Muster-Prüfprogramm

IT-Asset- und Konfigurationsmanagement

12 Prüfschritte · ISO 27001, DORA, NIS2

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

ISO/IEC 27001:2022 Anhang A 5.9 · NIS2-Richtlinie Art. 21 Abs. 2 lit. i · DORA Art. 8 Abs. 4 · ISO/IEC 27001:2022 Anhang A 5.12 · DORA Art. 8 Abs. 1 und 4 · ISO/IEC 27001:2022 Anhang A 8.9 · DORA Art. 8 Abs. 6 · ISO/IEC 27001:2022 Anhang A 8.32 · BSI NET.3.4 · ISO/IEC 27001:2022 Anhang A 5.10 und 5.11 · ISO/IEC 27001:2022 Anhang A 7.14 und 8.10 · BSI CON.6 · DORA Art. 8 Abs. 5 · DORA Art. 8 Abs. 7

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation ein vollständiges und aktuelles Inventar ihrer Informationswerte und IT-Komponenten führt, jedem Wert einen Verantwortlichen zuordnet und Kritikalität, Konfiguration und Abhängigkeiten nachvollziehbar dokumentiert. Sie beurteilt außerdem, ob Inventar und Konfigurationsverwaltung mit dem Änderungsprozess verzahnt sind und ausgesonderte Geräte sicher gelöscht werden.

GELTUNGSBEREICH

- Server, Clients, Netzkomponenten, mobile Geräte, Software und Cloud-Ressourcen der Organisation
- Inventar und Konfigurationsdatenbank (CMDB) einschließlich der Prozesse zur Pflege und zum Abgleich
- Aussonderung, Rückgabe und Wiederverwendung von Geräten und Datenträgern
- Nicht Gegenstand: die bilanzielle Anlagenbuchhaltung, soweit sie nicht als Quelle des Inventars dient

Prüfschritte 1 bis 3

Schritt 01 ISO/IEC 27001:2022 Anhang A 5.9; NIS2-Richtlinie Art. 21 Abs. 2 lit. i

Eine Richtlinie regelt, welche Werte zu inventarisieren sind, wer das Inventar pflegt und in welchem Turnus es überprüft wird.

Prüfhandlung Richtlinie lesen, Freigabe und Aktualität feststellen und die festgelegten Inventarklassen mit der gelebten Praxis vergleichen.

Nachweise Richtlinie zum Asset-Management mit Freigabevermerk, Rollenbeschreibung

Schritt 02 ISO/IEC 27001:2022 Anhang A 5.9; DORA Art. 8 Abs. 4

Das Inventar ist vollständig und umfasst auch Geräte an Außenstandorten, mobile Geräte, Netzressourcen und Cloud-Ressourcen.

Prüfhandlung Stichprobe in beide Richtungen ziehen: zehn Geräte vor Ort im Inventar suchen und zehn Inventareinträge physisch oder technisch nachweisen lassen.

Nachweise Inventarauszug, Abgleichprotokoll der Stichprobe

Schritt 03 ISO/IEC 27001:2022 Anhang A 5.9

Jedem Wert ist ein verantwortlicher Eigentümer zugeordnet, der Schutzbedarf und Nutzung kennt.

Prüfhandlung Für die Stichprobe prüfen, ob ein Eigentümer eingetragen ist, und bei drei Eigentümern die Kenntnis ihrer Rolle erfragen.

Nachweise Inventarauszug mit Eigentümerfeld, Interviewnotizen

Prüfschritte 4 bis 6

Schritt 04 ISO/IEC 27001:2022 Anhang A 5.12; DORA Art. 8 Abs. 1 und 4

Werte sind nach Kritikalität und Schutzbedarf eingestuft; kritische Werte sind gekennzeichnet.

Prüfhandlung Einstufungsschema ansehen und für fünf Werte nachvollziehen, ob die Einstufung begründet und aktuell ist.

Nachweise Klassifizierungsschema, Schutzbedarfsfeststellung, Inventarauszug

Schritt 05 ISO/IEC 27001:2022 Anhang A 8.9; DORA Art. 8 Abs. 4

Konfigurationen und Abhängigkeiten zwischen Systemen, Diensten und Geschäftsprozessen sind in der Konfigurationsverwaltung abgebildet.

Prüfhandlung Für einen wesentlichen Geschäftsprozess die Abhängigkeitskette in der CMDB nachvollziehen und mit dem Betrieb abstimmen.

