ISO 27001:2022 Checkliste für Unternehmen

Diese Checkliste dient Unternehmen als praxisorientierter Leitfaden für den Aufbau, die Bewertung und die Auditvorbereitung eines Informationssicherheits-Managementsystems (ISMS) nach ISO/IEC 27001:2022. Sie kombiniert die Anforderungen der Kapitel 4 bis 10 mit den Controls aus Annex A und eignet sich besonders für interne Readiness-Prüfungen vor einem Zertifizierungsaudit.

Grundlagen und Projektstart

- Relevante Normen beschafft und ausgewertet: ISO/IEC 27001:2022 sowie unterstützend ISO/IEC 27002:2022.
- Projektauftrag für die Einführung oder Weiterentwicklung des ISMS schriftlich definiert.
- Verantwortlichkeiten festgelegt, zum Beispiel Geschäftsleitung, ISMS-Leitung, Risk Owner, Asset Owner und Fachverantwortliche.
- Zeitplan mit Meilensteinen für Scope, Gap-Analyse, Risikobehandlung, Dokumentation, internes Audit und Management-Review erstellt.

Kontext der Organisation

- Interne und externe Themen ermittelt, die das ISMS beeinflussen, etwa regulatorische Anforderungen, Kundenanforderungen, Marktumfeld, Technologieeinsatz und Lieferkettenabhängigkeiten.
- Relevante interessierte Parteien identifiziert und ihre Anforderungen dokumentiert, zum Beispiel Kunden, Behörden, Versicherer, Gesellschafter und Mitarbeitende.
- Geltungsbereich des ISMS eindeutig definiert, einschließlich Standorten, Organisationseinheiten, Prozessen, Informationswerten und Systemen.
- Schnittstellen zu externen Dienstleistern und ausgelagerten Prozessen beschrieben.

Führung und Governance

- Informationssicherheitspolitik verabschiedet, freigegeben und intern kommuniziert.
- Messbare Informationssicherheitsziele festgelegt, inklusive Verantwortlichen, Kennzahlen und Zielterminen.
- Nachweisbares Commitment der Leitung vorhanden, etwa durch Ressourcenzuweisung, Freigaben, Reviews und Eskalationswege.

- Rollen, Verantwortlichkeiten und Befugnisse für Informationssicherheit dokumentiert und bekannt gemacht.

Risiko- und Maßnahmenmanagement

- Methodik für Risikoidentifikation, Risikoanalyse und Risikobewertung dokumentiert.
- Bewertungskriterien und Risikoakzeptanz definiert.
- Informationswerte oder Asset-Gruppen identifiziert und den relevanten Prozessen zugeordnet.
- Risiken systematisch bewertet, dokumentiert und freigegeben.
- Risikobehandlungsplan erstellt, mit Maßnahmen, Fristen, Verantwortlichkeiten und Umsetzungsstatus.
- Statement of Applicability (SoA) erstellt und für alle relevanten Annex-A-Controls begründet, ob diese anwendbar oder nicht anwendbar sind.

Unterstützung und dokumentierte Information

- Ausreichende personelle, technische und finanzielle Ressourcen für das ISMS bereitgestellt.
- Kompetenzanforderungen je Rolle festgelegt und Nachweise zu Schulung, Erfahrung oder Qualifikation gepflegt.
- Awareness-Maßnahmen für Mitarbeitende umgesetzt, etwa Schulungen, Lernmodule oder Phishing-Übungen.
- Interne und externe Kommunikationsregeln für Informationssicherheit dokumentiert.
- Dokumentierte Informationen gelenkt, zum Beispiel durch Versionierung, Freigabe, Zugriffssteuerung und Aufbewahrungsregeln.

Betrieb des ISMS

- Operative Sicherheitsprozesse dokumentiert und umgesetzt, etwa Incident-Management, Change-Management, Zugriffsmanagement und Backup.
- Sicherheitsmaßnahmen in laufende Geschäftsprozesse integriert.
- Risiken bei Änderungen, Projekten, neuen Anwendungen und Dienstleistern berücksichtigt.
- Lieferanten und externe Services in die Sicherheitssteuerung eingebunden, einschließlich Anforderungen, Prüfungen und Überwachung.

