	Datum:	Seite
Checkliste zur ISO/IEC 27001 Auditvorbereitung und Zertifizierung	14.02.2025	1 von 7

Erstelldatum	13.01.2023
Update	14.02.2025

Herausgeber	Teilnehmer der Bewertung zur Selbsteinschätzung	
	Name	Position
SMCT MANAGEMENT concept Stefan Strößenreuther Reuthweg 11 95100 Selb		

Inhaltsverzeichnis

Im Folgenden findest Du eine Zertifizierungsvorbereitungs-Checkliste für ISO/IEC 27001, die nicht nur die allgemeinen Anforderungen der Norm berücksichtigt, sondern Dir einen schrittweisen Fahrplan bietet, um Dein Informationssicherheitsmanagementsystem (ISMS) audit-ready zu machen.

Diese Checkliste fokussiert darauf, welche praktischen Schritte und Nachweise vor einer Zertifizierung besonders wichtig sind. Achte darauf, sie an Deine organisationstypischen Gegebenheiten anzupassen (Branche, Größe, IT-Landschaft usw.).

1. Projektorganisation und Ressourcen		
1.1 Projektteam & Rollen	Umgesetzt	Zufrieden
Projektleiter (z. B. Informationssicherheitsbeauftragter) und Kernteam benennen.	☐	☐
Verantwortlichkeiten für Teilbereiche (z. B. Risikoanalyse, Dokumentenmanagement, Kommunikation) festlegen.	☐	☐
1.2 Zeit- und Ressourcenplan	Umgesetzt	Zufrieden
Meilensteine (Gap-Analyse, internes Audit, Zertifizierungsaudit) definieren.	☐	☐
Budget und personelle Ressourcen (z. B. für Schulungen, Dokumentation) sicherstellen.	☐	☐
1.3 Bewusstsein des TOP-Managements	**Umgesetzt**	**Zufrieden**
Kick-off-Meeting mit der Führungsebene durchführen, Wichtigkeit der ISO 27001 erläutern.	☐	☐
Offizielle **Freigabe** für das Zertifizierungsprojekt (z. B. Projektauftrag, Budget) einholen.	☐	☐

2. Scope und Kontextanalyse		
2.1 Geltungsbereich (Scope)	Umgesetzt	Zufrieden
Festlegen, welche **Abteilungen, Standorte, IT-Systeme** und **Prozesse** das ISMS umfassen soll.	☐	☐
Begründete **Ausnahmen** (Exclusions) dokumentieren (z. B. externe Niederlassungen, falls nicht relevant).	☐	☐
2.2 Interne & externe Faktoren	**Umgesetzt**	**Zufrieden**
Kontextanalyse erstellen (z. B. Unternehmenskultur, relevante Technologien, gesetzliche Anforderungen.	☐	☐
Klimawandel-Faktoren (ab Nov. 2024 verpflichtend) auf potenzielle Auswirkungen auf ISMS prüfen.	☐	☐
2.3 Stakeholder Anforderungen	**Umgesetzt**	**Zufrieden**
Interessierte Parteien (z. B. Kunden, Behörden, Lieferanten) und deren Sicherheitsanforderungen identifizieren.	☐	☐
Dokumentation (z. B. Matrix, Stakeholder-Register) aktualisieren und im ISMS-Kontext erfassen.	☐	☐

