Muster-Prüfprogramm

Logging und Monitoring

12 Prüfschritte · ISO 27001, BSI, DORA

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

ISO/IEC 27001:2022 Anhang A 8.15 · BSI OPS.1.1.5 · ISO/IEC 27001:2022 Anhang A 8.17 · ISO/IEC 27001:2022 Anhang A 8.16 · BSI DER.1 · DORA Art. 10(1) und (2) · DORA Art. 10(2) · DORA Art. 10(3) · DORA Art. 10(1) · BSI DER.2.1 · ISO/IEC 27001:2022 Anhang A 8.15 und 5.22

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation festgelegt hat, welche Ereignisse in welchen Systemen protokolliert werden, ob die Protokolle vor Veränderung geschützt sind und ob eine wirksame Überwachung Auffälligkeiten erkennt und in die Behandlung von Sicherheitsvorfällen überführt. Sie beurteilt außerdem, ob Zeitquellen abgestimmt sind, damit Ereignisse systemübergreifend nachvollziehbar bleiben.

GELTUNGSBEREICH

- Server, Datenbanken, Verzeichnisdienste, Netzkomponenten, Firewalls und Anwendungen, die für wesentliche Dienste genutzt werden
- Zentrale Protokollsammlung, SIEM oder vergleichbare Auswertung sowie Alarmierungswege
- Betrieb durch eigene Mitarbeitende und durch Dienstleister, soweit sie Protokolle erzeugen oder auswerten
- Nicht Gegenstand: Videoüberwachung und die Protokollierung von Kundenanwendungen, sofern nicht gesondert vereinbart

Prüfschritte 1 bis 3

Schritt 01 ISO/IEC 27001:2022 Anhang A 8.15; BSI OPS.1.1.5

Eine Richtlinie legt fest, welche Ereignisse zu protokollieren sind, wie lange Protokolle aufbewahrt werden und wer sie auswertet.

Prüfhandlung Richtlinie lesen, Freigabe und Aktualität feststellen und mit der Systemübersicht abgleichen.

Nachweise Protokollierungsrichtlinie mit Freigabevermerk, Systemübersicht

Schritt 02 ISO/IEC 27001:2022 Anhang A 8.15

Für wesentliche Systeme sind die zu erfassenden Ereignisse festgelegt, darunter Anmeldungen, Rechteänderungen, Zugriffe auf sensible Daten und Konfigurationsänderungen.

Prüfhandlung Fünf wesentliche Systeme auswählen und die tatsächlich aktivierten Protokollquellen mit der Festlegung vergleichen.

Nachweise Protokollkonzept je System, Konfigurationsauszüge der Protokollierung

Schritt 03 ISO/IEC 27001:2022 Anhang A 8.15; BSI OPS.1.1.5

Protokolle werden zentral gesammelt, vor Änderung und Löschung geschützt und für die festgelegte Dauer aufbewahrt.

Prüfhandlung Zugriffsrechte auf die Protokollablage prüfen und stichprobenweise Protokolle aus dem Aufbewahrungszeitraum abrufen.

Nachweise Berechtigungsauszug der Protokollablage, Aufbewahrungseinstellungen, Abrufbeispiele

Prüfschritte 4 bis 6

Schritt 04 — ISO/IEC 27001:2022 Anhang A 8.15

Administratoren können Protokolle ihrer eigenen Tätigkeit weder verändern noch löschen.

Prüfhandlung Prüfen, ob privilegierte Konten Schreib- oder Löschrechte auf Protokolle besitzen, und die Trennung der Rollen nachvollziehen.

Nachweise Rollenmatrix, Berechtigungsauszug, Konfiguration der Protokollweiterleitung

Schritt 05 — ISO/IEC 27001:2022 Anhang A 8.17

Die Uhren der Systeme sind auf abgestimmte Zeitquellen synchronisiert, sodass Ereignisse über Systeme hinweg einander zugeordnet werden können.

Prüfhandlung Zeitquellen und Abweichungen auf einer Stichprobe von Servern und Netzkomponenten auslesen.

Nachweise Konfiguration der Zeitdienste, Auslesung der Zeitabweichung

Schritt 06 — ISO/IEC 27001:2022 Anhang A 8.16; BSI DER.1; DORA Art. 10(1) und (2)

Es besteht eine Überwachung, die Auffälligkeiten in Netzen, Systemen und Anwendungen erkennt, mit festgelegten Schwellen und Regeln für Alarme.

