Muster-Prüfprogramm

Security Awareness und Schulung

13 Prüfschritte · NIS2, ISO 27001, BSI

13 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 8 Unterlagen zur Anforderung und die typischen Feststellungen.

BSI ORP.3 · ISO/IEC 27001:2022 Anhang A 6.3 · DORA Art. 13 Abs. 6 · ISO/IEC 27001:2022 Kapitel 7.3 · NIS2-Richtlinie Art. 20 Abs. 2 · § 38 Abs. 3 BSIG · NIS2-Richtlinie Art. 21 Abs. 2 lit. g · § 30 Abs. 2 Nr. 7 BSIG · ISO/IEC 27001:2022 Kapitel 7.2 · ISO/IEC 27001:2022 Kapitel 9.1 · ISO/IEC 27001:2022 Anhang A 6.8 · Art. 39 Abs. 1 lit. b DSGVO · DORA Art. 5 Abs. 2 lit. g

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation ein Konzept zur Sensibilisierung und Schulung in Informationssicherheit hat, das alle Zielgruppen einschließlich Geschäftsleitung, IT-Personal und Dienstleistern erreicht. Sie beurteilt außerdem, ob Teilnahme nachverfolgt, Wirksamkeit gemessen und das Melden von Auffälligkeiten gefördert wird.

GELTUNGSBEREICH

- Sensibilisierungs- und Schulungsangebote zur Informationssicherheit für alle Beschäftigten
- Schulungen der Geschäftsleitung und Fachschulungen für IT-Personal und Administratoren
- Phishing-Simulationen, Lernplattform und Teilnahmeverfolgung
- Nicht Gegenstand: allgemeine fachliche Weiterbildung ohne Sicherheitsbezug

Prüfschritte 1 bis 3

Schritt 01 — BSI ORP.3; ISO/IEC 27001:2022 Anhang A 6.3

Ein Konzept regelt Ziele, Zielgruppen, Inhalte, Formate und Turnus der Sensibilisierung und Schulung.

Prüfhandlung Konzept lesen, Freigabe und Aktualität prüfen und mit dem Schulungsplan des laufenden Jahres abgleichen.

Nachweise Sensibilisierungs- und Schulungskonzept, Jahresplan

Schritt 02 — DORA Art. 13 Abs. 6; BSI ORP.3

Inhalte sind auf Rollen und Risiken der Zielgruppen zugeschnitten.

Prüfhandlung Für drei Zielgruppen die Inhalte mit typischen Risiken der Tätigkeit vergleichen.

Nachweise Schulungsunterlagen je Zielgruppe

Schritt 03 — ISO/IEC 27001:2022 Anhang A 6.3; ISO/IEC 27001:2022 Kapitel 7.3

Neue Mitarbeitende werden vor oder unmittelbar mit dem Zugang zu Informationen eingewiesen; alle nehmen regelmäßig teil.

Prüfhandlung Für zehn Eintritte das Datum der Einweisung mit dem Datum der Kontoeinrichtung vergleichen.

Nachweise Eintrittsliste, Teilnahmenachweise, Kontoerstellungsdaten

Prüfschritte 4 bis 6

Schritt 04 — NIS2-Richtlinie Art. 20 Abs. 2; § 38 Abs. 3 BSIG

Mitglieder der Geschäftsleitung nehmen regelmäßig an Schulungen zu Cyberrisiken teil.

Prüfhandlung Teilnahmenachweise der Leitung der letzten zwei Jahre und Inhalte der Schulung prüfen.

Nachweise Teilnahmenachweise, Schulungsunterlagen der Leitung

Schritt 05 — NIS2-Richtlinie Art. 21 Abs. 2 lit. g; § 30 Abs. 2 Nr. 7 BSIG

Grundlegende Verhaltensregeln der Cyberhygiene werden vermittelt und sind leicht auffindbar.

Prüfhandlung Verhaltensregeln im Intranet suchen lassen und bei fünf Mitarbeitenden Kenntnis wichtiger Regeln erfragen.