3. Risikoanalyse und -behandlung		
3.1 Methodik und Verfahren	Umgesetzt	Zufrieden
Eine **anerkannte Risikomethodik** (z. B. ISO/IEC 27005, NIST, eigene Matrix) auswählen und dokumentieren.	☐	☐
Risikokategorien (z. B. Netzwerk, Personal, physische Sicherheit) definieren.	☐	☐
3.2 Identifikation und Bewertung	**Umgesetzt**	**Zufrieden**
Assets (Hardware, Software, Datenbanken), **Bedrohungen** (Malware, Insider) und **Schwachstellen** bestimmen.	☐	☐
Risikobewertung (Eintrittswahrscheinlichkeit, Auswirkung) und Priorisierung durchführen.	☐	☐
3.3 Behandlung & Risikobehandlungsplan	**Umgesetzt**	**Zufrieden**
Maßnahmen (Minderung, Übertragung, Akzeptanz, Vermeidung) je Risiko definiere.	☐	☐
Risikobehandlungsplan erstellen: Maßnahmen mit Verantwortlichkeiten, Zeitplan, Status.	☐	☐
3.4 Freigabe durch Management	**Umgesetzt**	**Zufrieden**
Risikoergebnisse und empfohlene Maßnahmen mit dem Top-Management abstimmen.	☐	☐
Dokumentation (Risikoanalyse, -bewertung, -plan) genehmigen lassen.	☐	☐

4. ISMS Dokumentation		
4.1 ISMS Politik und Ziele	Umgesetzt	Zufrieden
Informationssicherheitspolitik formulieren, vom Top-Management unterzeichnet.	☐	☐
Ziele (z. B. Incident-Reduktion, Verfügbarkeit, Awareness-Level) festlegen, die SMART sind.	☐	☐
4.2 Verfahrensanweisungen & Richtlinien	**Umgesetzt**	**Zufrieden**
Richtlinien für **Passwortrichtlinien**, **Zugriffsrechte**, **Change Management**, **Notfallmanagement** usw. erstellen oder aktualisieren.	☐	☐
Dokumentierte Prozesse (z. B. On-/Offboarding, Patch-Management) klar definieren.	☐	☐
4.3 Anhang A Mapping	**Umgesetzt**	**Zufrieden**
ISO 27001 Anhang A (Controls) durchgehen; Begründung für angewendete oder nicht angewendete Controls dokumentieren.	☐	☐
Statement of Applicability (SoA) verfassen, um festzulegen, welche Controls relevant sind und wie sie umgesetzt werden.	☐	☐
4.4 Dokumentenlenkung	**Umgesetzt**	**Zufrieden**

Ein Dokumentationssystem (z. B. SharePoint, DMS) nutzen, um **Versionierung** und **Freigabeprozesse** zu gewährleisten.	☐	☐
Klar festlegen, wer was **veröffentlicht**, **prüft** und **archiviert.**	☐	☐

5. Technische und organisatorische Kontrollen		
5.1 Technische Sicherheit	Umgesetzt	Zufrieden
Firewall-, AV- und Patch-Management-Standards prüfen; regelmäßige **Vulnerability-Scans** durchführen.	☐	☐
Backup- und Recovery-Konzepte (z. B. Testwiederherstellung, Offsite-Backups) dokumentieren und testen.	☐	☐
Kryptografie-Richtlinien (Schlüsselmanagement, Verschlüsselungs-Level) definieren.	☐	☐
5.2 Physische Sicherheit	**Umgesetzt**	**Zufrieden**
Zugangskontrollen, Videoüberwachung, Brand- und Wasserschutzmaßnahmen in relevanten Räumlichkeiten verifizieren.	☐	☐
Serverräume, Infrastruktur, Schließkonzepte und Besucher-Management prüfen.	☐	☐
5.3 Organisatorische Maßnahmen	**Umgesetzt**	**Zufrieden**
Informationsklassifizierungskonzept (z. B. **Public, Internal, Confidential, Strictly Confidential**) einführen und anwenden.	☐	☐
Personal-Security (z. B. NDA, Verpflichtung auf Vertraulichkeit, Schulungen) sicherstellen.	☐	☐
Lieferanten- und Outsourcing-Verträge mit Sicherheitsklauseln (z. B. Auftragsverarbeitungsvertrag, SLA) hinterlegen.	☐	☐
5.4 Compliance	**Umgesetzt**	**Zufrieden**
DSGVO-Anforderungen und branchenspezifische Regelungen (z. B. PCI-DSS, KRITIS) überprüfen, ggf. in Kontrollset integrieren.	☐	☐

