

**Handbuch des Business Continuity
Management / IT-Notfallhandbuch
gemäß ISO 22301 und ISO 27031**

Inhaltsverzeichnis

Prüfung und Freigabe	2
Änderungshistorie	3
Dokumentensteuerung und Verteilerkreis	4
Abbildungsverzeichnis	8
1 Vorbemerkung zum Business Continuity Management	9
2 Ziel und Zweck des Handbuchs zum Business Continuity Management	10
3 Relevante Normen und Standards	12
4 Abkürzungen	12
5 Begriffe	12
5.1 Anmerkung zum Begriff „IT-Notfall“	13
6 Grundsätze des Business Continuity Management	15
6.1 Zusammenwirken des Business Continuity Management mit dem	16
6.1.1 IT-Betrieb, der Informationssicherheit und dem IT-Risikomanagement	16
6.1.2 Notfall- und Krisenmanagement	17
7 Das Business Continuity Management System	19
7.1 Management und Steuerung des BCMS	21
8 Kontext der Organisation	22
8.1 Verstehen der Organisation und Ihres Kontextes	22
8.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	23
8.2.1 Rechtliche und vertragliche Anforderungen (IT-Compliance)	24
8.3 Festlegung des Anwendungsbereichs des Business Continuity Management Systems	25
8.3.1 Anwendungsbereichs des Business Continuity Management Systems	25
9 Führung	27
9.1 Führung und Verpflichtung	27
9.2 Strategie für das Management und die Steuerung des BCMS	28
9.2.1 Aussagen der strategischen Ausrichtung der Business Continuity	29
9.2.2 Die Strategie der Business Continuity	29
9.2.3 Festlegung der Strategie für die Aufrechterhaltung der Betriebsfähigkeit der IT	31
9.2.4 Bekanntmachung der Strategien für die Aufrechterhaltung der Betriebsfähigkeit der IT	31
9.2.5 Leitlinie zur Business Continuity	31
9.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	32
9.3.1 Aufbauorganisation des Business Continuity Management	33
9.3.2 Zuweisung von organisatorischen Rollen, Verantwortlichkeiten, Befugnissen und Rechenschaftspflichten	35
9.3.3 Der Business Continuity Manager	36
9.3.4 Personen für die Informationsbereitstellung (Informationsgeber)	37
9.3.5 Personen für die Bestimmung und Bewertung der Kritikalität sowie der IT-Risikosteuerung	37
9.3.6 IT-Notfallstab	38

9.3.7 IT-Notfallteam.....	39
10 Planung und Steuerung des BCMS	40
10.1 Umgang mit Risiken.....	41
10.2 Festlegung von Zielen für die Aufrechterhaltung der Betriebsfähigkeit der IT	43
10.2.1 Bestimmung der Zielerfüllung	44
10.3 Planung von Änderungen am BCMS.....	45
11 Unterstützung des Betriebs des BCMS.....	47
11.1 Ressourcen.....	48
11.2 Kompetenzen.....	49
11.2.1 Kompetenzen der beteiligten Personen für den Betrieb des BCMS.....	49
11.2.2 Kompetenzen der Organisation für den Betrieb des BCMS	50
11.3 Awareness, Schulung und Unterweisung.....	52
11.4 Interne und externe Kommunikation.....	52
11.5 Dokumentierte Information	54
11.5.1 Erstellen und Aktualisieren.....	55
11.5.2 Lenkung dokumentierter Informationen	55
11.5.3 Ergänzende Verfahren und mitgeltende Dokumentationen der Dokumentenlenkung	56
12 Betrieb des BCMS	57
12.1 Planung und Steuerung der Aufrechterhaltung der Betriebsfähigkeit der IT.....	58
12.2 Business Impact Analyse.....	59
12.3 Risikobeurteilung	62
12.4 Kontinuitätsstrategien und Lösungskonzepte für die Aufrechterhaltung der Betriebsfähigkeit der IT	66
12.4.1 Identifizierung und Auswahl der Kontinuitätsstrategien und Lösungskonzepte für die Business Continuity	69
12.4.2 Vorhalten und Bereitstellen von Ressourcen und Kompetenzen für die Umsetzung der Lösungskonzepte und Maßnahmen.....	72
12.4.3 Umsetzung von Maßnahmen für die Gewährleistung der Wiederherstellung und Aufrechterhaltung der Betriebsfähigkeit der IT	73
12.4.3.1 Quellen für die Identifikation von Maßnahmen.....	74
12.4.3.2 Organisatorische Maßnahmen	76
12.4.3.3 Personelle Maßnahmen	78
12.4.3.4 Technische Maßnahmen	79
12.4.3.5 Infrastrukturelle Maßnahmen.....	80
12.5 Business Continuity Planning	81
12.5.1 Reaktionsstruktur	82
12.5.2 Management der Information und der Kommunikation.....	84
12.5.3 Management der in Kenntnissetzung, Benachrichtigung, Meldung und Warnung.....	85
12.5.4 Der Business Continuity-Plan	87
12.5.5 Die Reaktionspläne für Sofortmaßnahmen und für die Aufrechterhaltung der Betriebsfähigkeit der IT	90
12.5.6 Anforderungen an die Dokumentation des Business Continuity Planning.....	90

12.6 Bewältigung eines IT-Notfalls und Wiederherstellung	91
12.7 Übungsprogramm	93
12.8 Bewertung der Verfahren für die Aufrechterhaltung der Betriebsfähigkeit der IT.....	96
13 Bewertung der Leistung des BCMS	98
13.1 Überwachung und Messung	98
13.2 Critical Success Factor und Key Performance Indicator des BCMS	100
13.2.1 Bestimmung der kritischen Erfolgsfaktoren (Critical Success Factor)	100
13.2.2 Bestimmung der Schlüsselkennzahlen (Key Performance Indicator).....	101
13.2.2.1 Key Performance Indicator für die Business Continuity	101
13.2.2.2 KPI des Availability Management	103
13.2.2.3 KPI des ITSCM	104
13.3 Analyse und Bewertung	104
13.4 Internes Audit.....	105
13.4.1 Auditprogramme	106
13.5 Managementbewertung	108
13.5.1 Eingaben für die Managementbewertung	109
13.5.2 Ergebnisse der Managementbewertung	110
14 Verbesserung des BCMS	112
14.1 Fortlaufende Verbesserung	113
14.2 Nichtkonformität und Korrekturmaßnahmen.....	114
14.2.1 Korrigierende Maßnahmen	115
14.2.2 Präventive Maßnahmen	116
15 Reporting des BCMS.....	117
16 Liste der Verfahren und mitgeltenden Dokumentationen für die Aufrechterhaltung der Betriebsfähigkeit der IT	118

Abbildungsverzeichnis

Abbildung 1 - Darstellung einer beispielhaften Organisation des Business Continuity Management	35
Abbildung 2 - Integration des Business Continuity Management in relevante Risikobereiche	43
Abbildung 3 - Prozessablauf der Vorbereitung und Durchführung einer Business Impact Analyse (BIA)..	61
Abbildung 4 - Umsetzung eines IT Risk Assessments.....	65
Abbildung 5 - Von der Business Impact Analyse zur Umsetzung des Business Continuity Planning	67
Abbildung 6 - Phasen der IT-Notfallbewältigung und Wiederherstellung beispielhafter Service Level	92

Bitte dieses Dokument an Ihre Organisation anpassen