Prüfhandlung Regelwerk der Überwachung ansehen, Abdeckung der wesentlichen Systeme abgleichen und Schwellenwerte erfragen.

Nachweise Regelkatalog der Überwachung, Abdeckungsübersicht, Beschreibung der Schwellen

Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Anhang A 8.16; DORA Art. 10(2)

Alarme erreichen die zuständigen Personen zeitnah, werden bewertet und bis zur Erledigung nachverfolgt.

Prüfhandlung Zehn Alarme der letzten sechs Monate auswählen und Eingang, Bewertung, Reaktionszeit und Abschluss nachvollziehen.

Nachweise Alarmliste, Tickets, Bereitschaftsplan

Schritt 08 — DORA Art. 10(3); BSI DER.1

Für die Überwachung stehen ausreichend qualifiziertes Personal und Zeiten zur Verfügung, auch außerhalb der Geschäftszeiten.

Prüfhandlung Besetzung, Bereitschaftsmodell und Vertretungsregeln mit dem Alarmaufkommen vergleichen.

Nachweise Dienstplan, Bereitschaftsregelung, Statistik des Alarmaufkommens

Schritt 09 — DORA Art. 10(1); ISO/IEC 27001:2022 Anhang A 8.16

Die Überwachung wird regelmäßig auf Wirksamkeit getestet, etwa durch simulierte Ereignisse, und Lücken werden behoben.

Prüfhandlung Testprotokolle der letzten zwölf Monate ansehen und prüfen, ob Befunde zu Anpassungen der Regeln geführt haben.

Nachweise Testberichte, Regeländerungen, Maßnahmenliste

Prüfschritte 10 bis 12

Schritt 10

BSI DER.1; BSI DER.2.1

Ereignisse mit Sicherheitsbezug werden in die Behandlung von Sicherheitsvorfällen überführt und dort klassifiziert.

Prüfhandlung Für drei Alarme prüfen, ob und wie sie als Sicherheitsvorfall erfasst und bewertet wurden.

Nachweise Vorfallsregister, Verknüpfung von Alarm und Vorfall

Schritt 11

ISO/IEC 27001:2022 Anhang A 8.15 und 5.22

Protokolle von Dienstleistern und Cloud-Diensten sind verfügbar und werden in die Auswertung einbezogen.

Prüfhandlung Für zwei ausgelagerte Dienste prüfen, welche Protokolle bereitgestellt werden und ob sie in die Überwachung einfließen.

Nachweise Vertragsklauseln zu Protokollen, Anbindung der Protokollquellen

Schritt 12

Praxisanforderung

Datenschutz bei Protokollen ist geregelt: Zugriff, Zweckbindung und Löschfristen für personenbezogene Inhalte sind festgelegt.

Prüfhandlung Regelungen zu Zugriff und Löschung ansehen und mit der Betriebsvereinbarung beziehungsweise dem Datenschutzkonzept abgleichen.

Nachweise Datenschutzkonzept, Löschkonzept, Vereinbarung mit der Arbeitnehmervertretung

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Protokollierungs- und Überwachungsrichtlinie
2. Systemübersicht mit Protokollkonzept je wesentlichem System
3. Konfigurationsauszüge der Protokollierung und der Zeitsynchronisation
4. Regelkatalog der Überwachung und Abdeckungsübersicht
5. Alarmliste der letzten sechs Monate mit Tickets
6. Bereitschaftsplan und Eskalationsregeln
7. Berechtigungsauszug der zentralen Protokollablage
8. Testberichte zur Überwachung

TYPISCHE FESTSTELLUNGEN

- Wesentliche Systeme erzeugen keine oder nur lokale Protokolle, die nicht zentral gesammelt werden.
- Administratoren haben Schreib- oder Löschrechte auf die Protokolle, die ihre Tätigkeit festhalten.
- Zeitquellen sind nicht abgestimmt, Ereignisse lassen sich über Systeme hinweg nicht zuordnen.
- Alarme werden erzeugt, aber nicht zeitnah bewertet; es gibt keine Bereitschaft außerhalb der Geschäftszeiten.
- Die Überwachung ist nie getestet worden, Regeln stammen aus der Einführung und wurden nicht angepasst.
- Protokolle von Dienstleistern und Cloud-Diensten sind nicht angebunden.

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