Muster-Prüfprogramm

# ISMS nach ISO/IEC 27001

## 13 Prüfschritte · ISO 27001, BSI

13 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 9 Unterlagen zur Anforderung und die typischen Feststellungen.

ISO/IEC 27001:2022 Kapitel 4.1 und 4.2 · ISO/IEC 27001:2022 Kapitel 4.3 · ISO/IEC 27001:2022 Kapitel 5.1 und 5.2 · BSI-Standard 200-1 · ISO/IEC 27001:2022 Kapitel 5.3 · ISO/IEC 27001:2022 Kapitel 6.1 und 8.2 · BSI-Standard 200-3 · ISO/IEC 27001:2022 Kapitel 6.1.3 und 8.3 · ISO/IEC 27001:2022 Kapitel 6.2 · ISO/IEC 27001:2022 Kapitel 7.1, 7.2 und 7.3 · ISO/IEC 27001:2022 Kapitel 7.5 · ISO/IEC 27001:2022 Kapitel 9.1 · ISO/IEC 27001:2022 Kapitel 9.2 · ISO/IEC 27001:2022 Kapitel 9.3 · ISO/IEC 27001:2022 Kapitel 10.1 und 10.2

## Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation ein Managementsystem für Informationssicherheit eingerichtet hat, das Kontext, Geltungsbereich, Führung, Risikobeurteilung und Risikobehandlung, Unterstützung, Betrieb, Bewertung und Verbesserung schlüssig verbindet. Sie beurteilt außerdem, ob internes Audit und Managementbewertung zu Entscheidungen und Korrekturmaßnahmen führen.

### GELTUNGSBEREICH

- Managementsystem für Informationssicherheit im festgelegten Geltungsbereich
- Prozesse der Kapitel 4 bis 10 der ISO/IEC 27001:2022 einschließlich der Erklärung zur Anwendbarkeit
- Rollen der Leitung, des Informationssicherheitsbeauftragten und der Prozessverantwortlichen
- Nicht Gegenstand: die vertiefte Prüfung einzelner Maßnahmen aus Anhang A, die eigene Prüfprogramme haben

## Prüfschritte 1 bis 3

Schritt 01

ISO/IEC 27001:2022 Kapitel 4.1 und 4.2

### Interne und externe Themen sowie die Anforderungen interessierter Parteien sind ermittelt und werden aktuell gehalten.

**Prüfhandlung** Kontextanalyse und Liste der interessierten Parteien lesen und prüfen, ob gesetzliche und vertragliche Anforderungen enthalten sind.

**Nachweise** Kontextanalyse, Liste interessierter Parteien und ihrer Anforderungen

Schritt 02

ISO/IEC 27001:2022 Kapitel 4.3

### Der Geltungsbereich ist dokumentiert, begründet und berücksichtigt Schnittstellen und Abhängigkeiten.

**Prüfhandlung** Geltungsbereich mit Organigramm, Standorten und ausgelagerten Diensten abgleichen.

**Nachweise** Dokument zum Geltungsbereich, Standortliste, Schnittstellenbeschreibung

Schritt 03

ISO/IEC 27001:2022 Kapitel 5.1 und 5.2; BSI-Standard 200-1

### Die oberste Leitung zeigt Führung, hat eine Sicherheitsleitlinie freigegeben und stellt deren Bekanntmachung sicher.

**Prüfhandlung** Leitlinie lesen, Freigabe prüfen und im Interview mit der Leitung ihre Beteiligung am Managementsystem erfragen.

**Nachweise** Informationssicherheitsleitlinie, Bekanntmachung, Interviewnotizen

## Prüfschritte 4 bis 6

Schritt 04

ISO/IEC 27001:2022 Kapitel 5.3

### Rollen, Verantwortlichkeiten und Befugnisse im Managementsystem sind zugewiesen und bekannt gemacht.

**Prüfhandlung** Bestellung des Informationssicherheitsbeauftragten und Rollenbeschreibungen ansehen, Berichtsweg zur Leitung nachvollziehen.

**Nachweise** Bestellungsurkunde, Rollenbeschreibungen, Berichtsweg

Schritt 05

ISO/IEC 27001:2022 Kapitel 6.1 und 8.2; BSI-Standard 200-3

### Ein festgelegtes Verfahren zur Risikobeurteilung liefert wiederholbare Ergebnisse und wird in geplanten Abständen und bei Änderungen angewandt.

**Prüfhandlung** Methodenbeschreibung lesen und die letzte Risikobeurteilung an drei Risiken auf Bewertung und Begründung prüfen.

**Nachweise** Methode zur Risikobeurteilung, Risikoregister, Datum der letzten Beurteilung

Schritt 06

ISO/IEC 27001:2022 Kapitel 6.1.3 und 8.3

### Ein Plan zur Risikobehandlung und eine Erklärung zur Anwendbarkeit liegen vor; Restrisiken sind von den Risikoeigentümern akzeptiert.