6. Schulungen und Awareness		
6.1 Awareness Programm	Umgesetzt	Zufrieden
Mitarbeiterschulungen zu Themen wie **Social Engineering**, **Phishing**, **Passwortrichtlinien** anbieten.	☐	☐
Regelmäßige Sicherheitsupdates (Newsletter, E-Learning, Workshops) veranstalten.	☐	☐
6.2 Rollenspezifische Trainings	**Umgesetzt**	**Zufrieden**
IT-Administratoren, Entwickler, Management und Fachabteilungen erhalten **zielgruppenspezifische** Schulungen (z. B. Secure Coding, Incident Response).	☐	☐
Schulungsnachweise (z. B. Teilnahmelisten, Inhalte) aufbewahren.	☐	☐
6.3 Evaluation der Schulungsmaßnahmen	**Umgesetzt**	**Zufrieden**

Erfolgsmessung über z. B. **Phishing-Tests** oder **Wissensfragen**; Erkenntnisse in den KVP (Kap. 10) einfließen lassen.	☐	☐

7. Betrieb und Incident Management		
7.1 Operative Steuerung	Umgesetzt	Zufrieden
Tägliche oder wöchentliche Kontrollen (z. B. Log-Überwachung, Patch-Prozesse, Backup-Jobs) definieren und dokumentieren.	☐	☐
Eskalationsketten (z. B. wen benachrichtigen bei kritischen Alerts) festlegen.	☐	☐
7.2 Security Incident-Handling	**Umgesetzt**	**Zufrieden**
Incident Response-Konzept erstellen: Schritt-für-Schritt-Ablauf bei einem Sicherheitsvorfall (z. B. Malware, Datendiebstahl).	☐	☐
Forensik- und Reporting-Funktionen (z. B. SIEM) vorhanden und geschult?	☐	☐
7.4 Notfall- und Wiederanlaufpläne	**Umgesetzt**	**Zufrieden**
Business-Continuity-Planung (z. B. Stromausfall, Serverausfall, Klimakatastrophe) mit Verantwortlichkeiten und Workarounds beschreiben.	☐	☐
Wiederherstellungstests (Disaster Recovery-Übungen) durchführen und Ergebnisse dokumentieren.	☐	☐

8. Bewertung der Leistung - interne Audits		
8.1 Auditprogramm	Umgesetzt	Zufrieden
Jahresplan erstellen, welche Bereiche (z. B. IT-Infrastruktur, Abteilungen, Prozesse) wann auditiert werden.	☐	☐
Qualifizierte, möglichst unabhängige **Auditoren** benennen und/oder externe Auditoren.	☐	☐
8.2 Durchführung	**Umgesetzt**	**Zufrieden**
Checklisten erstellen (ggf. basierend auf Controls aus Anhang A), Auditinterviews und Dokumentenprüfungen durchführen.	☐	☐
Auditfeststellungen nach Kritikalität einstufen und dokumentieren.	☐	☐
8.3 Follow-Up	**Umgesetzt**	**Zufrieden**
Abweichungen in einem **Maßnahmenplan** mit Zuständigkeiten, Terminen und Status führen.	☐	☐
Regelmäßiger Bericht an Management, ob Korrekturen wirksam sind.	☐	☐

9. Managementbewertung		
9.1 Review Vorbereitung	Umgesetzt	Zufrieden
Audit-Ergebnisse, Risikoberichte, Vorfallstatistiken, Zielerreichung, neue Anforderungen zusammenfassen.	☐	☐

