Muster-Prüfprogramm

Notfallmanagement und BCM

14 Prüfschritte · BSI 200-4, NIS2

14 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 9 Unterlagen zur Anforderung und die typischen Feststellungen.

BSI-Standard 200-4 · BSI DER.4 · NIS2-Richtlinie Art. 20 · ISO/IEC 27001:2022 Anhang A 5.30 · NIS2-Richtlinie Art. 21 Abs. 2 lit. c · NIS2-Richtlinie Art. 23 · NIS2-Richtlinie Art. 21 Abs. 2 lit. d · ISO/IEC 27001:2022 Anhang A 5.29 · NIS2-Richtlinie Art. 21 Abs. 2 lit. f

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob ein Notfallmanagement besteht, das kritische Geschäftsprozesse und ihre Abhängigkeiten kennt, Vorsorge und Pläne daraus ableitet und durch Übungen belegt, dass die Pläne im Ernstfall tragen. Sie beurteilt auch, ob die Leitung das Thema verantwortet.

GELTUNGSBEREICH

- Notfallmanagement- bzw. BCM-System mit Leitlinie, Rollen, Auswirkungsanalyse, Strategien und Plänen
- IT-Notfallplanung und Wiederanlauf für die kritischen Prozesse
- Krisenkommunikation, Alarmierung und Meldewege
- Nicht Gegenstand: Brandschutz und Arbeitsschutz im Einzelnen, sofern nicht gesondert vereinbart

Prüfschritte 1 bis 3

Schritt 01

BSI-Standard 200-4; BSI DER.4; NIS2-Richtlinie Art. 20

Eine Leitlinie zum Notfallmanagement ist von der Leitung freigegeben und legt Ziele, Geltungsbereich und Verantwortung fest.

Prüfhandlung Leitlinie lesen, Freigabe und Aktualität prüfen und die Berichtslinie zur Leitung nachvollziehen.

Nachweise Leitlinie mit Freigabe, Beschlüsse der Leitung

Schritt 02

BSI-Standard 200-4; BSI DER.4

Rollen für das Notfallmanagement sind besetzt, einschließlich Notfallbeauftragten und Krisenstab, mit Vertretungsregelung.

Prüfhandlung Rollenbeschreibungen, Besetzung und Vertretungen prüfen und stichprobenhaft erreichbare Kontaktdaten testen.

Nachweise Rollenbeschreibungen, Besetzungsliste, Kontaktliste

Schritt 03

BSI-Standard 200-4; BSI DER.4

Eine Auswirkungsanalyse hat die kritischen Prozesse, ihre Wiederanlaufzeiten und ihre Abhängigkeiten ermittelt.

Prüfhandlung Methodik und Ergebnisse lesen, Prozesse und Abhängigkeiten stichprobenhaft mit den Fachbereichen bestätigen.

Nachweise Auswirkungsanalyse, Prozessliste mit Wiederanlaufzeiten, Abhängigkeitsübersicht

Prüfschritte 4 bis 6

Schritt 04 — BSI-Standard 200-4

Notfallszenarien und ihre Eintrittswahrscheinlichkeit sind bewertet, die Ergebnisse fließen in die Planung ein.

Prüfhandlung Risikoanalyse zu Notfällen ansehen und prüfen, ob Szenarien wie Ausfall von Standort, Dienstleister, IT oder Personal enthalten sind.

Nachweise Risikoanalyse, Szenarienliste

Schritt 05 — BSI-Standard 200-4

Aus der Analyse sind Fortführungs- und Wiederanlaufstrategien mit den nötigen Ressourcen abgeleitet und beschlossen.

Prüfhandlung Strategien und Ressourcenplanung mit den Ergebnissen der Auswirkungsanalyse abgleichen.

Nachweise Strategiedokumente, Budget- und Ressourcenplanung

Schritt 06 — BSI DER.4

Notfall- und Wiederanlaufpläne bestehen für die kritischen Prozesse und stehen im Ernstfall auch ohne die Hauptumgebung zur Verfügung.

Prüfhandlung Pläne für zwei kritische Prozesse lesen und feststellen, wo sie abgelegt sind und ob sie offline erreichbar sind.

Nachweise Notfallpläne, Ablagekonzept, Zugriffsnachweis

Prüfschritte 7 bis 10

Schritt 07 — ISO/IEC 27001:2022 Anhang A 5.30; NIS2-Richtlinie Art. 21 Abs. 2 lit. c

Wiederanlaufzeiten und zulässiger Datenverlust der IT stimmen mit den Anforderungen der Prozesse überein.

Prüfhandlung Vorgaben der Prozesse mit den technischen Möglichkeiten der IT und den Ergebnissen von Wiederherstellungstests vergleichen.

Nachweise Gegenüberstellung der Vorgaben, Testprotokolle der IT

Schritt 08 — BSI DER.4; NIS2-Richtlinie Art. 23

Alarmierung, interne und externe Kommunikation sowie die Meldewege für erhebliche Sicherheitsvorfälle sind festgelegt.

