



Inhalt

Vorwort	XI
Die Autoren	XIII
Danksagungen	XV
1 Einleitung	1
1.1 Zielgruppen - How to use this book	4
1.2 Disclaimer	5
1.3 Das erste Treffen oder wie alles begann	5
2 Die Grundlagen, Standards und Definitionen	11
2.1 Information Technology Infrastructure Library (ITIL®)	14
2.2 ITIL® und ISO/IEC 20000	20
2.3 Lean SixSigma	22
2.4 Incident Management nach ITIL®	26
2.5 Wechselwirkungen und Einflussfaktoren	27
2.5.1 Problem Management	28
2.5.2 Configuration Management	28
2.5.3 Change Management	29
2.5.4 Event Management	31
2.5.5 Service Level Management	31
2.5.6 Availability Management	32
2.5.7 Capacity Management	32
2.5.8 IT Service Continuity Management (ITSCM)	33
2.5.9 IT Financial Management	33
2.5.10 IT-Sicherheitsmanagement	34
2.5.11 Der Help Desk/Single Point of Contact	34
2.6 Incident Management vs. Problem Management	35
2.7 Key Performance Indicators	37
2.7.1 Kritische Erfolgsfaktoren und KPIs	38
2.7.2 Definition von KPIs	38

2.7.3	Implementierung von KPIs	45
2.7.4	Darstellung und Anpassung von KPIs und deren Messungen	46
3	Der Incident	53
3.1	Incident-Arten	55
3.2	Verfügbarkeit – „der Feind des Incident Management“	57
3.3	Ursachen von Incidents	63
3.3.1	Technologie	64
3.3.2	Architektur	72
3.3.3	Business	74
3.3.4	Prozesse	76
3.3.5	Personal	78
3.3.6	Umweltfaktoren/höhere Gewalt	80
3.3.7	Wechselwirkungen von Faktoren	81
3.4	Phasen eines Incidents	88
3.5	Kosten von Incidents	92
3.5.1	Direkte und indirekte Incident-Kosten	92
3.5.2	Kosten einer Incident-Lösung nach erfolgreicher Störungsbehebung	96
3.5.3	Kostenfaktoren – die waren Kostentreiber eines Incidents	97
3.5.4	Ermittlung der Kosten	106
3.6	Kosten des Incident-Management-Prozesses	111
3.7	Klassifizierung von Incidents (Incident-Kategorien)	113
3.7.1	Definition	114
3.7.2	Grauzonen und Angstfaktor	118
3.7.3	Review der Kategorien – wo endet E2E?	119
3.7.4	Zusätzliche Kategorien	120
4	Das Incident Handling	123
4.1	Erwarte das Unerwartete	123
4.2	First-Aid-Kit – erste Maßnahmen	127
4.3	Feueralarm und Sinnloseskalation	132
4.4	Stufenweise Notifikation und Eskalation	138
4.5	Automatisieren von Benachrichtigungen	140
4.6	Meet-Me-Line und „Incident-Touristen“	147
4.6.1	Ein Ausflug in die Kommunikationstheorie	147
4.6.2	Telefonkonferenzen und Meet-Me-Lines	152
4.6.3	Trennen der Meet-Me-Lines	154
4.6.4	Der Souffleur und Instant Messaging	158
4.6.5	Incident-Touristen verursachen Staus	160
4.6.6	Suchen Sie Verbündete!	165
4.6.7	Statusinformation	166
4.6.8	Beispiel – Durchführung Business-Update	171
4.6.9	Effiziente Telefonkonferenzen – wie lade ich Kollegen aus?	173

4.7	Priorisieren und Maßnahmen einleiten	177
4.7.1	Symptome genau verifizieren	180
4.7.2	Aus Symptomen eine Diagnose formulieren	182
4.7.3	Mit Wissen und Erfahrung vergleichen	183
4.7.4	Ursachen ausschließen anhand der Symptome	186
4.7.5	Die „Unbekannten“ definieren	190
4.7.6	Schritte zur Validierung und Lösungen definieren	192
4.7.7	Prioritäten vergeben und Schritte umsetzen	197
4.8	UAT und Lösung bekannt geben	201
4.9	Close-Down-Phase - Übergabe an das Problem Management	205
4.10	Fehleranalyse und Problemlösungstechniken	209
4.10.1	Problemdefinition	212
4.10.2	Unterschiedsreduktion und Separationsprinzip	213
4.10.3	Brainstorming	215
4.10.4	6-3-5-Methode	216
4.10.5	Ursache- und Wirkungsdiagramm	216
4.10.6	Provokationstechnik	218
4.11	Lessons Learned	219
5	Der Incident Manager	223
5.1	Einleitung	230
5.2	Rollen und Verantwortlichkeiten	232
5.2.1	Rollen	232
5.2.2	Verantwortlichkeiten	234
5.3	Know-how/Skill Set	237
5.3.1	Soft Skills	237
5.3.2	Technisches Know-how	238
5.3.3	Prozess-Know-how	240
5.4	Incident Management Training	241
5.4.1	Schwerpunkte	242
5.4.2	Übungssituationen	243
6	Der Faktor Mensch	247
6.1	Kulturelle Unterschiede	253
6.1.1	Arbeit ohne Grenzen	254
6.1.2	Auch Technologie kennt ihre Grenzen	256
6.1.3	Einflussfaktoren auf das Incident Management	258
6.1.4	Der Faktor Kultur	259
6.2	Internationale Zusammenarbeit	268
6.3	Fehlerkultur	278
6.3.1	Vertuscher	279
6.3.2	Blockierer	281
6.3.3	Mitläufer	281
6.3.4	Antreiber	282

6.4	Persönliche Beziehungen – Relationship	283
6.5	Motivation	285
7	Konzepte	293
7.1	Implementierung des Incident Management	298
7.1.1	Ist-Aufnahme	301
7.1.2	Analyse	304
7.1.3	Design-Phase	305
7.1.4	Implementierung und Optimierung	307
7.2	Help Desk	309
7.2.1	Aufgaben des Help Desk	309
7.2.2	Design und Implementierung Help Desk	311
7.2.3	Help Desk vs. Service Desk	315
7.2.4	Statistische Daten und KPI Help Desk	316
7.2.5	Berechnung der Kosten des IT Service Desk	317
7.3	Outsourcing und Multivendor-Konzept	319
7.3.1	Outsourcing-Konzepte	321
7.3.2	Auswirkungen der Vertragsform auf das Incident Management	338
7.3.3	Outsourcing und SLA	343
7.4	Notfallübung (Fire Drills)	344
7.4.1	Kalter oder theoretischer Fire Drill	345
7.4.2	Wartungsfenster/Changes	346
7.4.3	Heißer Test	347
7.5	Incident Management Center und Situation Command Center	347
7.5.1	Das Incident Management Center (IMC)	347
7.5.2	Situation Command Center (die Kommandozentrale)	352
7.6	Incidents und Follow the Sun	354
7.7	Das IT SWAT Team	360
7.7.1	Grundlagen	360
7.7.2	Stellung im Incident Management	362
7.7.3	Aktivierung	363
7.7.4	Aufbau und Struktur	364
7.8	Die 3Di-Analyse	366
7.8.1	3Di und Technologie	367
7.8.2	3Di und Architektur	367
7.8.3	3Di und Business	368
7.8.4	3Di und Prozesse	369
7.8.5	3Di und Personal	371
7.8.6	3Di und Umwelt	374
7.8.7	Beispiel einer 3Di-Analyse	374
7.9	Der Kreis schließt sich	376
	Index	379