Muster-Prüfprogramm

IT-Governance und IT-Strategie

12 Prüfschritte · NIS2, DORA, BSIG

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

DORA Art. 6 Abs. 8 · NIS2-Richtlinie Art. 20 Abs. 1 · § 38 Abs. 1 BSIG · ISO/IEC 27001:2022 Anhang A 5.2 · DORA Art. 5 Abs. 2 lit. c · DORA Art. 6 Abs. 8 lit. b · DORA Art. 6 Abs. 8 lit. c · DORA Art. 5 Abs. 2 lit. g · ISO/IEC 27001:2022 Anhang A 5.1 · NIS2-Richtlinie Art. 20 Abs. 2 · § 38 Abs. 3 BSIG · DORA Art. 5 Abs. 2 lit. i · DORA Art. 6 Abs. 8 lit. d · ISO/IEC 27001:2022 Anhang A 5.35 · DORA Art. 6 Abs. 6 · ISO/IEC 27001:2022 Anhang A 5.3

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob eine freigegebene IT-Strategie aus den Unternehmenszielen abgeleitet ist und ob Rollen, Gremien, Richtlinien, Kennzahlen und Berichtswege eine wirksame Steuerung der IT durch die Geschäftsleitung ermöglichen. Sie beurteilt außerdem, ob die Leitung die Maßnahmen zum Management von Cyberrisiken billigt, überwacht und sich dazu schulen lässt.

GELTUNGSBEREICH

- IT-Strategie, IT-Gremien und Entscheidungsprozesse der Organisation
- Rollen der Geschäftsleitung, der IT-Leitung, der Informationssicherheit und der Kontrollfunktionen
- Planung von Budget und Ressourcen, Kennzahlen und Berichterstattung an die Leitung
- Nicht Gegenstand: die fachliche Prüfung einzelner Projekte oder Systeme

Prüfschritte 1 bis 3

Schritt 01

DORA Art. 6 Abs. 8

Eine IT-Strategie liegt vor, ist aus der Unternehmensstrategie abgeleitet, von der Leitung freigegeben und wird regelmäßig überprüft.

Prüfhandlung Strategie lesen, Freigabe und Datum prüfen und die Ableitung aus den Unternehmenszielen an drei Zielen nachvollziehen.

Nachweise IT-Strategie mit Freigabe, Unternehmensziele, Protokoll der letzten Überprüfung

Schritt 02

NIS2-Richtlinie Art. 20 Abs. 1; § 38 Abs. 1 BSIG

Die Geschäftsleitung billigt die Maßnahmen zum Management von Cyberrisiken und überwacht deren Umsetzung.

Prüfhandlung Protokolle der Leitungssitzungen der letzten zwölf Monate auf Billigung, Berichte und Beschlüsse zu Sicherheitsthemen durchsehen.

Nachweise Sitzungsprotokolle, Beschlussvorlagen, Statusberichte

Schritt 03

ISO/IEC 27001:2022 Anhang A 5.2; DORA Art. 5 Abs. 2 lit. c

Rollen, Verantwortlichkeiten und Befugnisse für IT und Informationssicherheit sind festgelegt und besetzt.

Prüfhandlung Organigramm, Geschäftsordnungen der Gremien und Stellenbeschreibungen abgleichen; Lücken und Doppelzuständigkeiten notieren.

Nachweise Organigramm, Geschäftsordnungen, Rollenbeschreibungen

Prüfschritte 4 bis 6

Schritt 04

DORA Art. 6 Abs. 8 lit. b

Die Organisation hat festgelegt, welches IT-Risiko sie zu tragen bereit ist, und diese Toleranz ist mit der Risikoneigung abgestimmt.

Prüfhandlung Dokument zur Risikotoleranz lesen und prüfen, ob Schwellen in Entscheidungen und Berichten tatsächlich verwendet werden.

Nachweise Festlegung der Risikotoleranz, Risikobericht mit Schwellenwerten

Schritt 05

DORA Art. 6 Abs. 8 lit. c

Für die Ziele der IT und der Informationssicherheit sind Kennzahlen festgelegt, gemessen und berichtet.

Prüfhandlung Kennzahlenkatalog ansehen und für drei Kennzahlen Messmethode, Datenquelle und letzte Berichterstattung nachvollziehen.