Prüfhandlung Kommunikationsplan lesen und den Meldeweg an einem Beispiel nachvollziehen, einschließlich der Fristen.

Nachweise Kommunikationsplan, Alarmierungsliste, Meldevorlagen

Schritt 09 — NIS2-Richtlinie Art. 21 Abs. 2 lit. d

Abhängigkeiten von Dienstleistern sind erfasst und im Notfall durch Zusagen abgesichert.

Prüfhandlung Kritische Dienstleister aus der Auswirkungsanalyse auswählen und vertragliche Zusagen zu Verfügbarkeit und Unterstützung im Notfall prüfen.

Nachweise Dienstleisterliste, Verträge, Bestätigungen des Anbieters

Schritt 10 — BSI-Standard 200-4; BSI DER.4; ISO/IEC 27001:2022 Anhang A 5.30

Übungen und Tests sind geplant, werden durchgeführt und ausgewertet, die Ergebnisse führen zu Verbesserungen.

Prüfhandlung Übungsplan und Berichte der letzten zwei Jahre prüfen und feststellen, welche Maßnahmen aus den Ergebnissen folgten.

Nachweise Übungsplan, Übungsberichte, Maßnahmenliste

Prüfschritte 11 bis 14

Schritt 11 — BSI DER.4

Beteiligte werden geschult und für ihre Aufgaben im Notfall sensibilisiert.

Prüfhandlung Schulungsplan und Teilnahmelisten prüfen und stichprobenhaft Beteiligte nach ihren Aufgaben fragen.

Nachweise Schulungsplan, Teilnahmelisten

Schritt 12 — ISO/IEC 27001:2022 Anhang A 5.29

Während einer Störung bleiben Sicherheitsmaßnahmen wie Zugriffskontrollen im Notbetrieb wirksam.

Prüfhandlung Notbetriebsverfahren auf vorgesehene Ausnahmen bei Zugriffs- und Schutzmaßnahmen und deren Genehmigung prüfen.

Nachweise Notbetriebsverfahren, Ausnahmegenehmigungen

Schritt 13 — BSI-Standard 200-4

Pläne werden bei Änderungen und nach Vorfällen aktualisiert und mit Versionsstand geführt.

Prüfhandlung Änderungshistorie der Pläne mit Organisationsänderungen und Vorfällen des letzten Jahres abgleichen.

Nachweise Versionshistorie, Vorfallberichte, Änderungsanträge

Schritt 14 — BSI-Standard 200-4; NIS2-Richtlinie Art. 21 Abs. 2 lit. f

Die Leitung überprüft das Notfallmanagement regelmäßig und entscheidet über Verbesserungen.

Prüfhandlung Managementbewertungen und Berichte der letzten zwei Jahre ansehen und Beschlüsse nachverfolgen.

Nachweise Managementbewertung, Berichte, Beschlüsse

Unterlagenanforderung

Diese 9 Unterlagen vor Prüfungsbeginn anfordern

1. Leitlinie zum Notfallmanagement
2. Rollenbeschreibungen, Besetzungs- und Kontaktliste
3. Auswirkungsanalyse mit Prozessliste und Wiederanlaufzeiten
4. Risikoanalyse und Szenarienliste
5. Notfall- und Wiederanlaufpläne für die kritischen Prozesse
6. Kommunikations- und Alarmierungsplan
7. Übungsplan und Übungsberichte der letzten zwei Jahre
8. Verträge und Zusagen kritischer Dienstleister
9. Managementbewertung zum Notfallmanagement

TYPISCHE FESTSTELLUNGEN

- Die Auswirkungsanalyse ist veraltet oder deckt wesentliche Prozesse nicht ab.
- Pläne liegen nur auf Systemen, die im Ernstfall ausfallen würden.
- Übungen beschränken sich auf Planspiele am Tisch, ein technischer Wiederanlauf wurde nie getestet.
- Wiederanlaufzeiten der Prozesse und Möglichkeiten der IT passen nicht zusammen.
- Rollen sind nicht besetzt oder Kontaktdaten sind überholt.
- Pläne wurden nach Organisationsänderungen nicht angepasst.

Bibliothek Muster-Prüfprogramme

29 Muster-Prüfprogramme online

proauditmap.com/pruefprogramme/

Vollständiges Prüfpaket in ProAuditMap

proauditmap.com

ProAuditMap

Muster ohne Gewähr und keine Rechtsberatung. Gesetze, Verordnungen und Standards erscheinen nur als Fundstelle, Normtexte sind nicht abgedruckt. Passen Sie Umfang und Tiefe vor der Verwendung an Ihre Organisation, Ihre Risiken und die aktuelle Fassung der für Sie geltenden Vorschriften an. Stand: 13. Oktober 2026