

Karlheinz H. W. Thies

Management operationaler IT- und Prozess-Risiken

Methoden für eine
Risikobewältigungsstrategie

Inhalt

1	Einführung	1
2	IT-Sicherheitspolicy	3
2.1	Einordnung der IT-Sicherheitspolicy	3
2.2	Definition des Geltungsbereichs	3
2.3	Sicherheitsgrundsätze	4
2.3.1	Sicherheitsgrundsatz 1: Unternehmensziel	4
2.3.2	Sicherheitsgrundsatz 2: Schadensvermeidung	4
2.3.3	Sicherheitsgrundsatz 3: Sicherheitsbewusstsein	5
2.3.4	Sicherheitsgrundsatz 4: Gesetzliche, aufsichtsrechtliche und vertragliche Pflichten	5
2.3.5	Sicherheitsgrundsatz 5: Maßnahmen gemäß allgemeingültiger Sicherheitsstandards	6
2.3.6	Sicherheitsgrundsatz 6: Aufrechterhaltung des Geschäftsbetriebes	6
2.3.7	Sicherheitsgrundsatz 7: Sicherheitsarchitektur	7
2.4	Verantwortlichkeiten	7
2.4.1	Geschäftsführung und Management	7
2.4.2	Sicherheitsorganisation	8
2.4.3	Mitarbeiter	10
2.5	Umsetzung	10
2.5.1	Sicherheitsarchitektur	10
2.5.2	Aufgabengebiete	12
2.5.3	Kontrolle	12
3	Operationale Risiken	15
3.1	Grundbetrachtung der operationalen Risiken	15
3.1.1	Warum sind die operationalen Risiken für ein Unternehmen zu berücksichtigen?	15

3.1.2	Übersicht Risiken.....	16
3.1.3	Gesetzliche und „quasigesetzliche“ Vorgaben.....	18
3.1.4	KonTraG (u. a. Änderungen des AktG und des HGB).....	18
4	Aufbau eines Managements operationaler IT-Risiken	21
4.1	IT-Risikobetrachtung über ein Schichtenmodell	21
4.2	Welche Sicherheit ist angemessen?	22
4.3	Grobe Vorgehensweise für ein Risikomanagement.....	23
4.3.1	Das „operationale Risiko“	23
4.3.2	Aktualisierung der Werte des operationalen Risikos	23
4.3.3	Rollierender Report „Operationales Risiko“	24
4.4	Rahmen für Risikoeinschätzung operationaler Risiken	24
4.4.1	Definitionen	24
4.4.2	Schutzbedürftigkeitsskalen	26
4.4.3	Feststellung des Schutzbedarfs	30
4.4.4	Qualitative Risikoeinschätzung einzelner Produkte.....	30
4.4.5	Quantitative Risikoeinschätzung eines Produktes.....	34
4.4.6	Steuerung der operationalen Risiken.....	35
4.4.7	Aufbau des Reporting mit Darstellung der Risiken auf Prozess-/Produktebene	36
4.4.8	Risikodarstellung der Prozesse/Anwendungen in einem Risikoportfolio	37
4.4.9	Risikobewältigungsstrategien	38
4.5	Risikomanagement operationaler Risiken	38
5	Strukturierte Risikoanalyse	41
5.1	Schwachstellenanalyse und Risikoeinschätzung für die einzelnen IT-Systeme/Anwendungen mit der Methode FMEA	41
5.1.1	Übersicht	41
5.1.2	Kurzbeschreibung der Methode	42
5.1.3	Begriffsbestimmung.....	43
5.1.4	Anwendung der Methode FMEA.....	44
5.2	Strukturierte Risikoanalyse (smart scan)	52
5.2.1	Generelle Vorgehensweise.....	52
5.2.2	Übersicht über die Klassifizierung und Einschätzung	53
5.2.3	Feststellung des Schutzbedarfs	54
5.2.4	Checkliste Feststellung der Schutzbedarfsklasse bei Prozessen/Anwendungen	54
5.2.5	Checkliste Feststellung Schutzbedarfsklassen bei IT-Systemen/IT-Infrastruktur	56
5.2.6	Ermittlung des Gesamtschutzbedarfs	58
5.2.7	Feststellung der Grundsicherheit von IT-Komponenten und Infrastruktur	59