**Prüfhandlung** Erklärung zur Anwendbarkeit auf Begründungen für Ausschlüsse prüfen und Risikoakzeptanzen für drei Restrisiken nachvollziehen.

**Nachweise** Erklärung zur Anwendbarkeit, Risikobehandlungsplan, Akzeptanzvermerke

## Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Kapitel 6.2

### Messbare Sicherheitsziele sind festgelegt, mit Verantwortlichen, Ressourcen und Terminen geplant.

**Prüfhandlung** Zielübersicht ansehen und für drei Ziele Messung, Verantwortliche und Zielerreichung prüfen.

**Nachweise** Zielübersicht, Statusberichte zu den Zielen

Schritt 08 — ISO/IEC 27001:2022 Kapitel 7.1, 7.2 und 7.3

### Ressourcen stehen bereit; Personen mit Sicherheitsaufgaben sind kompetent, und Mitarbeitende kennen ihren Beitrag.

**Prüfhandlung** Kompetenznachweise für zwei Schlüsselrollen ansehen und bei fünf Mitarbeitenden die Kenntnis der Leitlinie erfragen.

**Nachweise** Qualifikationsnachweise, Schulungsplan, Interviewnotizen

Schritt 09 — ISO/IEC 27001:2022 Kapitel 7.5

### Dokumentierte Information wird gelenkt: Freigabe, Versionierung, Verteilung und Aufbewahrung sind geregelt.

**Prüfhandlung** Für fünf Dokumente des Managementsystems Version, Freigabe und Ablageort prüfen.

**Nachweise** Dokumentenlenkungsregel, Dokumentenverzeichnis

## Prüfschritte 10 bis 13

Schritt 10 — ISO/IEC 27001:2022 Kapitel 9.1

### Leistung und Wirksamkeit des Managementsystems werden überwacht, gemessen und ausgewertet.

**Prüfhandlung** Festlegungen zu Messgrößen, Methoden und Zeitpunkten ansehen und die letzten Auswertungen prüfen.

**Nachweise** Messkonzept, Auswertungen, Kennzahlenberichte

Schritt 11 — ISO/IEC 27001:2022 Kapitel 9.2

### Interne Audits werden nach einem Programm durchgeführt, von objektiven Auditoren, und ihre Ergebnisse werden an die Leitung berichtet.

**Prüfhandlung** Auditprogramm der letzten drei Jahre auf Abdeckung des Geltungsbereichs prüfen und zwei Auditberichte ansehen.

**Nachweise** Auditprogramm, Auditberichte, Nachweis der Unabhängigkeit der Auditoren

Schritt 12 — ISO/IEC 27001:2022 Kapitel 9.3

### Die Leitung bewertet das Managementsystem in geplanten Abständen mit den vorgesehenen Eingaben und trifft dokumentierte Entscheidungen.

**Prüfhandlung** Protokoll der letzten Managementbewertung auf Eingaben, Ergebnisse und Beschlüsse prüfen.

**Nachweise** Protokoll der Managementbewertung, Beschlussliste

Schritt 13 — ISO/IEC 27001:2022 Kapitel 10.1 und 10.2

### Nichtkonformitäten werden ursächlich behandelt, Korrekturmaßnahmen auf Wirksamkeit geprüft, und das Managementsystem wird fortlaufend verbessert.

**Prüfhandlung** Fünf Nichtkonformitäten aus Audits oder Vorfällen von der Ursachenanalyse bis zur Wirksamkeitsprüfung nachverfolgen.

**Nachweise** Register der Nichtkonformitäten, Ursachenanalysen, Wirksamkeitsnachweise

Unterlagenanforderung

# Diese 9 Unterlagen vor Prüfungsbeginn anfordern

1. Kontextanalyse und Liste interessierter Parteien
2. Dokument zum Geltungsbereich
3. Informationssicherheitsleitlinie und Rollenbeschreibungen
4. Methode zur Risikobeurteilung, Risikoregister und Risikobehandlungsplan
5. Erklärung zur Anwendbarkeit
6. Sicherheitsziele mit Statusberichten
7. Auditprogramm und interne Auditberichte
8. Protokoll der letzten Managementbewertung
9. Register der Nichtkonformitäten und Korrekturmaßnahmen

## TYPISCHE FESTSTELLUNGEN

- Die Erklärung zur Anwendbarkeit schließt Maßnahmen ohne Begründung aus.
- Die Risikobeurteilung wurde seit Jahren nicht wiederholt, auch nicht nach größeren Änderungen.
- Sicherheitsziele sind nicht messbar formuliert.
- Das Auditprogramm deckt den Geltungsbereich nicht ab, Auditoren prüfen ihre eigene Arbeit.
- Die Managementbewertung ist ein Kurzvermerk ohne Eingaben und ohne Beschlüsse.
- Korrekturmaßnahmen werden abgeschlossen, ohne ihre Wirksamkeit zu prüfen.

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