Muster-Prüfprogramm

Physische Sicherheit Rechenzentrum

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 7.1 · BSI INF.2 · ISO/IEC 27001:2022 Anhang A 7.2 · ISO/IEC 27001:2022 Anhang A 7.4 · ISO/IEC 27001:2022 Anhang A 7.5 · ISO/IEC 27001:2022 Anhang A 7.11 · ISO/IEC 27001:2022 Anhang A 7.12 · BSI INF.12 · ISO/IEC 27001:2022 Anhang A 7.13 · BSI INF.5 · ISO/IEC 27001:2022 Anhang A 7.14 · ISO/IEC 27001:2022 Anhang A 8.14

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation ihre Räume für IT-Technik in Sicherheitszonen gliedert, den Zutritt wirksam kontrolliert und überwacht und die Technik gegen Umgebungsgefahren und den Ausfall der Versorgung schützt. Sie beurteilt außerdem, ob Wartung, Prüfungen und Notfallmaßnahmen der Gebäudetechnik nachweisbar durchgeführt werden.

GELTUNGSBEREICH

- Eigene Rechenzentren, Serverräume und Technikräume einschließlich Verteilerräumen an Standorten
- Zutrittskontrolle, Überwachungstechnik, Brandschutz, Klima, Stromversorgung und Verkabelung
- Wartungsverträge und Prüfnachweise der Gebäudetechnik
- Nicht Gegenstand: Rechenzentren von Dienstleistern, die über Zertifikate oder Berichte gesondert betrachtet werden

Prüfschritte 1 bis 3

Schritt 01 — ISO/IEC 27001:2022 Anhang A 7.1; BSI INF.2

Sicherheitszonen sind festgelegt; Räume für IT-Technik liegen in einem geschützten Bereich mit klaren Grenzen.

Prüfhandlung Zonenplan ansehen und bei einer Begehung die Grenzen, Türen, Fenster und Zugänge prüfen.

Nachweise Zonenplan, Begehungsprotokoll mit Fotos

Schritt 02 — ISO/IEC 27001:2022 Anhang A 7.2

Zutritt erhalten nur berechtigte Personen; Berechtigungen werden beantragt, genehmigt und regelmäßig überprüft.

Prüfhandlung Liste der Zutrittsberechtigten mit Personal- und Dienstleisterlisten abgleichen und die letzte Überprüfung ansehen.

Nachweise Auszug der Zutrittsberechtigungen, Genehmigungen, Überprüfungsprotokoll

Schritt 03 — ISO/IEC 27001:2022 Anhang A 7.2

Besucher und Dienstleister werden erfasst, begleitet und ihr Aufenthalt protokolliert.

Prüfhandlung Besucherbuch oder elektronisches Protokoll der letzten drei Monate mit Wartungseinsätzen abgleichen.

Nachweise Besucherprotokoll, Wartungsnachweise

Prüfschritte 4 bis 6

Schritt 04 — ISO/IEC 27001:2022 Anhang A 7.4

Zugänge und Räume werden überwacht; Alarme der Einbruchmeldung und der Türüberwachung werden verfolgt.

Prüfhandlung Überwachungstechnik vorführen lassen und für drei Alarme Reaktion und Abschluss nachvollziehen.

Nachweise Alarmprotokolle, Aufschaltung auf Leitstelle oder Wachdienst

Schritt 05 — ISO/IEC 27001:2022 Anhang A 7.5; BSI INF.2

Brandmeldung und Löschtechnik sind vorhanden, auf die Technik abgestimmt und werden geprüft; Gefahren durch Wasser sind berücksichtigt.

Prüfhandlung Brandschutzkonzept und Prüfberichte ansehen und bei der Begehung Wasserleitungen, Melder und Löschtechnik prüfen.