Leistungsauswertung und Verbesserung

- Kriterien für Überwachung und Messung der Wirksamkeit des ISMS und der Sicherheitsmaßnahmen definiert.
- Auditprogramm für interne Audits geplant und durchgeführt.
- Auditfeststellungen dokumentiert und in Maßnahmen überführt.
- Management-Reviews regelmäßig durchgeführt und protokolliert.
- Nichtkonformitäten, Ursachenanalysen und Korrekturmaßnahmen systematisch bearbeitet.
- Kontinuierliche Verbesserung des ISMS nachweisbar umgesetzt.

Annex A: Organisatorische Controls

- Richtlinien und Verfahren zur Informationssicherheit vorhanden und aktuell.
- Regelungen zur Informationsklassifizierung und zum Umgang mit Informationen definiert.
- Lieferantenmanagement mit Sicherheitsanforderungen und Überwachung etabliert.
- Nutzung von Cloud-Diensten geregelt und risikobasiert bewertet.
- Prozesse für Incident-Reporting, Business Continuity und Lessons Learned vorhanden.

Annex A: Personelle Controls

- Sicherheitsanforderungen im Onboarding, während des Beschäftigungsverhältnisses und beim Offboarding geregelt.
- Vertraulichkeits- und Geheimhaltungsverpflichtungen dokumentiert.
- Disziplinarische und organisatorische Maßnahmen bei Verstößen definiert.
- Rollenbezogene Schulung und Sensibilisierung umgesetzt.

Annex A: Physische Controls

- Zutrittskontrollen für Gebäude, Büros, Technikräume und Rechenzentrumsbereiche definiert und wirksam.
- Schutz gegen Feuer, Wasser, Stromausfall und andere physische Risiken berücksichtigt.
- Clean-Desk- und Clear-Screen-Regeln vorhanden.
- Sicherheitsanforderungen für mobile Arbeit und Homeoffice umgesetzt.

Annex A: Technologische Controls

- Identity- und Access-Management umgesetzt, einschließlich Berechtigungsvergabe, Rezertifizierung und Least-Privilege-Prinzip.
- Netzwerksicherheitsmaßnahmen wie Segmentierung, sichere Fernzugriffe und Firewalls etabliert.
- Schwachstellenmanagement und Patch-Management geregelt.
- Schutz vor Malware und unautorisierten Änderungen implementiert.
- Logging und Monitoring sicherheitsrelevanter Ereignisse eingerichtet.
- Backup- und Wiederherstellungsmaßnahmen definiert, getestet und dokumentiert.
- Sicherheitsanforderungen in Entwicklung, Test und Betrieb von Anwendungen berücksichtigt.[

Zentrale Pflichtdokumente und Nachweise

Dokument oder Nachweis	Zweck
Scope des ISMS	Abgrenzung des Geltungsbereichs.
Informationssicherheitspolitik	Strategische Leitlinie und Managementvorgabe.
Informationssicherheitsziele	Messbare Zieldefinition.
Risikoanalyse und Methodik	Strukturierte Bewertung von Risiken.
Risikobehandlungsplan	Nachweis geplanter Maßnahmen.
Statement of Applicability	Begründete Auswahl der Annex-A-Controls.
Auditprogramm und Auditberichte	Nachweis interner Prüfungen.
Management-Review-Protokolle	Nachweis der Lenkung durch das Management.
Nachweise zu Schulung und Kompetenz	Eignung und Befähigung relevanter Rollen.
Korrekturmaßnahmen und Verbesserungen	Nachweis systematischer Weiterentwicklung.]

Einsatz der Checkliste

Diese Checkliste eignet sich für eine Erstbewertung, ein internes Pre-Assessment, die Vorbereitung auf ein Stage-1- oder Stage-2-Audit sowie für die strukturierte Fortschrittskontrolle im

CONSUVATION GmbH
Tilsiter Str. 6
71065 Sindelfingen
www.consuvation.com

Telefon: +49 7031 4181-860
E-Mail: contact@consuvation.com