Nachweise Kennzahlenkatalog, Kennzahlenbericht, Datenquellen

Schritt 06

DORA Art. 5 Abs. 2 lit. g

Budget und Ressourcen für IT, Sicherheit und Qualifizierung werden geplant und regelmäßig überprüft.

Prüfhandlung Budgetplanung und Ist-Werte ansehen und prüfen, ob Sicherheits- und Schulungsbedarf ausgewiesen ist.

Nachweise Budgetplanung, Budgetbericht, Ressourcenplanung

Prüfschritte 7 bis 9

Schritt 07

ISO/IEC 27001:2022 Anhang A 5.1

Ein Rahmenwerk von Richtlinien ist freigegeben, bekannt gemacht und wird in festen Abständen überprüft.

Prüfhandlung Richtlinienverzeichnis auswerten: Freigabe, Verantwortliche, Datum der letzten Überprüfung.

Nachweise Richtlinienverzeichnis, Freigabevermerke

Schritt 08

NIS2-Richtlinie Art. 20 Abs. 2; § 38 Abs. 3 BSIG

Mitglieder der Geschäftsleitung nehmen regelmäßig an Schulungen zu Cyberrisiken teil.

Prüfhandlung Teilnahmenachweise der Leitung anfordern und Inhalte der Schulung auf Risikobewertung und Auswirkungen prüfen.

Nachweise Teilnahmenachweise, Schulungsunterlagen

Schritt 09

DORA Art. 5 Abs. 2 lit. i

Die Leitung wird regelmäßig über wesentliche Vorfälle, Dienstleisterverträge und geplante Änderungen bei kritischen Dienstleistern unterrichtet.

Prüfhandlung Berichte an die Leitung der letzten vier Quartale auf diese Inhalte prüfen.

Nachweise Leitungsberichte, Verteiler, Protokolle

Prüfschritte 10 bis 12

Schritt 10 — DORA Art. 6 Abs. 8 lit. d

Eine Zielarchitektur ist beschrieben, und Investitionen und Projekte werden daran ausgerichtet.

Prüfhandlung Zielarchitektur und Projektportfolio vergleichen und für drei Vorhaben die Begründung im Portfolio nachvollziehen.

Nachweise Zielarchitektur, Projektportfolio, Entscheidungsvorlagen

Schritt 11 — ISO/IEC 27001:2022 Anhang A 5.35; DORA Art. 6 Abs. 6

Die Steuerung der IT und der Informationssicherheit wird unabhängig überprüft, etwa durch die interne Revision.

Prüfhandlung Prüfungsplan und Berichte der letzten zwei Jahre ansehen und den Stand der Maßnahmen nachverfolgen.

Nachweise Prüfungsplan, Prüfberichte, Maßnahmenverfolgung

Schritt 12 — ISO/IEC 27001:2022 Anhang A 5.3

Unvereinbare Aufgaben, etwa Betrieb und Kontrolle derselben Systeme, sind getrennt.

Prüfhandlung Rollenzuschnitte der IT auf Konflikte prüfen und bei Restkonflikten die ausgleichenden Kontrollen nachvollziehen.

Nachweise Rollenbeschreibungen, Konfliktmatrix, Nachweise ausgleichender Kontrollen

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. IT-Strategie mit Freigabe und Überprüfungsnachweis
2. Organigramm und Geschäftsordnungen der IT-Gremien
3. Festlegung der Risikotoleranz
4. Kennzahlenkatalog und Kennzahlenberichte
5. Budgetplanung und Budgetbericht der IT
6. Richtlinienverzeichnis
7. Berichte an die Geschäftsleitung der letzten vier Quartale
8. Schulungsnachweise der Geschäftsleitung

TYPISCHE FESTSTELLUNGEN

- Die IT-Strategie ist veraltet oder nie von der Leitung freigegeben worden.
- Die Geschäftsleitung erhält keine regelmäßigen Berichte zu Cyberrisiken.
- Kennzahlen sind festgelegt, werden aber nicht gemessen oder nicht berichtet.
- Die Risikotoleranz ist nicht beschrieben, Entscheidungen bleiben ohne Maßstab.
- Mitglieder der Geschäftsleitung haben keine Schulung zu Cyberrisiken besucht.
- Richtlinien werden nicht überprüft, Verantwortliche sind nicht benannt.

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