Nachweise Brandschutzkonzept, Prüfberichte der Brandmelde- und Löschanlage

Schritt 06 — ISO/IEC 27001:2022 Anhang A 7.11; BSI INF.2

Temperatur und Luftfeuchte werden überwacht; die Klimatisierung ist für die Last ausgelegt und redundant.

Prüfhandlung Messwerte der letzten drei Monate auswerten und Redundanz sowie Alarmierung der Klimatechnik prüfen.

Nachweise Messprotokolle, Alarmierungskonzept, Auslegung der Klimatechnik

Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Anhang A 7.11

Die Stromversorgung ist gegen Ausfall geschützt; USV und Netzersatzanlage werden regelmäßig unter Last getestet.

Prüfhandlung Testprotokolle der USV und der Netzersatzanlage ansehen und Überbrückungszeit mit dem Bedarf vergleichen.

Nachweise Testprotokolle, Kapazitätsberechnung, Wartungsberichte

Schritt 08 — ISO/IEC 27001:2022 Anhang A 7.12; BSI INF.12

Strom- und Datenkabel sind gegen Beschädigung und Abhören geschützt und dokumentiert.

Prüfhandlung Kabelwege bei der Begehung ansehen und mit der Dokumentation vergleichen.

Nachweise Verkabelungsplan, Begehungsprotokoll

Schritt 09 — ISO/IEC 27001:2022 Anhang A 7.13

Die Technik wird nach Herstellervorgaben gewartet; Wartungsarbeiten sind nachvollziehbar.

Prüfhandlung Wartungsplan mit Wartungsnachweisen der letzten zwölf Monate für Klima, USV und Brandschutz abgleichen.

Nachweise Wartungsplan, Wartungsberichte, Wartungsverträge

Prüfschritte 10 bis 12

Schritt 10

BSI INF.5

Dezentrale Technikräume und Verteilerschränke an Standorten sind verschlossen und gegen Umgebungsgefahren geschützt.

Prüfhandlung Zwei Standorte auswählen und Verschluss, Zugang und Umgebung der Technikräume prüfen.

Nachweise Standortliste, Begehungsprotokolle

Schritt 11

ISO/IEC 27001:2022 Anhang A 7.14

Geräte werden vor Entsorgung oder Wiederverwendung so behandelt, dass keine Daten in fremde Hände gelangen.

Prüfhandlung Ablauf für ausgesonderte Geräte aus dem Rechenzentrum nachvollziehen und Vernichtungsnachweise anfordern.

Nachweise Aussonderungsprotokolle, Vernichtungsnachweise

Schritt 12

ISO/IEC 27001:2022 Anhang A 8.14

Für den Ausfall eines Standorts besteht ausreichende Redundanz, und Standortrisiken sind bewertet.

Prüfhandlung Standortrisikobewertung und Redundanzkonzept ansehen und den Abstand und die Unabhängigkeit der Standorte bewerten.

Nachweise Standortrisikoanalyse, Redundanzkonzept

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Zonenplan und Grundrisse der Räume für IT-Technik
2. Auszug der Zutrittsberechtigungen und letzte Überprüfung
3. Besucherprotokolle
4. Brandschutzkonzept und Prüfberichte
5. Messprotokolle von Temperatur und Luftfeuchte
6. Testprotokolle von USV und Netzersatzanlage
7. Wartungsplan und Wartungsberichte
8. Standortrisikoanalyse und Redundanzkonzept

TYPISCHE FESTSTELLUNGEN

- Zutrittsberechtigungen ausgeschiedener Mitarbeitender und Dienstleister sind noch aktiv.
- Dienstleister arbeiten unbegleitet und ohne Protokoll im Serverraum.
- Die Netzersatzanlage wurde nie unter Last getestet.
- Im Serverraum lagern brennbare Materialien, Wasserleitungen verlaufen über den Racks.
- Klimaalarme gehen an ein nicht besetztes Postfach.
- Technikräume an Standorten sind unverschlossen oder werden als Lager genutzt.

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