Muster-Prüfprogramm

Dienstleistersteuerung

12 Prüfschritte · 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 5.19 · NIS2-Richtlinie Art. 21 Abs. 2 lit. d · § 30 Abs. 2 Nr. 4 BSIG · NIS2-Richtlinie Art. 21 Abs. 3 · ISO/IEC 27001:2022 Anhang A 5.20 · ISO/IEC 27001:2022 Anhang A 5.21 · ISO/IEC 27001:2022 Anhang A 5.19 und 5.15 · ISO/IEC 27001:2022 Anhang A 5.22 · BSI DER.2.1 · ISO/IEC 27001:2022 Anhang A 5.19 und 5.18 · NIS2-Richtlinie Art. 20

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation die Informationssicherheit in Beziehungen zu Dienstleistern und Lieferanten steuert: von der Erfassung und Einstufung über die Auswahl und die vertragliche Absicherung bis zur Überwachung der Leistung, zum Umgang mit Änderungen und zur Beendigung. Sie beurteilt außerdem, ob Lieferketten und Unterauftragnehmer berücksichtigt sind.

GELTUNGSBEREICH

- Dienstleister und Lieferanten mit Zugriff auf Informationen, Systeme oder Räume der Organisation sowie IT-Lieferanten für wesentliche Dienste
- Prozesse für Auswahl, Beauftragung, Überwachung, Änderung und Beendigung
- Verantwortliche Stellen in Einkauf, Fachbereichen, Informationssicherheit und Recht
- Nicht Gegenstand: Regelungen speziell für Finanzunternehmen nach DORA und die Cloud-Nutzung, die in eigenen Mustern behandelt werden

Prüfschritte 1 bis 3

Schritt 01 ISO/IEC 27001:2022 Anhang A 5.19; NIS2-Richtlinie Art. 21 Abs. 2 lit. d

Eine Richtlinie zur Informationssicherheit in Lieferantenbeziehungen besteht, ist freigegeben und legt Anforderungen nach Einstufung des Dienstleisters fest.

Prüfhandlung Richtlinie lesen und prüfen, ob Einstufung, Rollen und Mindestanforderungen festgelegt sind.

Nachweise Richtlinie mit Freigabevermerk, Einstufungsschema

Schritt 02 ISO/IEC 27001:2022 Anhang A 5.19; § 30 Abs. 2 Nr. 4 BSIG

Ein vollständiges Verzeichnis der Dienstleister und Lieferanten mit Einstufung, Ansprechperson und Vertragsdaten wird gepflegt.

Prüfhandlung Verzeichnis mit Kreditorenliste und Zugriffsberechtigungen von Externen abgleichen, um nicht erfasste Dienstleister zu finden.

Nachweise Dienstleisterverzeichnis, Kreditorenauszug, Liste externer Benutzer

Schritt 03 ISO/IEC 27001:2022 Anhang A 5.19; NIS2-Richtlinie Art. 21 Abs. 3

Vor der Beauftragung werden Risiken bewertet und Dienstleister auf ihre Eignung geprüft, auch hinsichtlich der Informationssicherheit.

Prüfhandlung Für fünf neue Dienstleister der letzten zwölf Monate die Bewertung vor Vertragsschluss ansehen.

Nachweise Risikobewertungen, Fragebögen, Zertifikate, Entscheidungsvermerke

Prüfschritte 4 bis 6

Schritt 04 ISO/IEC 27001:2022 Anhang A 5.20

Verträge enthalten Sicherheitsanforderungen, Regelungen zum Umgang mit Informationen, Meldepflichten bei Vorfällen, Prüfrechte und Folgen bei Verstößen.

Prüfhandlung Verträge der Stichprobe anhand einer Checkliste durchsehen und fehlende Regelungen festhalten.

Nachweise Verträge und Anlagen, ausgefüllte Checkliste

Schritt 05 ISO/IEC 27001:2022 Anhang A 5.21; NIS2-Richtlinie Art. 21 Abs. 2 lit. d

Die Lieferkette ist betrachtet: Unterauftragnehmer sind bekannt, werden genehmigt und unterliegen gleichwertigen Anforderungen.

Prüfhandlung Für drei wesentliche Dienstleister die Unterauftragnehmer erfragen und Genehmigung sowie Weitergabe der Anforderungen prüfen.

