Muster-Prüfprogramm

Sicherheitsvorfälle und Meldewesen

13 Prüfschritte · NIS2, DORA, ISO 27001

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

ISO/IEC 27001:2022 Anhang A 5.24 · BSI DER.2.1 · NIS2-Richtlinie Art. 21 Abs. 2 lit. b · ISO/IEC 27001:2022 Anhang A 6.8 · ISO/IEC 27001:2022 Anhang A 5.25 · DORA Art. 18(1) · DORA Art. 17(2) · ISO/IEC 27001:2022 Anhang A 5.26 · DORA Art. 17(3) · ISO/IEC 27001:2022 Anhang A 5.28 · BSI DER.2.2 · NIS2-Richtlinie Art. 23 · § 32 Abs. 1 BSIG · DORA Art. 19(1) und (4) · DSGVO Art. 33(1) und (5) · DSGVO Art. 33(2) · ISO/IEC 27001:2022 Anhang A 5.20 · NIS2-Richtlinie Art. 20 · ISO/IEC 27001:2022 Anhang A 5.27

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation einen Prozess für Informationssicherheitsvorfälle betreibt, der Meldung, Bewertung, Einstufung, Eindämmung, Wiederherstellung und Nachbereitung umfasst. Sie beurteilt außerdem, ob die Meldepflichten gegenüber Behörden, Aufsicht und Betroffenen mit ihren Fristen erfüllt werden können und ob Verantwortlichkeiten und Vertretungen geklärt sind.

GELTUNGSBEREICH

- Sicherheitsvorfälle in IT, Anwendungen, Netzen und bei Dienstleistern, die Auswirkungen auf Vertraulichkeit, Integrität oder Verfügbarkeit haben
- Meldewege innerhalb der Organisation und an Behörden, Aufsicht, Kunden und Betroffene
- Beteiligte Stellen: Informationssicherheit, IT-Betrieb, Datenschutz, Recht, Kommunikation und Leitung
- Nicht Gegenstand: die technische Forensik im Einzelfall und die Vorfallbehandlung im Bereich der physischen Sicherheit

Prüfschritte 1 bis 3

Schritt 01 ISO/IEC 27001:2022 Anhang A 5.24; BSI DER.2.1; NIS2-Richtlinie Art. 21 Abs. 2 lit. b

Ein Prozess zur Behandlung von Sicherheitsvorfällen besteht, ist freigegeben und legt Rollen, Abläufe und Eskalation fest.

Prüfhandlung Prozessbeschreibung lesen, Freigabe und Aktualität prüfen und Rollen mit der Organisation abgleichen.

Nachweise Prozessbeschreibung mit Freigabe, Rollenübersicht, Eskalationsplan

Schritt 02 ISO/IEC 27001:2022 Anhang A 6.8

Beschäftigte und Dienstleister kennen den Meldeweg für Ereignisse und können Auffälligkeiten jederzeit melden.

Prüfhandlung Meldekanal und Bekanntmachung prüfen und bei zwei Fachbereichen erfragen, wie gemeldet wird.

Nachweise Meldeweg im Intranet, Schulungsunterlagen, Befragungsnotizen

Schritt 03 ISO/IEC 27001:2022 Anhang A 5.25; DORA Art. 18(1)

Ereignisse werden bewertet und anhand festgelegter Kriterien als Vorfall eingestuft; die Einstufung berücksichtigt Auswirkungen, Dauer und betroffene Daten oder Dienste.

Prüfhandlung Zehn Ereignisse der letzten zwölf Monate auswählen und die Einstufung anhand der Kriterien nachvollziehen.

Nachweise Einstufungsschema, Ereignis- und Vorfallsregister

Prüfschritte 4 bis 6

Schritt 04 DORA Art. 17(2); ISO/IEC 27001:2022 Anhang A 5.26

Alle Vorfälle werden in einem Register erfasst, mit Ursache, Auswirkung, Maßnahmen und Status.

Prüfhandlung Register auf Vollständigkeit der Angaben prüfen und mit Meldungen aus Überwachung und Service Desk abgleichen.

Nachweise Vorfallsregister, Auswertung von Service Desk und Überwachung

Schritt 05 ISO/IEC 27001:2022 Anhang A 5.26; DORA Art. 17(3)

Für die Behandlung stehen Reaktionspläne zur Verfügung, die Eindämmung, Beseitigung und Wiederherstellung beschreiben und Entscheidungsbefugnisse festlegen.

Prüfhandlung Reaktionspläne lesen und an zwei abgeschlossenen Vorfällen prüfen, ob sie angewendet wurden.

Nachweise Reaktionspläne, Vorfallsakten, Entscheidungsprotokolle

Schritt 06 ISO/IEC 27001:2022 Anhang A 5.28; BSI DER.2.2

Beweise werden gesichert, sodass Vorfälle später nachvollziehbar und rechtlich verwertbar bleiben.

