

ISO 27001:2024 Checkliste

Diese Checkliste enthält alle Anforderungen der ISO 27001:2024 aus den Kapiteln 4 bis 10 sowie die Referenzmaßnahmen und -ziele des Anhang A (Kapitel A.5 bis A.18). Für jedes Kapitel sind Beispiele enthalten.

Kapitel 4: Kontext der Organisation

- Interne und externe Themen identifizieren
- Interessierte Parteien bestimmen
- Anwendungsbereich des ISMS festlegen

Kapitel 5: Führung

- ISMS-Politik erstellen
- Rollen und Verantwortlichkeiten festlegen

Kapitel 6: Planung

- Risikoanalyse durchführen
- ISMS-Ziele definieren

Kapitel 7: Unterstützung

- Ressourcen bereitstellen
- Kompetenz und Bewusstsein sicherstellen

Kapitel 8: Betrieb

- Risikobehandlung umsetzen
- Dokumentierte Informationen pflegen

Kapitel 9: Bewertung der Leistung

- Interne Audits durchführen
- Managementbewertung umsetzen

Kapitel 10: Verbesserung

- Korrekturmaßnahmen ergreifen
- Kontinuierliche Verbesserung sicherstellen

Anhang A: Referenzmaßnahmen und -ziele

A.5: Informationssicherheitsrichtlinien

Ziel: Sicherstellen, dass Richtlinien für Informationssicherheit erstellt und kommuniziert werden.

Maßnahmen:

- Erstellung einer Informationssicherheitsrichtlinie
- Regelmäßige Überprüfung und Aktualisierung

Beispiel: Dokumentierte ISMS-Politik, die allen Mitarbeitern zugänglich ist.

A.6: Organisation der Informationssicherheit

Ziel: Sicherstellen, dass Verantwortlichkeiten für Informationssicherheit definiert sind.

Maßnahmen:

- Benennung eines ISMS-Beauftragten
- Trennung von Aufgaben

Beispiel: Organigramm mit klaren Rollen für Informationssicherheit.

A.7: Personalsicherheit

Ziel: Sicherstellen, dass Mitarbeiter ihre Sicherheitsverantwortung kennen.

Maßnahmen:

- Schulungen zur Informationssicherheit
- Verpflichtungserklärungen

Beispiel: Onboarding-Prozess mit Sicherheitsunterweisung.

A.8: Asset Management

Ziel: Sicherstellen, dass Werte identifiziert und geschützt werden.

Maßnahmen:

- Inventarisierung von Assets
- Klassifizierung nach Schutzbedarf

Beispiel: Asset-Liste mit Klassifizierung (z.B. vertraulich, öffentlich).

A.9: Zugriffskontrolle

Ziel: Sicherstellen, dass Zugriffe kontrolliert und autorisiert sind.

Maßnahmen:

- Rollenkonzept für Zugriffsrechte
- Regelmäßige Überprüfung von Berechtigungen

Beispiel: Implementierung von MFA für kritische Systeme.

A.10: Kryptographie

Ziel: Sicherstellen, dass kryptografische Maßnahmen zum Schutz von Informationen eingesetzt werden.

Maßnahmen:

- Verwendung starker Verschlüsselungsalgorithmen
- Schlüsselmanagement

Beispiel: AES-256-Verschlüsselung für gespeicherte Daten.

A.11: Physische und umgebungsbezogene Sicherheit

Ziel: Schutz physischer Assets vor unbefugtem Zugriff und Umwelteinflüssen.

Maßnahmen:

- Zutrittskontrollsysteme
- Brandschutzmaßnahmen

Beispiel: Serverraum mit Zugangskontrolle und Brandmeldeanlage.

A.12: Betriebssicherheit

Ziel: Sicherstellen, dass IT-Betrieb sicher und kontrolliert erfolgt.

Maßnahmen:

- Patch-Management
- Malware-Schutz

Beispiel: Regelmäßige Updates und Virenskans.

A.13: Kommunikationssicherheit

Ziel: Schutz von Informationen in Netzwerken und bei Übertragung.

Maßnahmen:

- VPN für externe Zugriffe
- TLS für Datenübertragung

Beispiel: E-Mail-Verschlüsselung mit S/MIME.

A.14: Systemakquisition, Entwicklung und Wartung

Ziel: Sicherstellen, dass Sicherheitsanforderungen in den Lebenszyklus von Systemen integriert sind.

Maßnahmen:

- Sicherheitsanforderungen in Spezifikationen
- Code-Reviews

Beispiel: Secure Coding Guidelines für Entwickler.

A.15: Lieferantenbeziehungen

Ziel: Sicherstellen, dass Lieferanten Sicherheitsanforderungen erfüllen.

Maßnahmen:

- Vertragliche Sicherheitsvereinbarungen
- Lieferantenbewertungen

Beispiel: Sicherheitsklauseln in Dienstleistungsverträgen.

A.16: Management von Informationssicherheitsvorfällen

Ziel: Sicherstellen, dass Sicherheitsvorfälle erkannt und behandelt werden.

Maßnahmen:

- Incident-Response-Plan
- Meldesystem für Vorfälle

Beispiel: 24/7-Hotline für Sicherheitsvorfälle.

A.17: Informationssicherheitsaspekte beim Business Continuity Management

Ziel: Sicherstellen, dass Informationssicherheit in Notfallplänen berücksichtigt wird.

Maßnahmen:

- Backup-Strategien
- Notfallübungen

Beispiel: Regelmäßige Tests des Disaster-Recovery-Plans.

A.18: Compliance

Ziel: Sicherstellen, dass gesetzliche und vertragliche Anforderungen erfüllt werden.

Maßnahmen:

- Regelmäßige Compliance-Prüfungen
- Lizenzmanagement

Beispiel: Dokumentierte DSGVO-Konformität.

Wichtiger Hinweis: Diese Checkliste dient ausschließlich als unverbindliche Orientierungshilfe zur Umsetzung der Normen-Anforderungen und ersetzt keine individuelle Beratung. Die Anwendung der Checkliste erfolgt auf eigene Verantwortung. Eine Haftung für die Vollständigkeit, Aktualität und Richtigkeit der Inhalte sowie für daraus resultierende Schäden ist ausgeschlossen. Insbesondere ersetzt die Checkliste keine rechtliche Prüfung im Einzelfall oder die Berücksichtigung spezifischer betrieblicher Gegebenheiten. Es wird empfohlen, bei Unsicherheiten oder spezifischen Fragestellungen fachkundigen Rat (z. B. bei QAS-Company AG oder einem Rechtsanwalt) einzuholen.