Nachweise Listen der Unterauftragnehmer, Genehmigungen, Vertragsklauseln

Schritt 06 ISO/IEC 27001:2022 Anhang A 5.19 und 5.15

Zugriffe von Dienstleistern sind auf das Nötige beschränkt, einzeln freigegeben, befristet und werden protokolliert.

Prüfhandlung Externe Konten auslesen und für eine Stichprobe Freigabe, Befristung und Nutzung der letzten Monate prüfen.

Nachweise Auszug externer Konten, Freigaben, Protokolle

Prüfschritte 7 bis 9

Schritt 07

ISO/IEC 27001:2022 Anhang A 5.22

Leistung und Sicherheit der Dienstleister werden regelmäßig überwacht, etwa über Berichte, Zertifikate und Prüfungen vor Ort oder aus der Ferne.

Prüfhandlung Überwachungsplan und Berichte der letzten zwölf Monate für wesentliche Dienstleister ansehen.

Nachweise Überwachungsplan, Leistungsberichte, Prüfberichte, Zertifikate

Schritt 08

ISO/IEC 27001:2022 Anhang A 5.22

Feststellungen aus der Überwachung werden verfolgt und mit dem Dienstleister bis zur Erledigung geklärt.

Prüfhandlung Offene und abgeschlossene Feststellungen der letzten zwölf Monate ansehen und Fristen sowie Erledigung prüfen.

Nachweise Maßnahmenliste, Schriftverkehr, Besprechungsprotokolle

Schritt 09

ISO/IEC 27001:2022 Anhang A 5.22

Änderungen an den Leistungen und Verträgen werden bewertet, bevor sie wirksam werden, auch hinsichtlich der Informationssicherheit.

Prüfhandlung Vertragsänderungen und angekündigte Änderungen der Dienstleister der Stichprobe auf eine Bewertung durchsehen.

Nachweise Änderungsmitteilungen, Bewertungsvermerke

Prüfschritte 10 bis 12

Schritt 10 — ISO/IEC 27001:2022 Anhang A 5.20; BSI DER.2.1

Sicherheitsvorfälle bei Dienstleistern werden gemeldet, erfasst und in das eigene Vorfallsmanagement übernommen.

Prüfhandlung Prüfen, ob Vorfälle von Dienstleistern im Vorfallsregister vorkommen und die Meldewege vereinbart sind.

Nachweise Vorfallsregister, Kontaktliste, Meldewege im Vertrag

Schritt 11 — ISO/IEC 27001:2022 Anhang A 5.19 und 5.18

Bei Beendigung einer Beziehung werden Zugänge entzogen, Informationen zurückgegeben oder gelöscht und die Löschung bestätigt.

Prüfhandlung Zwei beendete Dienstleisterbeziehungen auswählen und Entzug der Zugänge sowie Rückgabe oder Löschung der Daten prüfen.

Nachweise Beendigungsprotokoll, Löschbestätigung, Auszug der Zugänge

Schritt 12 — NIS2-Richtlinie Art. 20

Die Leitung wird über die Risiken aus der Lieferkette und über wesentliche Feststellungen informiert.

Prüfhandlung Berichte und Protokolle der letzten zwölf Monate auf Themen zur Dienstleistersteuerung durchsehen.

Nachweise Berichte an die Geschäftsleitung, Sitzungsprotokolle

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Richtlinie zur Informationssicherheit in Lieferantenbeziehungen
2. Dienstleisterverzeichnis mit Einstufung
3. Risikobewertungen und Auswahlunterlagen der Stichprobe
4. Verträge mit Anlagen zu Sicherheit und Datenverarbeitung
5. Listen der Unterauftragnehmer
6. Überwachungsplan, Leistungsberichte und Prüfberichte
7. Auszug externer Konten und Zugriffe von Dienstleistern
8. Beendigungsprotokolle und Löschbestätigungen

TYPISCHE FESTSTELLUNGEN

- Das Dienstleisterverzeichnis ist unvollständig, einzelne Dienstleister mit Systemzugriff fehlen.
- Die Auswahl erfolgt nach Preis und Fachlichkeit, eine Bewertung der Informationssicherheit findet nicht statt.
- Verträge enthalten keine Meldepflicht bei Sicherheitsvorfällen und keine Prüfrechte.
- Unterauftragnehmer sind nicht bekannt oder nicht genehmigt.
- Die Überwachung beschränkt sich auf die Entgegennahme von Berichten, Feststellungen werden nicht verfolgt.
- Zugänge von Dienstleistern bleiben nach Vertragsende bestehen.

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