DIN EN ISO 22301:2014-12 (D)

Sicherheit und Schutz des Gemeinwesens - Business Continuity Management System - Anforderungen (ISO 22301:2012); Deutsche Fassung EN ISO 22301:2014

Inhalt

Seite

Vorwort ... 4

0 Einleitung ... 5
0.1 Allgemeines ... 5
0.2 Das Planen-Durchführen-Prüfen-Handeln-Modell (PDCA-Modell) ... 5
0.3 Bestandteile des PDCA-Modells in dieser Internationalen Norm ... 7

1 Anwendungsbereich ... 8

2 Normative Verweisungen ... 8

3 Begriffe ... 8

4 Kontext der Organisation ... 16
4.1 Verstehen der Organisation und ihres Kontextes ... 16
4.2 Verstehen der Bedürfnisse und Erwartungen der Interessensgruppen ... 17
4.2.1 Allgemeines ... 17
4.2.2 Rechtliche und behördliche Anforderungen ... 17
4.3 Festlegung des Anwendungsbereichs des Business Continuity Managements ... 17
4.3.1 Allgemeines ... 17
4.3.2 Anwendungsbereich des BCMS ... 17
4.4 Business Continuity Management System ... 18

5 Führung ... 18
5.1 Führung und Selbstverpflichtung ... 18
5.2 Selbstverpflichtung der Leitung ... 18
5.3 Leitlinien ... 19
5.4 Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation ... 20

6 Planung ... 20
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten ... 20
6.2 Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit und Pläne zur Zielerreichung ... 20

7 Unterstützung ... 21
7.1 Ressourcen ... 21
7.2 Kompetenz ... 21
7.3 Bewusstseinsbildung ... 21
7.4 Kommunikation ... 22
7.5 Dokumentierte Information ... 22
7.5.1 Allgemeines ... 22
7.5.2 Erstellung und Aktualisierung ... 23
7.5.3 Steuerung dokumentierter Information ... 23

8 Betrieb ... 24
8.1 Ablaufplanung und Kontrolle ... 24
8.2 Business Impact Analyse und Risikobewertung ... 24
8.2.1 Allgemeines ... 24
8.2.2 Business Impact Analyse ... 24
8.2.3 Risikobewertung ... 25
8.3 Strategie zur Aufrechterhaltung der Betriebsfähigkeit ... 25
8.3.1 Festlegung und Auswahl ... 25
8.3.2 Ressourcenbedarf ... 25
8.3.3 Schutz und Schadensminderung ... 26
8.4 Einführung und Umsetzung von Maßnahmen zur Aufrechterhaltung der Betriebsfähigkeit ... 26
8.4.1 Allgemeines ... 26

8.4.2 Struktur zur Reaktion auf einen Zwischenfall 27
8.4.3 Warnung und Kommunikation 27
8.4.4 Pläne zur Aufrechterhaltung der Betriebsfähigkeit 28
8.4.5 Wiederherstellung 29
8.5 Übungen und Überprüfungen 29

9 Leistungsüberprüfung 29
9.1 Überwachung, Messung, Analyse und Bewertung 29
9.1.1 Allgemeines 29
9.1.2 Bewertung der Verfahren zur Aufrechterhaltung der Betriebsfähigkeit 30
9.2 Internes Audit 30
9.3 Managementüberprüfung 31

10 Verbesserung 33
10.1 Abweichungen und Korrekturmaßnahmen 33
10.2 Ständige Verbesserung 33

Literaturhinweise 34