Muster-Prüfprogramm

Software-Lizenzmanagement

12 Prüfschritte · ISO 27001, BSI

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

ISO/IEC 27001:2022 Anhang A 5.32 · ISO/IEC 27001:2022 Anhang A 5.9 · BSI APP.6 · ISO/IEC 27001:2022 Anhang A 8.19 · ISO/IEC 27001:2022 Anhang A 5.11 · ISO/IEC 27001:2022 Anhang A 8.8

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation die Nutzung von Software und Cloud-Abonnements mit ihren erworbenen Rechten in Einklang hält: über Verantwortlichkeiten, ein vollständiges Inventar, einen nachgewiesenen Lizenzbestand und einen regelmäßigen Abgleich. Sie beurteilt außerdem, ob Beschaffung und Installation gesteuert werden und Lizenzen bei Wegfall der Nutzung zurückgewonnen werden.

GELTUNGSBEREICH

- Installierte Software auf Clients und Servern sowie Software in virtualisierten Umgebungen
- Cloud-Abonnements und nutzerbasierte Lizenzen
- Verträge, Lizenznachweise und Beschaffungsprozess für Software
- Nicht Gegenstand: die vertragsrechtliche Würdigung einzelner Lizenzbedingungen

Prüfschritte 1 bis 3

Schritt 01 ISO/IEC 27001:2022 Anhang A 5.32

Eine Richtlinie regelt Verantwortung, Beschaffung, Nutzung und Nachweis von Softwarelizenzen.

Prüfhandlung Richtlinie lesen und die benannten Verantwortlichen zu Abläufen und Werkzeugen befragen.

Nachweise Richtlinie zum Lizenzmanagement, Rollenbeschreibung

Schritt 02 ISO/IEC 27001:2022 Anhang A 5.9; BSI APP.6

Ein vollständiges Inventar zeigt installierte und genutzte Software einschließlich Cloud-Abonnements.

Prüfhandlung Datenquellen des Inventars erfragen und die Abdeckung mit der Geräte- und Kontenzahl vergleichen.

Nachweise Softwareinventar, Abdeckungsbericht des Erkennungswerkzeugs

Schritt 03 ISO/IEC 27001:2022 Anhang A 5.32

Der Lizenzbestand mit Verträgen, Rechnungen und Lizenzschlüsseln ist zentral und vollständig nachgewiesen.

Prüfhandlung Für fünf Hersteller den Lizenzbestand mit Kaufnachweisen abgleichen.

Nachweise Lizenzverzeichnis, Verträge, Rechnungen

Prüfschritte 4 bis 6

Schritt 04 — ISO/IEC 27001:2022 Anhang A 5.32

Bestand und Nutzung werden regelmäßig gegenübergestellt; Unter- und Überlizenzierung werden bereinigt.

Prüfhandlung Letzte Lizenzbilanz für die wesentlichen Hersteller ansehen und den Umgang mit Fehlmengen nachvollziehen.

Nachweise Lizenzbilanzen, Maßnahmenliste

Schritt 05 — BSI APP.6

Software wird nur über einen festgelegten Prozess beschafft, der Lizenzbedarf und Freigabe einschließt.

Prüfhandlung Fünf Beschaffungen der letzten zwölf Monate von der Anforderung bis zur Lizenzerfassung nachvollziehen.

Nachweise Beschaffungsanträge, Freigaben, Einträge im Lizenzverzeichnis

Schritt 06 — ISO/IEC 27001:2022 Anhang A 8.19

Nutzer können Software nicht eigenmächtig installieren; Installationen erfolgen über freigegebene Wege.

Prüfhandlung Technische Einschränkungen auf Clients prüfen und nicht freigegebene Software im Inventar suchen.

Nachweise Konfiguration der Softwareverteilung, Liste nicht freigegebener Software

Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Anhang A 5.32

Lizenzmetriken für Virtualisierung, Server und Cloud werden richtig angewendet.

Prüfhandlung Für einen Hersteller mit Metriken nach Prozessorkernen oder Hosts die Berechnung nachvollziehen.

Nachweise Berechnung der Lizenzposition, Infrastrukturübersicht

Schritt 08 — ISO/IEC 27001:2022 Anhang A 5.32

Lizenzbedingungen kostenloser und quelloffener Software werden vor dem Einsatz geprüft.

Prüfhandlung Prüfverfahren für frei verfügbare Software ansehen und für drei Komponenten die Prüfung nachvollziehen.

Nachweise Freigabeverfahren, Lizenzprüfungen, Komponentenliste

Schritt 09 — ISO/IEC 27001:2022 Anhang A 5.32

Die Organisation ist auf Herstelleraudits vorbereitet: Zuständigkeit, Ablauf und Datenbereitstellung sind geregelt.

Prüfhandlung Ablauf für Herstelleraudits erfragen und Ergebnisse vergangener Audits mit Nachzahlungen ansehen.

Nachweise Ablaufbeschreibung, Berichte vergangener Audits

Prüfschritte 10 bis 12

Schritt 10 — ISO/IEC 27001:2022 Anhang A 5.11

Lizenzen werden bei Austritt, Rollenwechsel oder fehlender Nutzung zurückgewonnen.

Prüfhandlung Zugewiesene Abonnements ohne Nutzung seit 90 Tagen auswerten und Rückgewinnung bei fünf Austritten prüfen.

Nachweise Nutzungsbericht der Abonnements, Austrittschecklisten

Schritt 11 — BSI APP.6; ISO/IEC 27001:2022 Anhang A 8.8

Software ohne Herstellerunterstützung wird erkannt und abgelöst oder als Risiko behandelt.

Prüfhandlung Liste der Software mit abgelaufener Unterstützung ansehen und Ablösepläne prüfen.

Nachweise Liste abgekündigter Software, Ablösepläne, Risikoakzeptanzen

Schritt 12 — Praxisanforderung

Die Leitung erhält regelmäßig Berichte zu Lizenzrisiken, Kosten und Einsparungen.

Prüfhandlung Berichte der letzten zwölf Monate auf Inhalte und Maßnahmen prüfen.

Nachweise Berichte zum Lizenzmanagement

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Richtlinie zum Lizenzmanagement
2. Softwareinventar mit Abdeckungsbericht
3. Lizenzverzeichnis mit Verträgen und Kaufnachweisen
4. Lizenzbilanzen der wesentlichen Hersteller
5. Beschaffungsanträge und Freigaben der letzten zwölf Monate
6. Nutzungsberichte der Cloud-Abonnements
7. Liste abgekündigter Software
8. Berichte vergangener Herstelleraudits

TYPISCHE FESTSTELLUNGEN

- Kaufnachweise für ältere Lizenzen sind nicht mehr auffindbar.
- Die Lizenzbilanz wird nur bei einem angekündigten Herstelleraudit erstellt.
- Nutzer installieren Software selbst, das Inventar ist lückenhaft.
- Lizenzmetriken für virtualisierte Server werden falsch berechnet.
- Abonnements ausgeschiedener Mitarbeitender werden weiter bezahlt.
- Abgekündigte Software läuft ohne Ablöseplan und ohne Risikobewertung.

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