Nachweise Verhaltensregeln, Interviewnotizen

Schritt 06 — ISO/IEC 27001:2022 Kapitel 7.2

IT-Personal und Administratoren erhalten Fachschulungen, die ihre Kompetenz für Sicherheitsaufgaben sichern.

Prüfhandlung Kompetenzanforderungen für zwei IT-Rollen mit Schulungsnachweisen vergleichen.

Nachweise Kompetenzprofile, Schulungsnachweise, Zertifikate

Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Anhang A 6.3; BSI ORP.3

Phishing-Simulationen werden regelmäßig durchgeführt, ausgewertet und mit Lernangeboten verbunden.

Prüfhandlung Ergebnisse der letzten Simulationen ansehen: Klickquote, Meldequote und Folgemaßnahmen.

Nachweise Auswertungen der Simulationen, Folgeschulungen

Schritt 08 — ISO/IEC 27001:2022 Anhang A 6.3

Die Teilnahme wird verfolgt; ausstehende Pflichtschulungen werden erinnert und eskaliert.

Prüfhandlung Teilnahmequote je Bereich abrufen und den Umgang mit Säumigen nachvollziehen.

Nachweise Teilnahmebericht, Erinnerungen, Eskalationen

Schritt 09 — ISO/IEC 27001:2022 Kapitel 9.1

Die Wirksamkeit der Maßnahmen wird gemessen und in die Planung zurückgeführt.

Prüfhandlung Kennzahlen zur Wirksamkeit ansehen und prüfen, ob Ergebnisse zu Anpassungen des Programms geführt haben.

Nachweise Kennzahlenbericht, Anpassungen im Schulungsplan

Prüfschritte 10 bis 13

Schritt 10 — ISO/IEC 27001:2022 Anhang A 6.8

Mitarbeitende kennen den Meldeweg für Sicherheitsereignisse und nutzen ihn.

Prüfhandlung Zahl der Meldungen über die Zeit auswerten und bei fünf Mitarbeitenden den Meldeweg erfragen.

Nachweise Meldestatistik, Interviewnotizen

Schritt 11 — DORA Art. 13 Abs. 6

Dienstleister mit Zugriff auf Systeme oder Informationen sind in die Sensibilisierung einbezogen.

Prüfhandlung Verträge und Teilnahmenachweise für zwei Dienstleister mit Zugriff prüfen.

Nachweise Vertragsklauseln, Teilnahmenachweise der Dienstleister

Schritt 12 — Art. 39 Abs. 1 lit. b DSGVO

Schulungen zum Datenschutz sind mit dem Datenschutzbeauftragten abgestimmt.

Prüfhandlung Abstimmung der Inhalte und Zuständigkeiten zwischen Informationssicherheit und Datenschutz erfragen.

Nachweise Schulungsplan Datenschutz, Abstimmungsprotokoll

Schritt 13 — DORA Art. 5 Abs. 2 lit. g

Für Sensibilisierung und Schulung sind Budget und Verantwortliche festgelegt.

Prüfhandlung Budget und Ressourcen des Programms ansehen und mit dem Umfang des Jahresplans vergleichen.

Nachweise Budgetplanung, Rollenbeschreibung

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Sensibilisierungs- und Schulungskonzept
2. Jahresplan der Schulungen
3. Schulungsunterlagen je Zielgruppe
4. Teilnahmeberichte je Bereich
5. Teilnahmenachweise der Geschäftsleitung
6. Auswertungen der Phishing-Simulationen
7. Kennzahlen zur Wirksamkeit
8. Meldestatistik für Sicherheitsereignisse

TYPISCHE FESTSTELLUNGEN

- Schulungen sind für alle gleich und berücksichtigen keine Rollen.
- Neue Mitarbeitende erhalten Zugang Wochen vor ihrer ersten Schulung.
- Die Geschäftsleitung ist von Pflichtschulungen ausgenommen.
- Teilnahmequoten sind niedrig, Säumige werden nicht nachverfolgt.
- Phishing-Simulationen werden durchgeführt, aber nicht ausgewertet.
- Dienstleister mit Administratorzugriff sind nicht einbezogen.

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