

IT Service Continuity Management

Prävention, IT-Notfallvorsorge, Resilienz

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhalt

Materialien zum Buch	19
1 Einführung: Ihr Weg durch dieses Buch	21
1.1 Besonderheiten dieses Ratgebers	24
1.2 Ich möchte mich kurz vorstellen: Wer schreibt dieses Buch?	25
1.3 Was Sie schon wissen sollten und was Sie lernen werden	27
2 Motivation, Vorgaben und Anforderungen an ein ITSCM	29
2.1 Was ist ITSCM?	32
2.1.1 Prävention und Erhöhung der Resilienz	32
2.1.2 Proaktives Arbeiten	33
2.2 Ziele und Zweck eines ITSCM: Der Nutzen	34
2.2.1 Ziele eines ITSCM	35
2.2.2 Was sind (kritische) IT-Services?	36
2.2.3 Gründe für ein ITSCM	38
2.3 Was ist kein ITSCM?	40
2.4 ITSCM und ITSCMS	44
2.5 Der Zeitfaktor für die Umsetzung eines ITSCM	45
2.6 Anforderungen und Erwartungen an ein ITSCM	45
2.7 Regularien und Vorgaben aus Normen und Gesetzen	46
2.7.1 ISO 27031 (Norm)	47
2.7.2 BSI 200-4 (Standard)	48
2.7.3 NIS 2 (Gesetz)	49
2.7.4 KRITIS (Gesetz)	50
2.7.5 IT-SiG 2.0 (Gesetz)	51
2.7.6 Zusätzliche regulative und normative Vorgaben	51
2.7.7 ITIL	52
2.8 Meldepflichten	53
2.9 Zertifizierung im ITSCM	54
2.10 Woran können Sie sich grundsätzlich orientieren?	55
2.11 Weitere Vorgehensweise und Übungen	56

3	Auf in die Praxis: Wie wird das ITSCM umgesetzt?	57
3.1	Offizielle Benennung einer verantwortlichen Person	57
3.2	Aufbau und Schulung des verantwortlichen Mitarbeiters	59
3.2.1	Welche Schulungen sind wichtig?	61
3.2.2	Internes Schulungsprogramm aufbauen	66
3.2.3	Schulungsstrategie (Ziele) erstellen	66
3.2.4	Schulungskonzept (»Wie?«)	66
3.2.5	Schulungsplan (»Was?«)	67
3.2.6	Hospitationen	70
3.3	Wo sollte das ITSCM organisatorisch verortet werden?	71
3.3.1	ITSCM in einer Stabsstelle (hohe Sichtbarkeit und Durchschlagskraft)	71
3.3.2	Im BCM (meine Empfehlung!)	73
3.3.3	In der Technik	75
3.4	Weitere Vorgehensweise und Übungen	77
4	Die Policy schreiben: Der Arbeitsauftrag	79
4.1	Den Zweck und die Ziele eines ITSCM definieren	80
4.2	Den Geltungsbereich bestimmen	81
4.3	Allgemeine Definitionen	82
4.3.1	Das »Big Picture« (Vorgehensmodell)	82
4.3.2	Rollenbeschreibungen in Kurzform	83
4.3.3	Störungskategorien definieren	85
4.4	Prozesse beschreiben	91
4.5	Die Organisation für den Normal- und den Notbetrieb beschreiben	91
4.6	Die wichtigsten Schnittstellen im Tagesgeschäft in Kurzform vorstellen	92
4.7	Die fünf Standard-Worst-Case-Szenarien kurz benennen	93
4.8	Scoping: den Umfang eines ITSCM definieren	94
4.9	Awareness-Maßnahmen und -Ziele kurz beschreiben	95
4.10	Die Ressourcenfrage klären: Personal, Schulungen, Budget	96
4.11	Die Sicherheit der Dokumentationen beschreiben	98
4.12	Unterschrift und Commitment	99
4.12.1	Aktualisierung der Policy	99
4.12.2	Laufweg einer Policy zur Offizialisierung	100