Prüfhandlung Verfahren zur Beweissicherung und seine Anwendung in zwei Vorfällen prüfen.

Nachweise Verfahrensbeschreibung, Nachweise der Sicherung, Protokoll der Beweiskette

Prüfschritte 7 bis 9

Schritt 07

NIS2-Richtlinie Art. 23; § 32 Abs. 1 BSIG

Die Organisation kann erhebliche Sicherheitsvorfälle innerhalb der Fristen melden: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussmeldung nach einem Monat.

Prüfhandlung Meldeprozess mit Zuständigkeiten, Vorlagen und Erreichbarkeit nachvollziehen und einen Meldefall oder eine Übung auf die Einhaltung der Fristen prüfen.

Nachweise Meldeprozess, Vorlagen, Kontaktliste der Behörde, Nachweis der Übung oder Meldung

Schritt 08

DORA Art. 19(1) und (4)

Für Finanzunternehmen: Schwerwiegende IKT-Vorfälle werden an die zuständige Behörde gemeldet, in Erstmeldung, Zwischenbericht und Abschlussbericht.

Prüfhandlung Prüfen, ob Meldewege, Vorlagen und Zuständigkeiten für die drei Meldestufen festgelegt sind und angewendet wurden.

Nachweise Meldeprozess, Vorlagen, Nachweise der Meldungen

Schritt 09

DSGVO Art. 33(1) und (5)

Verletzungen des Schutzes personenbezogener Daten werden bewertet und, soweit erforderlich, binnen 72 Stunden an die Aufsichtsbehörde gemeldet; Verletzungen werden dokumentiert.

Prüfhandlung Verfahren zur Bewertung prüfen, die Zusammenarbeit mit dem Datenschutz klären und Dokumentation sowie Meldungen der letzten zwölf Monate ansehen.

Nachweise Verfahren zur Meldung von Datenpannen, Dokumentation der Verletzungen, Meldungen

Prüfschritte 10 bis 13

Schritt 10 DSGVO Art. 33(2); ISO/IEC 27001:2022 Anhang A 5.20

Dienstleister sind verpflichtet, Vorfälle unverzüglich zu melden, und der Meldeweg ist vereinbart.

Prüfhandlung Verträge von drei Dienstleistern auf Meldefristen und Ansprechpersonen prüfen.

Nachweise Vertragsklauseln, Kontaktlisten

Schritt 11 NIS2-Richtlinie Art. 20; DORA Art. 17(3)

Leitung und betroffene Bereiche werden bei erheblichen Vorfällen unterrichtet, die Kommunikation nach außen ist geregelt.

Prüfhandlung Eskalation und Berichte an die Leitung in den Vorfällen der Stichprobe nachvollziehen und das Kommunikationskonzept lesen.

Nachweise Eskalationsprotokolle, Berichte an die Leitung, Kommunikationskonzept

Schritt 12 ISO/IEC 27001:2022 Anhang A 5.27; DORA Art. 17(2)

Nach erheblichen Vorfällen findet eine Nachbetrachtung statt, deren Ergebnisse in Maßnahmen, Schulung und Anpassung der Prozesse einfließen.

Prüfhandlung Nachbetrachtungen der letzten zwölf Monate ansehen und die Umsetzung der Maßnahmen prüfen.

Nachweise Berichte der Nachbetrachtung, Maßnahmenliste, Änderungen an Plänen

Schritt 13 ISO/IEC 27001:2022 Anhang A 5.24

Der Vorfallsprozess wird geübt und die Meldefähigkeit regelmäßig getestet.

Prüfhandlung Übungsprotokolle der letzten zwölf Monate ansehen und prüfen, ob Meldeweg und Fristen Teil der Übung waren.

Nachweise Übungsplanung, Übungsprotokolle, Befunde

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Prozessbeschreibung zum Management von Sicherheitsvorfällen
2. Einstufungsschema und Reaktionspläne
3. Vorfallsregister der letzten zwölf Monate
4. Meldeprozess mit Vorlagen, Zuständigkeiten und Kontaktlisten der Behörden
5. Nachweise abgesetzter Meldungen oder durchgeführter Übungen
6. Dokumentation von Verletzungen des Schutzes personenbezogener Daten
7. Vertragsklauseln zur Meldung von Vorfällen bei Dienstleistern
8. Berichte der Nachbetrachtung

TYPISCHE FESTSTELLUNGEN

- Vorfälle werden in verschiedenen Systemen erfasst, ein vollständiges Register fehlt.
- Es gibt keine festgelegten Kriterien für die Einstufung, die Bewertung hängt von der handelnden Person ab.
- Zuständigkeit und Vertretung für Meldungen an Behörden sind nicht geklärt, Fristen würden nicht eingehalten.
- Der Datenschutz wird bei Vorfällen mit Personenbezug erst spät eingebunden.
- Dienstleister sind nicht zur schnellen Meldung verpflichtet.
- Nachbetrachtungen finden nicht statt oder führen nicht zu verfolgten Maßnahmen.

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