Nachweise Auszug aus der CMDB mit Beziehungen, Architekturübersicht

Schritt 06 DORA Art. 8 Abs. 6; ISO/IEC 27001:2022 Anhang A 8.32

Inventar und Konfigurationsverwaltung werden bei Änderungen zeitnah aktualisiert und regelmäßig überprüft.

Prüfhandlung Fünf abgeschlossene Änderungen auswählen und prüfen, ob die CMDB den neuen Stand zeigt; Nachweise der letzten Überprüfung ansehen.

Nachweise Änderungstickets, Änderungshistorie der CMDB, Überprüfungsprotokoll

Prüfschritte 7 bis 9

Schritt 07 — BSI NET.3.4

Unbekannte Geräte im Netz werden automatisch erkannt, mit dem Inventar abgeglichen und geklärt.

Prüfhandlung Funktionsweise der Netzwerkerkennung erläutern lassen und die Abweichungsliste der letzten drei Monate auf Bearbeitung prüfen.

Nachweise Berichte der Erkennungswerkzeuge, Abweichungsliste mit Klärungsvermerken

Schritt 08 — ISO/IEC 27001:2022 Anhang A 8.9

Für Systemklassen gibt es dokumentierte Sicherheitskonfigurationen, deren Einhaltung überwacht wird.

Prüfhandlung Konfigurationsvorgaben für zwei Systemklassen lesen und Berichte zur Abweichung von der Vorgabe auswerten.

Nachweise Konfigurationsvorgaben, Compliance-Berichte der Konfigurationsüberwachung

Schritt 09 — ISO/IEC 27001:2022 Anhang A 5.10 und 5.11

Regeln zur zulässigen Nutzung sind bekannt, und Werte werden bei Austritt oder Rollenwechsel zurückgegeben.

Prüfhandlung Für fünf Austritte der letzten sechs Monate die Rückgabe der zugeordneten Geräte nachvollziehen.

Nachweise Nutzungsrichtlinie, Austrittschecklisten, Rückgabeprotokolle

Prüfschritte 10 bis 12

Schritt 10 — ISO/IEC 27001:2022 Anhang A 7.14 und 8.10; BSI CON.6

Ausgesonderte Geräte und Datenträger werden vor Entsorgung oder Wiederverwendung nachweisbar gelöscht oder vernichtet.

Prüfhandlung Aussonderungsprozess ansehen und für fünf ausgesonderte Geräte Lösch- oder Vernichtungsnachweise anfordern.

Nachweise Aussonderungsliste, Löschprotokolle, Vernichtungszertifikate des Dienstleisters

Schritt 11 — DORA Art. 8 Abs. 5

Abhängigkeiten von IKT-Drittdienstleistern sind erfasst, besonders für kritische oder wichtige Funktionen.

Prüfhandlung Prüfen, ob in der CMDB oder im Dienstleisterregister erkennbar ist, welche Werte von welchem Dienstleister abhängen.

Nachweise Dienstleisterregister, Verknüpfung von Diensten und Dienstleistern in der CMDB

Schritt 12 — DORA Art. 8 Abs. 7

Altsysteme sind als solche gekennzeichnet, und ihre Risiken werden regelmäßig bewertet.

Prüfhandlung Liste der Altsysteme anfordern und die letzte Risikobewertung sowie die geplanten Maßnahmen ansehen.

Nachweise Liste der Altsysteme, Risikobewertung, Maßnahmenplan zur Ablösung

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Richtlinie zum Asset- und Konfigurationsmanagement
2. Aktueller Inventarauszug mit Eigentümer und Einstufung
3. Klassifizierungsschema und Schutzbedarfsfeststellung
4. Auszug aus der CMDB mit Beziehungen für einen wesentlichen Geschäftsprozess
5. Berichte der Netzwerkerkennung und Abweichungsliste
6. Konfigurationsvorgaben je Systemklasse
7. Aussonderungsliste mit Lösch- und Vernichtungsnachweisen
8. Liste der Altsysteme mit Risikobewertung

TYPISCHE FESTSTELLUNGEN

- Mehrere Inventare werden parallel geführt und widersprechen sich.
- Cloud-Ressourcen und mobile Geräte fehlen im Inventar.
- Eigentümer sind nicht eingetragen oder haben das Unternehmen verlassen.
- Die CMDB bildet Abhängigkeiten nicht ab und wird bei Änderungen nicht gepflegt.
- Für ausgesonderte Datenträger gibt es keine Löschnachweise.
- Altsysteme sind bekannt, ihre Risiken aber nie bewertet worden.

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