4.13	Mitteltende Dokumente aufführen	101
4.14	Weitere Vorgehensweise und Übungsaufgaben	101
5	Das ITSCM in Ihrer Organisation:	
	Die Ist-Aufnahme	103
5.1	Die Bestandsaufnahme: Der Ist-Stand	104
5.2	Ist ein Business Continuity Management (BCM) vorhanden?	105
5.2.1	Sind »Zeitkritische Geschäftsprozesse« vorhanden	106
5.2.2	Business-Impact-Analysen (BIAs)	109
5.2.3	Business-Continuity-Pläne (BCP)	111
5.2.4	Risk Assessment (RA) oder Bedrohungsanalyse (BA)	111
5.3	Ist ein Informationssicherheitsmanagement (ISM) vorhanden?	113
5.3.1	Sicherheitskonzepte (SiKos)	114
5.3.2	Risk Assessment (RA)	115
5.4	Ist ein Change-Management (CM oder ChM) vorhanden?	115
5.5	Ist ein Service-Level-Management (SLM) vorhanden?	116
5.6	Gab es schon mal ein ITSCM?	116
5.6.1	Gap-Analysen	117
5.6.2	IT-Notfallvorsorgekonzept, IT-Notfallhandbuch, ITSCM-Handbuch	117
5.6.3	Anforderungsanalyse	117
5.7	Ist ein Risikomanagement (RM) vorhanden?	118
5.8	Ist ein Resilienz-Management (ReM) vorhanden?	119
5.9	Ist ein Lieferanten- bzw. Dienstleistermanagement vorhanden?	119
5.10	Ist eine Configuration Management Database (CMDB) vorhanden?	120
5.11	Ist ein Skill- und Kapazitätsmanagement vorhanden?	120
5.12	Ist ein IT-Architektur-Management (IT-AM) vorhanden?	120
5.13	Vorhandene IT-Infrastrukturpläne sammeln und sichten	121
5.13.1	Netzwerkübersicht (Netzwerkplan)	121
5.13.2	Netzstrukturplan	124
5.14	Technikbereiche zu wichtigen IT-Services und IT-Infrastrukturen befragen	124
5.15	Service-Desk (SD), Help-Desk (HD) und Hotline befragen	125
5.16	Weitere Informationsquellen (Presse, Fachzeitschriften, Newsletter)	125
5.17	Konsolidierung der Informationen	125
5.18	Weitere Vorgehensweise und Übungen	126

6	Das ITSCM planen: Der Soll-Zustand	127
6.1	Der Ist/Soll-Abgleich	128
6.2	Erste Vorsorgemaßnahmen dokumentieren	129
6.2.1	Allgemeines Vorgehen	129
6.3	ITSCM in der Kultur Ihrer Organisation etablieren	131
6.4	Weitere Vorgehensweise und Übungen	131
7	Die ITSCM-Organisation aufbauen	133
7.1	Der Zeitfaktor für den Aufbau	133
7.2	Kosten und Ressourcen	135
7.3	Stellen besetzen (aber wen zuerst?)	136
7.4	Mitarbeiter schulen	138
7.5	Rollen definieren und detailliert beschreiben (Langfassung)	138
7.5.1	Die strategische Ebene (Strategien, Vorgaben, Entscheidungen)	140
7.5.2	Die taktische Ebene (Vorbereitungen und Übersetzung der strategischen Vorgaben)	143
7.5.3	Die operative Ebene (Umsetzung der taktischen Vorgaben in die Praxis)	146
7.6	Dokumente für den Normalbetrieb	153
7.6.1	Die Policy	153
7.6.2	Das IT-Notfallvorsorgekonzept	154
7.6.3	Das Prozessmodell	155
7.6.4	Das ITSC-Lösungskonzept	155
7.6.5	Arbeitsunterlagen, FAQs, Hilfen und Checklisten	163
7.6.6	Das ITSCM-Handbuch kommt später	164
7.7	Dokumente für den Notbetrieb	165
7.7.1	Exkurs: Veränderte Wahrnehmung unter Stress	166
7.7.2	Der ITSC-Plan oder das IT-Notfallhandbuch	168
7.7.3	Der Reaktionsplan	170
7.7.4	Die Koordinationspläne (je Ausfallszenario)	171
7.7.5	Der Wiederanlaufplan (WAP)	172
7.7.6	Der Wiederherstellungsplan (WHP)	173
7.7.7	Disaster-Recovery	173
7.8	Wie organisiert man sich als ITSCM-Team?	173
7.8.1	Per Kanban-Board	174
7.8.2	Per Confluence (Atlassian)	178