5.2.8	Feststellung der Sicherheit und Verfügbarkeit von Anwendungen	61
5.2.9	Feststellung der Risikovorsorge	63
5.2.10	Feststellung des Risikos	64
5.2.11	Zuordnung und Bewertung der Risikoanalyse für die FMEA	64
5.2.12	Überführung der Bewertung in die FMEA	65
6	Das IT-Security & Contingency Management	67
6.1	Warum IT-Security & Contingency Management?	67
6.2	Risiken im Fokus des IT-Security & Contingency Managements	68
6.3	Aufbau und Ablauforganisation des IT-Security & Contingency Managements	68
6.3.1	Zuständigkeiten	68
6.3.2	Aufbauorganisation	69
6.3.3	Teamleitung IT-Security & Contingency Management	70
6.3.4	Rolle: Security & Prevention IT-Systeme/Infrastruktur	70
6.3.5	Rolle: Contingency Management Fachbereichsbetreuung	70
6.3.6	Rolle: IT-Risikosteuerung	71
6.3.7	Schnittstellen zu anderen Bereichen	71
6.3.8	Besondere Aufgaben	74
6.3.9	Anforderungsprofil an Mitarbeiter des IT-Security & Contingency Managements	75
7	IT-Krisenorganisation	81
7.1	Aufbauorganisation des IT-Krisenmanagements	81
7.2	Zusammensetzung, Kompetenzen und Informationspflichten der Krisenstäbe	81
7.2.1	Operativer Krisenstab	82
7.2.2	Strategischer Krisenstab	83
7.3	Verhältnis zwischen den beiden Krisenstäben	83
7.4	Zusammenkunft des Krisenstabs (Kommandozentrale)	83
7.5	Auslöser für die Aktivierung des Krisenstabs	84
7.6	Arbeitsaufnahme des operativen Krisenstabs	87
7.6.1	Bilden von Arbeitsgruppen	88
7.6.2	Unterlagen für den Krisenstab	90
7.7	Verfahrensanweisungen zu einzelnen K-Fall-Situationen	94
7.7.1	Brand	94
7.7.2	Wassereintrich	95
7.7.3	Stromausfall	95
7.7.4	Ausfall der Klimaanlage	95

7.7.5	Flugzeugabsturz	95
7.7.6	Geiselnahme	95
7.7.7	Ausfall der Datenübertragung intern, zum RZ, zu den Kunden	95
7.7.8	Ausfall des Host, des Rechenzentrums	96
7.7.9	Verstrahlung, Kontamination, Pandemie	96
7.7.10	Sabotage	97
7.7.11	Spionage	97
8	Präventiv-, Notfall-, K-Fall-Planung	99
8.1	Präventiv- und Ausfallvermeidungsmaßnahmen	99
8.1.1	Generelle Vorgehensweise	99
8.1.2	Präventivmaßnahmen, die einen möglichen Schaden verlagern	100
8.1.3	Präventiv- und Ausfallvermeidungsmaßnahmen, die den Eintritt des Notfalles verhindern	100
8.1.4	Präventivmaßnahmen, die die Ausübung des Notfallplans ermöglichen	101
8.1.5	Praktische Umsetzung und Anwendung	101
8.1.6	Bestehende Grundsicherheit in technischen Räumen	101
8.1.7	Maßnahmen in der Projektarbeit	102
8.1.8	Maßnahmen in der Linienaufgabe	102
8.1.9	Verfügbarkeitsklasse	102
8.1.10	Überprüfung von Präventiv- und Ausfallvermeidungsmaßnahmen	104
8.1.11	Versicherung	104
8.1.12	Checkliste zur Feststellung des Schutzbedarfs bei Präventiv- und Ausfallvermeidungsmaßnahmen	104
8.1.13	Checkliste zur Überprüfung von Ausfallvermeidungsmaßnahmen	106
8.2	Notfall- und Kontinuitätspläne	107
8.2.1	Inhalte des Notfallhandbuches	107
8.2.2	Handhabung des Notfallhandbuches (IT-Krisenstab, Notfallpläne, Anhang)	107
8.2.3	Ziele des Notfallhandbuches	108
8.2.4	Praktische Anwendung und Umsetzung	108
8.2.5	Notfall- und K-Fall-Übungen	112
8.2.6	Notfallübungen	114
8.2.7	K-Fall-Übungen	121
Anhang	129
A.1	Begriffsdefinitionen Sicherheit	129
A.2	Checkliste: Organisation der IT-Sicherheit	131
A.3	Checklisten für innere Sicherheit	132
A.4	Checklisten für äußere Sicherheit	132

A.5	Checkliste Mitarbeiter	133
A.6	Checkliste Datensicherung	133
A.7	Checkliste Risikoanalyse und Sicherheitsziele	134
A.8	Mustervorlage E-Mail-Richtlinien.....	134
I.	Gegenstand und Geltungsbereich	134
II.	Verhaltensgrundsätze	135
III.	Einwilligung und Vertretungsregelung	136
IV.	Leistungs- und Verhaltenskontrolle/Datenschutz für E-Mail.....	136
A.9	Übersicht von Normen für Zwecke des Notfall- und Kontinuitätsmanagements	137
Abkürzungsverzeichnis		139
Abbildungsverzeichnis.....		141
Tabellenverzeichnis		143
Literatur- und Quellenverweise.....		145
Index		147