

Checkliste: ISMS-Mindestanforderungen

1. Organisationskontext, Führung & Richtlinien (ISO 27001 Kap. 4.1–4.4, 5.1–5.3 / ISO 27002 Controls 5.1–5.4)

| Prüfpunkt | Bewertung |
|--|---|
| Sind interne und externe Themen, die das ISMS beeinflussen, bestimmt und dokumentiert? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Sind relevante interessierte Parteien und deren Anforderungen dokumentiert? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Ist der Geltungsbereich (Scope) des ISMS eindeutig festgelegt und dokumentiert? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Hat die Leitung die Informationssicherheitspolitik genehmigt und kommuniziert? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Sind Rollen, Verantwortlichkeiten und Befugnisse definiert und kommuniziert? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |

2. Informationssicherheitsmanagement & Verantwortlichkeiten (Kap. 5.2–5.3, 7.1 / Controls 5.5–5.12)

| Prüfpunkt | Bewertung |
|--|---|
| Bestehen festgelegte Kommunikationswege zu Behörden und Interessengruppen? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Werden Informationssicherheitsaufgaben und Zuständigkeiten regelmäßig überprüft? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Wird Threat Intelligence systematisch erhoben und bewertet? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Ist Informationssicherheit in Projektmanagementprozesse integriert? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Existieren aktuelle Inventarlisten für Informationswerte und deren Eigentümer? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |

3. Risikomanagement & Risikobehandlung (Kap. 6.1.1–6.1.3 / Controls 5.7, 5.24–5.28)

| Prüfpunkt | Bewertung |
|---|---|
| Gibt es ein dokumentiertes Verfahren zur Informationssicherheits-Risikobeurteilung? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Wird die Risikobeurteilung regelmäßig und bei Änderungen durchgeführt? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Ist ein Risikobehandlungsplan vorhanden und genehmigt? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Ist die SoA vollständig und spiegelt alle relevanten Controls wider? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Werden Erkenntnisse aus Sicherheitsvorfällen in die Risikobehandlung integriert? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |

4. Lieferantenmanagement & Compliance (Kap. 4.2, 5.5, 6.1.3 / Controls 5.19–5.23, 5.31)

| Prüfpunkt | Bewertung |
|--|---|
| Sind Sicherheitsanforderungen an Lieferanten in Verträgen festgelegt? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Werden Lieferanten regelmäßig auf Informationssicherheitsrisiken überprüft? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Besteht ein Verfahren zur Überwachung von Lieferantenleistungen (SLA-Kontrolle)? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Wird die rechtliche und regulatorische Compliance regelmäßig bewertet? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |

5. Personelle Sicherheit & Kompetenzmanagement (Kap. 7.1–7.3 / Controls 6.1–6.3, 6.8)

| Prüfpunkt | Bewertung |
|--|---|
| Sind Rollen und Verantwortlichkeiten vor Eintritt klar definiert? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Werden Sicherheitsüberprüfungen vor Beschäftigung durchgeführt? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Erhalten Mitarbeitende regelmäßig Schulungen zur Informationssicherheit? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Werden Verstöße gegen Sicherheitsrichtlinien disziplinarisch behandelt? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |

6. Betriebssicherheit, Monitoring & Incident-Management (Kap. 8.1, 9.1 / Controls 8.15–8.24 / 5.24–5.27)

| Prüfpunkt | Bewertung |
|--|---|
| Werden sicherheitsrelevante Ereignisse kontinuierlich protokolliert und überwacht? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Gibt es dokumentierte Verfahren zur Meldung und Behandlung von Sicherheitsvorfällen? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Werden Vorfall-Trends regelmäßig analysiert und bewertet? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Wird die Effektivität des Incident-Response-Prozesses regelmäßig überprüft? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |

7. Interne Audits, Managementbewertung & kontinuierliche Verbesserung (Kap. 9.2–10.2 / Controls 5.35–5.37)

| Prüfpunkt | Bewertung |
|---|---|
| Gibt es ein dokumentiertes internes Auditprogramm mit Frequenzen, Verantwortlichkeiten und Kriterien? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Werden Auditfeststellungen nachverfolgt und Korrekturmaßnahmen dokumentiert? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Führt die Leitung regelmäßig eine Managementbewertung gemäß 9.3 durch? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Werden Ergebnisse aus Audits, KPI-Analysen und Vorfällen in Verbesserungsmaßnahmen umgesetzt? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Ist der PDCA-Zyklus (Plan-Do-Check-Act) im ISMS nachweisbar etabliert? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |

8. Wirksamkeitsprüfung & Trends
(Kap. 9–10 / Controls 8.15, 8.16, 5.27, 5.36, 5.37)

| Prüfpunkt | Bewertung |
|---|---|
| Werden Wirksamkeitskennzahlen (KPI-Trends) regelmäßig erhoben und ausgewertet? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Werden Ergebnisse aus KPI-Analysen dokumentiert und in Verbesserungsplänen umgesetzt? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Sind die Ergebnisse der Wirksamkeitsprüfung Teil der Managementbewertung? | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |