konnte ich rund 400 Risikomanagement-Projekte in Industrie, Energiewirtschaft, Finanz- und Gesundheitswesen leiten, rund 2500 Risikomanager in mehrtägigen Weiterbildungslehrgängen qualifizieren und hunderte von Studierenden an der Technischen Hochschule in Deggendorf (Bayern) sowie an anderen Universitäten und Fachhochschulen unterrichten.

Dieses Buch ist ein Ergebnis langjähriger und zielgerichteter Arbeiten im Risikomanagement, wo sich nun Praxis und Theorie miteinander verbinden. Ich wünsche mir, dass viele Menschen an meinen Erkenntnissen und Erfahrungen teilhaben können.

Ein sehr herzliches Dankeschön gehört meiner lieben Doris. Sie hat mich – einmal mehr – mit ihren sprachlichen Fähigkeiten und mit dem seit vielen Jahren gewachsenen Verständnis für mein komplexes Fachgebiet tatkräftig unterstützt. Sie war auch bei dieser vierten, überarbeiteten Auflage des Buches unentbehrlich.

Zürich, im März 2016
Bruno Brühwiler