7.8.3	Per Microsoft Sharepoint	179
7.8.4	Per Microsoft Teams	179
7.8.5	Per Jour Fixe («Daily« oder tägliche Besprechung)	179
7.8.6	Per zentralem Funktionspostfach	180
7.8.7	Externe Notfallkopien (Backups) einrichten	181
7.9	Weitere Vorgehensweise und Übungen	181
8	Awareness (Bewusstsein) organisationsweit aufbauen	183
8.1	Awareness herstellen	185
8.2	Werbung	187
8.2.1	Intranetseite	188
8.2.2	Newsletter	188
8.2.3	E-Learning-Videos	189
8.2.4	Aufsteller und Plakate	190
8.2.5	Give-Aways	190
8.2.6	Glossare (Wissensmanagement)	191
8.3	Infoveranstaltungen: Vorträge, Schulungen, Workshops, Onboarding etc.	191
8.3.1	Infoveranstaltung(en)	192
8.3.2	Vorträge	192
8.3.3	Schulungen	192
8.3.4	Workshops	193
8.3.5	Awareness durch Übungen und Tests	193
8.3.6	Onboarding	193
8.4	Sprechstunden oder offener Austausch	194
8.5	Awareness adressatengerecht und auf unterschiedlichen Ebenen vermitteln	195
8.5.1	Awareness für alle Mitarbeiter: allgemein, umfassend, verständlich	195
8.5.2	Awareness für alle Führungskräfte: Aufgaben, Ressourcen	196
8.5.3	Awareness für ITSCM-Sponsor, ITSCM-Owner, Top-Management: Planungen, Ergebnisse, Zukunft	196
8.6	Fazit	197
8.7	Weitere Vorgehensweise und Übungen	198

9	Den ITSCM-Prozess definieren	199
9.1	Den ITSCM-Prozess oder -Teilprozess beschreiben	200
9.1.1	Prozesse modellieren und visualisieren	201
9.1.2	Business Process Model and Notation (BPMN)	202
9.2	Der ITSCM-Lifecycle	203
9.2.1	Der komplette ITSCM-Prozess	204
9.2.2	Teilprozess(e)	205
9.3	Der PDCA-Zyklus	209
9.4	Den Kontinuierlichen Verbesserungsprozess (KVP) beschreiben	210
9.4.1	Prozesskritiken (PKs)	210
9.4.2	Prozesspaten	211
9.4.3	Regelmäßige oder anlassbezogene Prüfungen von Prozessen	211
9.4.4	Prozesserkenntnisse aus Übungen und Tests	212
9.4.5	Lessons Learned	213
9.4.6	Presse, Medien, Publikationen, Vernetzungen mit anderen Organisationen	213
9.5	Reifegradmodell aufbauen	214
9.6	Weitere Vorgehensweise und Übungen	216
10	Vernetzungen und Schnittstellen (intern und extern)	219
10.1	Interne Vernetzung	219
10.1.1	Business Continuity Management (BCM)	221
10.1.2	Informationssicherheitsmanagement (ISM)	222
10.1.3	Computer Emergency Response Team (CERT)	223
10.1.4	Krisenmanagement (KM)/Crisis-Management (CM)	225
10.1.5	Service-Level-Management (SLM)	225
10.1.6	Resilienz-Management (ReM)	228
10.1.7	Lieferanten- und Dienstleistungsmanagement	229
10.1.8	Business-Relationship-Management als Kundenschnittstelle (BRM)	230
10.1.9	Skill- und Kapazitätsmanagement (Ressourcenmanagement)	231
10.1.10	Incident-Management (IM)	235
10.1.11	Risikomanagement (RM)	236
10.1.12	Change-Management (CM oder ChM)	239
10.1.13	Problem-Management (PM)	244
10.1.14	Monitoring (Überwachung oder Event-Management)	245

