Muster-Prüfprogramm

Cloud-Nutzung und Auslagerung

12 Prüfschritte · ISO 27001, DORA, BSI

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

ISO/IEC 27001:2022 Anhang A 5.23 · BSI OPS.2.2 · DORA Art. 28(4) · DORA Art. 30(2) · ISO/IEC 27001:2022 Anhang A 5.20 · DORA Art. 28(3) · ISO/IEC 27001:2022 Anhang A 8.2 · § 30 Abs. 2 Nr. 10 BSIG · ISO/IEC 27001:2022 Anhang A 5.23 und 8.9 · ISO/IEC 27001:2022 Anhang A 5.22 · DORA Art. 30(3)(a) und (b) · DORA Art. 29 · DORA Art. 28(8) · ISO/IEC 27001:2022 Anhang A 5.30

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation die Nutzung von Cloud-Diensten steuert: von der Entscheidung und Risikobewertung über die Vertragsgestaltung und die Aufgabenteilung mit dem Anbieter bis zur sicheren Konfiguration, zur laufenden Überwachung und zum geordneten Ausstieg. Sie beurteilt außerdem, ob die zusätzlichen Anforderungen für Finanzunternehmen berücksichtigt sind, soweit sie gelten.

GELTUNGSBEREICH

- Software, Plattformen und Infrastruktur als Dienst, die von der Organisation genutzt werden, einschließlich Schatten-IT, die bekannt wird
- Entscheidungs-, Vertrags- und Betriebsprozesse für Cloud-Dienste
- Konfiguration und Zugriffe der Mandanten der Organisation beim Anbieter
- Nicht Gegenstand: die interne Sicherheit der Rechenzentren des Anbieters, sofern nicht über Zertifikate oder Berichte gesondert betrachtet

Prüfschritte 1 bis 3

Schritt 01 ISO/IEC 27001:2022 Anhang A 5.23; BSI OPS.2.2

Eine Cloud-Strategie oder Richtlinie legt fest, für welche Daten und Prozesse Cloud-Dienste genutzt werden dürfen und nach welchen Kriterien Anbieter ausgewählt werden.

Prüfhandlung Strategie und Richtlinie lesen, Freigabe prüfen und mit den tatsächlich genutzten Diensten abgleichen.

Nachweise Cloud-Richtlinie mit Freigabe, Liste der genutzten Cloud-Dienste

Schritt 02 ISO/IEC 27001:2022 Anhang A 5.23; DORA Art. 28(4)

Vor der Nutzung wird der Schutzbedarf der betroffenen Daten festgestellt und das Risiko bewertet, einschließlich der Frage, ob die Funktion kritisch oder wichtig ist.

Prüfhandlung Für drei Cloud-Dienste die Risikobewertung vor der Einführung ansehen und die Einstufung der Funktion nachvollziehen.

Nachweise Risikobewertungen, Schutzbedarfsfeststellung, Entscheidungsvorlagen

Schritt 03 ISO/IEC 27001:2022 Anhang A 5.23; BSI OPS.2.2

Die Aufgaben zwischen Organisation und Anbieter sind schriftlich abgegrenzt, sodass klar ist, wer Konfiguration, Zugriffe, Datensicherung und Protokolle verantwortet.

Prüfhandlung Verantwortungsmatrix und Vertragsunterlagen lesen und für zwei Dienste prüfen, ob die Aufgaben tatsächlich wahrgenommen werden.

Nachweise Verantwortungsmatrix, Verträge und Leistungsbeschreibungen

Prüfschritte 4 bis 6

Schritt 04 — DORA Art. 30(2); ISO/IEC 27001:2022 Anhang A 5.20

Die Verträge enthalten Regelungen zu Informationssicherheit, Standort der Daten, Unterauftragnehmern, Meldung von Vorfällen, Prüfrechten und Beendigung.

Prüfhandlung Verträge der wesentlichen Cloud-Anbieter anhand einer Checkliste auf die genannten Punkte durchsehen.

Nachweise Verträge, Anlagen zu Sicherheit und Datenverarbeitung, ausgefüllte Checkliste

Schritt 05 — DORA Art. 28(3)

Ein Register erfasst alle ausgelagerten Dienste mit Vertragsdaten und Einstufung; es wird aktuell gehalten.

Prüfhandlung Register mit Beschaffungsunterlagen und Rechnungen abgleichen, um nicht erfasste Dienste zu finden.

Nachweise Register der Auslagerungen, Rechnungsauswertung, Liste der Beschaffungen

Schritt 06 — ISO/IEC 27001:2022 Anhang A 8.2; § 30 Abs. 2 Nr. 10 BSIG

Zugänge zu Cloud-Konsolen sind auf Berechtigte beschränkt und durch Mehrfaktor-Authentifizierung abgesichert, privilegierte Rollen werden regelmäßig überprüft.

