Muster-Prüfprogramm

Fernzugriff und mobiles Arbeiten

12 Prüfschritte · BSI, ISO 27001, NIS2

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

ISO/IEC 27001:2022 Anhang A 6.7 · BSI OPS.1.2.4 · BSI NET.3.3 · ISO/IEC 27001:2022 Anhang A 8.20 · NIS2-Richtlinie Art. 21 Abs. 2 lit. j · § 30 Abs. 2 Nr. 10 BSIG · ISO/IEC 27001:2022 Anhang A 8.5 · ISO/IEC 27001:2022 Anhang A 8.1 · ISO/IEC 27001:2022 Anhang A 8.8 · BSI TR-02102-3 · ISO/IEC 27001:2022 Anhang A 8.22 · BSI OPS.1.2.5 · ISO/IEC 27001:2022 Anhang A 8.15 und 8.16 · BSI INF.8 · BSI INF.9 · ISO/IEC 27001:2022 Anhang A 7.7 · BSI CON.7 · ISO/IEC 27001:2022 Anhang A 5.18

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation Fernzugriffe von Beschäftigten und Dienstleistern über freigegebene, gehärtete Zugänge mit Mehrfaktor-Anmeldung abwickelt, die Zugriffe auf das Erforderliche begrenzt und überwacht. Sie beurteilt außerdem, ob Regeln für das Arbeiten zu Hause, unterwegs und im Ausland bestehen und eingehalten werden.

GELTUNGSBEREICH

- VPN, Zugänge nach dem Zero-Trust-Prinzip, Remote-Desktop-Gateways und vergleichbare Fernzugänge
- Fernwartungszugänge von Dienstleistern
- Arbeit im häuslichen Umfeld, unterwegs und auf Auslandsreisen
- Nicht Gegenstand: die allgemeine Netzarchitektur, die ein eigenes Prüfprogramm hat

Prüfschritte 1 bis 3

Schritt 01 ISO/IEC 27001:2022 Anhang A 6.7; BSI OPS.1.2.4

Eine Richtlinie regelt mobiles Arbeiten und Telearbeit einschließlich zulässiger Orte, Geräte und Verhaltensregeln.

Prüfhandlung Richtlinie lesen, Freigabe prüfen und mit der Vereinbarung zur mobilen Arbeit abgleichen.

Nachweise Richtlinie mobiles Arbeiten, Vereinbarung mit der Arbeitnehmervertretung

Schritt 02 BSI NET.3.3; ISO/IEC 27001:2022 Anhang A 8.20

Fernzugriffe sind nur über freigegebene und zentral verwaltete Zugänge möglich.

Prüfhandlung Übersicht der Fernzugänge mit einem Scan der von außen erreichbaren Dienste vergleichen.

Nachweise Liste der Fernzugänge, Ergebnis des externen Scans

Schritt 03 NIS2-Richtlinie Art. 21 Abs. 2 lit. j; § 30 Abs. 2 Nr. 10 BSIG; ISO/IEC 27001:2022 Anhang A 8.5

Jeder Fernzugriff erfordert eine Anmeldung mit mehreren Faktoren.

Prüfhandlung Anmeldekonfiguration der Zugänge prüfen und Konten ohne zweiten Faktor auflisten lassen.

Nachweise Konfiguration der Anmeldung, Ausnahmeliste

Prüfschritte 4 bis 6

Schritt 04 — ISO/IEC 27001:2022 Anhang A 8.1

Nur verwaltete Geräte in einem geprüften Zustand dürfen sich verbinden.

Prüfhandlung Prüfregeln für den Gerätezustand ansehen und einen Verbindungsversuch mit einem nicht verwalteten Gerät nachvollziehen.

Nachweise Regeln zur Geräteprüfung, Protokoll abgewiesener Verbindungen

Schritt 05 — BSI NET.3.3; ISO/IEC 27001:2022 Anhang A 8.8

VPN-Gateways und Zugangssysteme sind gehärtet und werden zeitnah aktualisiert.

Prüfhandlung Versionsstand der Zugangssysteme mit Herstellerhinweisen vergleichen und die Reaktion auf die letzte kritische Schwachstelle nachvollziehen.