10.1.15	Leitstandtechnik (LST)	247
10.1.16	Qualitätsmanagement (QM)	250
10.1.17	Dokumentenmanagement (DM)	251
10.1.18	IT-Architektur-Management (IT-AM)	252
10.1.19	Die Configuration Management Database (CMDB)	253
10.2	Externe Vernetzung	255
10.2.1	Bundesamt für Sicherheit in der Informationstechnik (BSI)	255
10.2.2	Landeskriminalamt (LKA)	256
10.2.3	Behörden und Organisationen mit Sicherheitsaufgaben (BOS)	257
10.2.4	Teilnehmer von Schulungen, Lehrgängen und Workshops	257
10.2.5	Social Media (z. B. LinkedIn, XING, Facebook, X etc.)	257
10.2.6	Arbeitskreise, Arbeitsgruppen, Communitys, Gremien etc.	258
10.3	Weitere Vorgehensweise und Übungen	259
11	Die Gap-Analyse (Lücken- oder Differenzanalyse)	261
11.1	Sinn und Zweck einer Gap-Analyse	263
11.2	Mit Soll-Vorgaben eine Gap-Analyse durchführen	264
11.2.1	RTO (Recovery Time Objective) und RTA (Recovery Time Actual)	266
11.2.2	RPO (Recovery Point Objective) und RPA (Recovery Point Actual)	269
11.2.3	MBCO (Minimum Business Continuity Objective)	270
11.2.4	MTPD (Maximum Tolerable Period of Disruption)	272
11.2.5	Zusammenfassung: Die Werte abgleichen	273
11.3	Ohne Soll-Vorgaben eine Gap-Analyse durchführen	274
11.3.1	CMDB (Configuration Management Database)	275
11.3.2	SLAs (aus dem SLM)	278
11.3.3	OLAs (aus dem SLM)	280
11.3.4	Schutzbedarfsanalysen (des ISM)	283
11.3.5	Risikomanagement (Risk-Assessment, RA)	284
11.3.6	Informationen aus technischen Bereichen	284
11.4	Vorbereitung der Gap-Analyse	284
11.4.1	Manuelle Datenerhebung (mit Confluence oder Excel)	285
11.4.2	Webgestützte Datenerhebung	287
11.4.3	Zentralisierte Datenerhebung zusammen mit dem BCM	287
11.5	Durchführung einer Gap-Analyse	288
11.5.1	Optimaler Bearbeitungsweg bei der Durchführung einer Gap-Analyse (theoretisches Grundprinzip)	289
11.5.2	Durchführung der Gap-Analyse (detaillierter praktischer Weg)	290