Prüfhandlung Administratorrollen in zwei Mandanten auslesen und Authentifizierung sowie letzte Überprüfung nachvollziehen.

Nachweise Rollen- und Benutzerauszüge, Richtlinie zur Authentifizierung, Überprüfungsprotokoll

Prüfschritte 7 bis 9

Schritt 07 ISO/IEC 27001:2022 Anhang A 5.23 und 8.9; BSI OPS.2.2

Cloud-Ressourcen werden nach festgelegten Vorgaben konfiguriert, Abweichungen werden erkannt und behoben.

Prüfhandlung Konfigurationsvorgaben mit den Einstellungen eines Mandanten vergleichen, insbesondere öffentliche Freigaben und Verschlüsselung.

Nachweise Konfigurationsstandards, Auswertung der Konfigurationsprüfung, Auszug der Einstellungen

Schritt 08 ISO/IEC 27001:2022 Anhang A 5.23

Daten sind im Ruhezustand und bei der Übertragung geschützt, Schlüssel werden kontrolliert verwaltet.

Prüfhandlung Verschlüsselungseinstellungen und Verwaltung der Schlüssel für zwei Dienste prüfen.

Nachweise Konfigurationsauszüge, Schlüsselverwaltungskonzept

Schritt 09 ISO/IEC 27001:2022 Anhang A 5.22; DORA Art. 30(3)(a) und (b)

Leistung, Verfügbarkeit und Sicherheitsvorfälle der Anbieter werden überwacht; Berichte und Zertifikate werden ausgewertet.

Prüfhandlung Berichte der letzten zwölf Monate ansehen und prüfen, ob Abweichungen verfolgt wurden.

Nachweise Leistungsberichte, Zertifikate und Prüfberichte, Besprechungsprotokolle

Prüfschritte 10 bis 12

Schritt 10

DORA Art. 28(4); DORA Art. 29

Konzentrationsrisiken, etwa durch die Abhängigkeit von einem Anbieter für mehrere wesentliche Dienste, sind erkannt und bewertet.

Prüfhandlung Verteilung der wesentlichen Dienste auf Anbieter auswerten und die Bewertung des Konzentrationsrisikos ansehen.

Nachweise Auswertung nach Anbietern, Risikobewertung, Entscheidungen der Leitung

Schritt 11

DORA Art. 28(8); ISO/IEC 27001:2022 Anhang A 5.23

Für kritische Dienste bestehen dokumentierte und getestete Ausstiegs- und Rückführungspläne.

Prüfhandlung Ausstiegspläne lesen und nachvollziehen, ob Datenexport und Alternativen geprüft oder erprobt wurden.

Nachweise Ausstiegspläne, Testprotokolle, Nachweis des Datenexports

Schritt 12

ISO/IEC 27001:2022 Anhang A 5.30

Notfall- und Wiederherstellungspläne berücksichtigen den Ausfall eines Cloud-Anbieters.

Prüfhandlung Notfallpläne auf die Berücksichtigung der Cloud-Dienste prüfen und Ergebnisse der letzten Übung ansehen.

Nachweise Notfallpläne, Übungsprotokolle, Wiederanlaufzeiten

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Cloud-Strategie oder Richtlinie zur Nutzung von Cloud-Diensten
2. Register der genutzten und ausgelagerten Dienste mit Einstufung
3. Verträge, Leistungsbeschreibungen und Anlagen zur Datenverarbeitung
4. Risikobewertungen und Entscheidungsvorlagen zu den Diensten der Stichprobe
5. Verantwortungsmatrix zwischen Organisation und Anbieter
6. Rollen- und Konfigurationsauszüge aus den Mandanten
7. Berichte, Zertifikate und Prüfberichte der Anbieter
8. Ausstiegs- und Notfallpläne

TYPISCHE FESTSTELLUNGEN

Cloud-Dienste werden von Fachbereichen ohne Beteiligung der Informationssicherheit beschafft und sind nicht im Register erfasst.

Die Verantwortung für Datensicherung und Protokolle ist zwischen Organisation und Anbieter nicht geklärt.

Verträge enthalten keine Prüfrechte und keine Regelung zu Unterauftragnehmern.

Öffentliche Freigaben oder schwache Konfigurationen werden nicht durch eine laufende Prüfung erkannt.

Administratorzugänge zur Cloud-Konsole sind nicht durch Mehrfaktor-Authentifizierung geschützt.

Ein Ausstiegsplan fehlt oder wurde nie erprobt, der Datenexport ist unklar.

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