DIN EN ISO 22313:2020-10 (D)

Sicherheit und Resilienz - Business Continuity Management System - Anleitung zur Verwendung von ISO 22301 (ISO 22313:2020); Deutsche Fassung EN ISO 22313:2020

Inhalt

Seite

Europäisches Vorwort 4

Vorwort 5

Einleitung 6

1 Anwendungsbereich 15

2 Normative Verweisungen 15

3 Begriffe 15

4 Kontext der Organisation 16
4.1 Verstehen der Organisation und ihres Kontextes 16
4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien 17
4.2.1 Allgemeines 17
4.2.2 Rechtliche und behördliche Anforderungen 17
4.3 Festlegung des Anwendungsbereichs des Business Continuity Management Systems 18
4.3.1 Allgemeines 18
4.3.2 Anwendungsbereichs des Business Continuity Management Systems 18
4.3.3 Ausschlüsse aus dem Anwendungsbereich 19
4.4 Business Continuity Management System 19

5 Führung 20
5.1 Führung und Verpflichtung 20
5.1.1 Allgemeines 20
5.1.2 Oberste Leitung 20
5.1.3 Andere Managementfunktionen 20
5.2 Politik 21
5.2.1 Erstellen der Politik zur Aufrechterhaltung der Betriebsfähigkeit 21
5.2.2 Kommunikation der Politik zur Aufrechterhaltung der Betriebsfähigkeit 22
5.3 Rollen, Verantwortlichkeiten und Befugnisse 22

6 Planung 24
6.1 Maßnahmen zum Umgang mit Risiken und Chancen 24
6.1.1 Bestimmung von Risiken und Chancen 24
6.1.2 Umgang mit Risiken und Chancen 24
6.2 Ziele zur Aufrechterhaltung der Betriebsfähigkeit und Planung, um diese zu erreichen 25
6.2.1 Festlegung von Zielen zur Aufrechterhaltung der Betriebsfähigkeit 25
6.2.2 Bestimmung der Ziele für die Aufrechterhaltung der Betriebsfähigkeit 25
6.3 Planung von Änderungen am BCMS 26

7 Unterstützung 26
7.1 Ressourcen 26
7.1.1 Allgemeines 26
7.1.2 BCMS-Ressourcen 26
7.2 Kompetenz 27
7.3 Bewusstsein 28
7.4 Kommunikation 30
7.5 Dokumentierte Information 30
7.5.1 Allgemeines 30
7.5.2 Erstellen und Aktualisieren 32

7.5.3 Lenkung dokumentierter Information 32

8 Betrieb 33
8.1 Betriebliche Planung und Steuerung 33
8.1.1 Allgemeines 33
8.1.2 Business Continuity Management 34
8.1.3 Aufrechterhaltung der Betriebsfähigkeit 35
8.2 Business-Impact-Analyse und Risikobeurteilung 36
8.2.1 Allgemeines 36
8.2.2 Business-Impact-Analyse 36
8.2.3 Risikobeurteilung 40
8.3 Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit 42
8.3.1 Allgemeines 42
8.3.2 Festlegung der Strategien und Lösungen 42
8.3.3 Auswahl der Strategien und Lösungen 45
8.3.4 Ressourcenbedarf 46
8.3.5 Umsetzung von Lösungen 53
8.4 Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit 54
8.4.1 Allgemeines 54
8.4.2 Reaktionsstruktur 54
8.4.3 Warnung und Kommunikation 56
8.4.4 Pläne zur Aufrechterhaltung der Betriebsfähigkeit 57
8.4.5 Wiederherstellung 64
8.5 Übungsprogramm 65
8.5.1 Allgemeines 65
8.5.2 Gestaltung des Übungsprogramms 65
8.5.3 Übungen zu Plänen für die Aufrechterhaltung der Betriebsfähigkeit 66
8.6 Bewertung der Dokumentation und Fähigkeiten zur Aufrechterhaltung der Betriebsfähigkeit 70
8.6.1 Allgemeines 70
8.6.2 Messen der Wirksamkeit 71
8.6.3 Ergebnisse 72

9 Bewertung der Leistung 73
9.1 Überwachung, Messung, Analyse und Bewertung 73
9.1.1 Allgemeines 73
9.1.2 Aufbewahrung von Nachweisen 73
9.1.3 Bewertung der Leistung 73
9.2 Internes Audit 73
9.2.1 Allgemeines 73
9.2.2 Auditprogramm(e) 74
9.3 Managementbewertung 74
9.3.1 Allgemeines 74
9.3.2 Eingaben für die Managementbewertung 74
9.3.3 Ergebnisse der Managementbewertung 75

10 Verbesserung 75
10.1 Nichtkonformität und Korrekturmaßnahmen 75
10.1.1 Allgemeines 75
10.1.2 Auftreten von Nichtkonformitäten 76
10.1.3 Aufbewahrung dokumentierter Informationen 76
10.2 Fortlaufende Verbesserung 77

Literaturhinweise 78