11.6	Auswertung einer Gap-Analyse	293
11.6.1	Verantwortungen klären	294
11.6.2	Die nächste Gap-Analyse planen	295
11.7	Reporting an den Prozess-Owner (Sponsor, BCM etc.)	295
11.8	Weitere Vorgehensweise und Übungen	297
12	IT-Notfallvorsorgemaßnahmen (inklusive Tracking)	299
12.1	Allgemeines Vorgehen	299
12.2	IT-Notfallvorsorgemaßnahmenverfolgung aufbauen	301
12.2.1	IT-Notfallvorsorgemaßnahmen definieren, dokumentieren und priorisieren	302
12.2.2	Verantwortung festlegen (pro IT-Notfallvorsorgemaßnahme)	302
12.2.3	IT-Notfallvorsorgemaßnahme genehmigen bzw. freigeben lassen	303
12.2.4	IT-Notfallvorsorgemaßnahme(n)-Wiedervorlage(n) einrichten	303
12.2.5	Eskalationsweg(e) definieren	304
12.2.6	IT-Notfallvorsorgemaßnahme umsetzen oder nicht umsetzen?	304
12.2.7	IT-Notfallvorsorgemaßnahmen-Controlling und -Berichtswesen einrichten	305
12.3	Weitere Vorgehensweise und Übungen	306
13	IT-Risikomanagement (RA, BA)	307
13.1	Auf BCM- oder ISM-Ergebnisse verweisen	308
13.1.1	Verweis auf das Risk Assessment bzw. die Risiko-Analyse (RA) des ISM	309
13.1.2	Verweis auf die Bedrohungsanalyse (BA) des BCM	309
13.2	Als ITSCM eine Bedrohungsanalyse (BA) durchführen?	309
13.3	Was macht man nun mit den ganzen Ergebnissen?	311
13.4	Allgemeines Risikomanagement (RM)	311
13.5	Praxisbeispiel: Eine Risikomeldung	313
13.6	Weitere Vorgehensweise und Übungen	314
14	Worst-Case-Szenarien (WCS)	315
14.1	Was sind Worst-Case-Szenarien?	316
14.2	Beispiele für Worst-Case-Szenarien	317

14.2.1	Ausfall eines Rechenzentrums	317
14.2.2	Nichtzugänglichkeit eines Rechenzentrums	320
14.2.3	Ausfall der WAN-RZ-Kopplung	322
14.2.4	Ausfall durch kompromittierte IT-Infrastruktur	324
14.2.5	Ausfall Cloud	327
14.2.6	Weitere Worst-Case-Szenarien	332
14.3	Alternativen zu Worst-Case-Szenarien (Ansatz und Ideen)	333
14.3.1	Risiko-Ansatz	334
14.3.2	Incident-Ansatz	334
14.4	Weitere Vorgehensweise und Übungen	335
15	Übungen und Tests	337
15.1	Strategie, Konzept und Plan: Was wird wann wie getestet?	339
15.1.1	Übungs- und Teststrategie erstellen (das »Was?«)	339
15.1.2	Übungs- und Testkonzept (das »Wie?«)	339
15.1.3	Übungs- und Testplanung (konkrete Jahresplanung, das »Wann?«)	341
15.2	Psychologische Aspekte und Soft-Skills beachten	342
15.3	Anforderungen an Übungen und Tests	343
15.3.1	Übungen und Tests planen	343
15.3.2	Übungshygiene (Fingerpointing, Shaming, Blaming etc.)	345
15.3.3	Übungsmüdigkeit	348
15.3.4	Übungskünstlichkeit	348
15.4	Test-Arten definieren	349
15.4.1	Desktop-Test (Einzeltest)	349
15.4.2	Walkthrough-Test (Gruppentest)	350
15.4.3	Funktionstest (auch Teilttest; als Einzel- oder Gruppentest)	351
15.4.4	Simulation (Einzel- und/oder Gruppentest)	351
15.4.5	Vollübung (Real-Test)	352
15.4.6	Review (Nachbearbeitung)	353
15.5	Erhöhung der Resilienz durch Übungen und Tests	354
15.6	Weitere Vorgehensweise und Übungen	355
16	Meldetechniken und Alarmierungsverfahren (Wege und Kanäle)	357
16.1	Welche Alarmierungsverfahren gibt es?	358
16.2	Welche zusätzlichen Alarmierungsverfahren sollte es geben?	359