Nachweise Versionsstand, Patchprotokoll, Sicherheitshinweise des Herstellers

Schritt 06 — BSI TR-02102-3

Für den VPN-Tunnel werden empfohlene Protokolle und Verfahren verwendet.

Prüfhandlung Konfiguration von Protokollversionen und Verschlüsselungsverfahren auslesen und mit den Empfehlungen vergleichen.

Nachweise Konfigurationsauszug des VPN

Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Anhang A 8.22

Fernzugriffe reichen nur in die Netze und Systeme, die für die jeweilige Aufgabe nötig sind.

Prüfhandlung Zugriffsregeln je Nutzergruppe auswerten und pauschale Freigaben auf das gesamte interne Netz markieren.

Nachweise Regelwerk des Zugangs je Gruppe

Schritt 08 — BSI OPS.1.2.5

Fernwartung durch Dienstleister erfolgt nur nach Freigabe, zeitlich begrenzt und nachvollziehbar.

Prüfhandlung Fünf Fernwartungssitzungen auf Anlass, Freigabe, Dauer und Protokoll prüfen.

Nachweise Fernwartungsprotokolle, Freigaben, Vertragsregelungen

Schritt 09 — ISO/IEC 27001:2022 Anhang A 8.15 und 8.16

Anmeldungen und Sitzungen über Fernzugänge werden protokolliert und auf Auffälligkeiten überwacht.

Prüfhandlung Überwachungsregeln für Fernzugriffe ansehen, etwa für Anmeldungen aus ungewöhnlichen Ländern, und einen Alarm nachvollziehen.

Nachweise Protokollauszug, Regelkatalog, Alarmbeispiel

Prüfschritte 10 bis 12

Schritt 10 — BSI INF.8; BSI INF.9; ISO/IEC 27001:2022 Anhang A 7.7

Regeln für den Arbeitsplatz zu Hause und unterwegs schützen Informationen vor Einsicht und Verlust.

Prüfhandlung Regeln zu Sichtschutz, Ausdrucken und Aufbewahrung prüfen und ihre Bekanntheit bei fünf Mitarbeitenden erfragen.

Nachweise Verhaltensregeln, Interviewnotizen

Schritt 11 — BSI CON.7

Für Reisen und Arbeit im Ausland gelten besondere Regeln, etwa zu Geräten und Datenmitnahme.

Prüfhandlung Regelung für Auslandsreisen lesen und für zwei Reisen die Anwendung nachvollziehen.

Nachweise Regelung für Auslandsreisen, Reisegeräte, Genehmigungen

Schritt 12 — ISO/IEC 27001:2022 Anhang A 5.18

Berechtigungen für Fernzugriffe werden regelmäßig überprüft und bei Austritt sofort entzogen.

Prüfhandlung Mitglieder der Zugangsgruppen mit dem Personalstand abgleichen und die letzte Überprüfung ansehen.

Nachweise Gruppenmitglieder, Austrittsliste, Überprüfungsprotokoll

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Richtlinie mobiles Arbeiten und Telearbeit
2. Liste der Fernzugänge und Ergebnis eines externen Scans
3. Konfiguration von Anmeldung und Geräteprüfung
4. Versionsstand und Patchprotokoll der Zugangssysteme
5. Regelwerk der Fernzugänge je Nutzergruppe
6. Fernwartungsprotokolle und Vertragsregelungen mit Dienstleistern
7. Regelung für Auslandsreisen
8. Protokoll der letzten Überprüfung der Zugangsberechtigungen

TYPISCHE FESTSTELLUNGEN

- Ein alter Fernzugang ist noch von außen erreichbar und ohne zweiten Faktor nutzbar.
- VPN-Gateways wurden nach kritischen Herstellerhinweisen nicht zeitnah aktualisiert.
- Über den Fernzugang ist das gesamte interne Netz erreichbar.
- Fernwartungszugänge von Dienstleistern sind dauerhaft offen.
- Private Geräte können sich ohne Prüfung verbinden.
- Zugangsberechtigungen werden nie überprüft.

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