16.3	Wer muss wie wann und worüber informiert werden?	359
16.4	Weitere Vorgehensweise und Übungen	359
17	Notfallvorsorge durch Resilienz	361
17.1	Technische Resilienz herstellen – aber wie?	363
17.1.1	Resilienz durch technische Vorsorge	363
17.1.2	Resilienz durch Server-Virtualisierung	364
17.1.3	Resilienz durch Storage-Virtualisierung	366
17.1.4	Resilienz durch Clustering	367
17.1.5	Resilienz durch Redundanz	368
17.1.6	Resilienz durch Loadbalancing (Lastverteilung)	371
17.1.7	Resilienz durch die Cloud	372
17.1.8	Resilienz durch ein Datensicherungskonzept	372
17.1.9	Resilienz durch Proxy-Struktur und Firewalls	378
17.1.10	Resilienz durch Netzsegmentierung	378
17.1.11	Resilienz durch Rechte- und Zugriffsmanagement (IAM)	379
17.1.12	Resilienz durch Patchmanagement	380
17.1.13	Resilienz durch Testing- und Staging-Umgebungen	380
17.1.14	Resilienz durch weitere technische Härtenungen	381
17.1.15	Resilienz durch den »Stand der Technik«	382
17.1.16	Resilienz durch Penetrationstests	382
17.1.17	Resilienz durch Kryptografie und Verschlüsselung	383
17.1.18	Resilienz durch eine Notfallarbeitsumgebung per USB-Stick	384
17.2	Nicht technische Resilienz	385
17.2.1	Notlieferabkommen	385
17.2.2	Software-Lizenzen für den Notfall	386
17.2.3	Zugriffe (und Rechte)	387
17.2.4	Standardisierte und optimierte Prozesse	387
17.2.5	Eine gelebte Fehlerkultur etablieren	387
17.2.6	E-Mail-Struktur für den Notfall vorhalten	388
17.2.7	Sicherheitsüberprüfungen (Ü1, Ü2, Ü3)	389
17.2.8	Personal (Skills) redundant aufbauen	389
17.2.9	Notfall-Website aufbauen	389
17.2.10	Externe Kooperationen	390
17.2.11	Aufgaben für das BCM	390
17.3	Weitere Vorgehensweise und Übungen	391
18	Interne und externe (Notfall-)Kommunikation	393
18.1	Wer soll kommunizieren?	393

18.2	Strategien für die Kommunikation	394
18.3	Kommunikationsrollen beschreiben	396
18.4	Kollaborationstools und Kommunikationstools (inklusive Ausweichtools) festlegen	396
18.5	Kommunikationswege und Kanäle beschreiben (inklusive Ausweichmöglichkeiten)	400
18.6	Notfallkommunikation	401
18.7	Notfallalarmierungstools	403
18.8	Weitere Vorgehensweise und Übungen	405
19	Das ITSCM-Handbuch erstellen	407
19.1	Die Vor- und Nachteile eines ITSCM-Handbuches	409
19.2	Inhalte und Aufbau eines ITSCM-Handbuchs	411
19.2.1	ITSCM-Handbücher in der Übersicht	411
19.2.2	Mein ITSCM-Handbuch als Beispiel	418
19.2.3	Weitere Themen für das ITSCM-Handbuch	428
19.3	Notfallbackup des ITSCM-Handbuches	428
19.4	Weitere Vorgehensweise	428
20	Das Tool	431
20.1	Das Tool den Prozessen anpassen oder die Prozesse dem Tool?	431
20.2	Warum brauchen Sie ein Tool?	433
20.3	SaaS oder On Prem?	436
20.3.1	Cloudbasierte Systeme: Software-as-a-Service (SaaS)	436
20.3.2	Serverbasierte Systeme: On Premises	437
20.4	Einführung eines Tools	438
20.4.1	Die Vorplanung	438
20.4.2	Organisatorisches	439
20.4.3	Das Implementierungsprojekt	440
20.4.4	Das Customizing	441
20.5	Betrieb eines Tools	442
20.6	Exit-Strategie festlegen	443
20.7	Einige Anbieter	443
20.8	Weitere Vorgehensweise und Übungen	446

21	Dokumentationen	449
21.1	Notfallbackup der wichtigsten ITSCM-Dokumente	452
21.1.1	Wichtige Dokumente identifizieren	452
21.1.2	Wie und wo sollte man diese Unterlagen ablegen?	453
21.1.3	Wie hält man all diese Dokumente aktuell?	453
21.1.4	Sollen die Dokumente in digitaler Form oder in Papierform vorgehalten werden?	453
21.2	Dokument-Arten	454
21.2.1	Policy (Richtlinie)	455
21.2.2	IT-Notfallvorsorgekonzept	456
21.2.3	ITSCM-Handbuch	456
21.2.4	Reaktionsplan	456
21.2.5	Koordinationspläne	456
21.2.6	Wiederanlaufpläne (WAP)	457
21.2.7	Wiederherstellungspläne (WHP)	458
21.2.8	Desaster-Recovery-Pläne (DRP)	458
21.2.9	Arbeitsunterlage	458
21.2.10	Templates	458
21.2.11	Checklisten	458
21.3	Kontinuierlicher Verbesserungsprozess (KVP) für die Dokumentation	459
21.4	Abhängigkeit der Dokumente (Dokumentenpyramide)	459
21.5	Die Dokumentenablage (Wo?, Wer?, Aktualität?)	461
21.6	Reporting an Prozess-Owner, Prozess-Sponsor, BCM und ISM	463
21.7	Weitere Vorgehensweise und Übungen	464
22	Datenschutz und Datensicherheit	465
22.1	Das Sicherheitskonzept	465
22.2	Archivierung und Aufbewahrungsfristen	466
22.3	Weitere Vorgehensweise und Übungen	467
23	Outsourcing eines ITSCM	469
23.1	Vorteile	470
23.2	Nachteile	471
23.3	Ist Outsourcing eine Alternative?	473
23.4	Weitere Vorgehensweise und Übungen	474

24 Stolpersteine bei Einführung und Betrieb eines ITSCM	475
24.1 Falsche Erwartungshaltungen	475
24.2 Zu viele parallele Aufgaben	476
24.3 Unklarer Auftrag bzw. unklare Aufgaben	476
24.4 Doppelrollen	477
24.5 Nebenbei arbeiten	478
24.6 Fehlendes Commitment	478
24.7 Die häufigsten Probleme im ITSCM	479
24.8 Weitere Vorgehensweise und Übungen	481
25 Qualitätsmessung und Controlling	483
25.1 Self-Assessment	483
25.2 Kennzahlen-Erhebung (KPIs)	484
25.2.1 Informations-KPIs	485
25.2.2 Steuerungs-KPIs	486
25.3 Metriken	486
25.4 Reifegradmodell	487
25.5 Audit	488
25.5.1 Audits planen	488
25.5.2 Ablauf eines Audits	489
25.6 Finaler Check-up	491
25.7 Weitere Vorgehensweise und Übungen	496
26 Cloud-Systeme im ITSCM	499
26.1 Resilienz durch die Cloud	500
26.1.1 Die Vor- und Nachteile der Cloud	501
26.2 Die Aufgaben des ITSCM	503
26.3 Cloud-Systeme überwachen	505
26.4 Weitere Vorgehensweise und Übungen	508

27	Ausblick: To the future ...	509
27.1	Trends	510
27.2	Megatrends	514
27.3	ITSCM und KI	518
27.3.1	Was kann KI leisten?	518
27.3.2	»Wo Licht ist, ist aber auch Schatten«	521
27.3.3	Use-Cases im ITSCM	522
27.4	Weitere Vorgehensweise und Übungen	527
28	Schlussworte: Danke, und bis bald!	529
28.1	Danksagungen	529
28.2	Feedback	531
28.3	Fazit	531
28.3.1	Veränderung von unten: Das Mindset ändern!	532
28.3.2	Veränderung von oben: Das Commitment durch die Führung	533
28.4	Bis bald!	534
 Anhang		
A	Wichtige Links	537
B	Glossar	539
C	Lösungen zu den Übungsaufgaben	581
	Index	583