Zuständige (z. B. IS-Beauftragter, ISB) bereiten Unterlagen auf.	☐	☐
9.2 Review Durchführung (Top Management bespricht:)	Umgesetzt	Zufrieden
Risikolage, interne Auditergebnisse, externe Veränderungen (z. B. gesetzliche Vorgaben), Performance der Controls (siehe Kapitel 9.3).	☐	☐
Klimawandel-Faktoren (ab Nov. 2024).	☐	☐
Protokoll anfertigen, Beschlüsse zu Maßnahmen oder Ressourcen dokumentieren		
9.3 Ergebniskommunikation	Umgesetzt	Zufrieden
Beschlüsse (z. B. neue Ziele, zusätzliche Kontrollen, Toolanschaffungen) an alle Betroffenen kommunizieren.	☐	☐
Umsetzung und Nachverfolgung in **Management-Meetings** sicherstellen.	☐	☐

10. Verbesserung		
10.1 Korrekturmaßnahmen	Umgesetzt	Zufrieden
Nichtkonformitäten (aus internen Audits oder Sicherheitsvorfällen) in ein formales Abweichungsmanagement überführen.	☐	☐
Ursachenanalysen (z. B. 5-Why, Ishikawa) durchführen, Wirksamkeit der Korrekturen überwachen	☐	☐
10.2 Kontinuerliche Verbesserung (KVP)	Umgesetzt	Zufrieden
Lessons Learned-Workshops (z. B. nach Incidents, Testübungen) organisieren.	☐	☐
Erkenntnisse über Fehlersituationen, neue Bedrohungen oder Technologie-Trends in Policies und Prozesse einfließen lassen.	☐	☐
Protokoll anfertigen, Beschlüsse zu Maßnahmen oder Ressourcen dokumentieren		
10.3 Zertifizierungsvorbereitung	Umgesetzt	Zufrieden
Abschluss-Gap-Analyse durchführen: Sind alle Anforderungen (Kap. 4–10 + Anhang A) ausreichend dokumentiert und gelebt?	☐	☐
Prüfen, ob Management und Team für das externe **Zertifizierungsaudit** bereit sind (Fragen, Nachweise, Verantwortlichkeiten).	☐	☐

11. Externes Zertifizierungsaudit		
11.1 Zertifizierungsstelle auswählen	Umgesetzt	Zufrieden
Akkreditierte Zertifizierungsgesellschaft recherchieren (Kosten, Branchenreferenzen, Verfügbarkeit).	☐	☐
Terminplanung (z. B. Stage 1 und Stage 2 Audit) abstimmen.	☐	☐
11.2 Stage 1 (Dokumentenprüfung)	Umgesetzt	Zufrieden

Sicherstellen, dass alle Dokumentationen (Politiken, Risikoanalyse, SoA, Protokolle) verfügbar und aktuell sind.	☐	☐
Falls es Korrekturbedarf gibt, umgehend Maßnahmen einleiten.	☐	☐
11.3 Stage 2 (Systemaudit)	Umgesetzt	Zufrieden
Teammitglieder auf mögliche Auditfragen (Prozessabläufe, Sicherheitsrichtlinien) vorbereiten.	☐	☐
11.4 Abweichungsmanagement	Umgesetzt	Zufrieden
Dokumentation von eventuell festgestellten Non-Conformities (Minor/Major).	☐	☐
Umgehende Korrektur- und Verbesserungspläne erstellen, ggf. Nachaudit-Zeitraum einhalten.	☐	☐
11.5 Zertifikat	Umgesetzt	Zufrieden
Nach Umsetzung aller Non-Conformities (Minor/Major) erhalten Sie ihr Zertifikat. Das Zertifikat ist 3 Jahre gültig.	☐	☐
Die Zertifizierung erfolgt in einem 3-Jahres-Zyklus (Erstzertifizierung, 1. Überwachungsaudit, 2. Überwachungsaudit, RE-Zertifizierung.	☐	☐

So unterstützen wir Sie bei Ihrer ISO-27001-Zertifizierung

Wir begleiten Sie auf dem gesamten Weg zum zertifizierten Informationssicherheitsmanagementsystem. Gemeinsam legen wir den Projektumfang fest, führen eine Gap-Analyse durch und entwickeln passgenaue Maßnahmen zum Schließen erkannter Lücken. Anschließend erstellen wir die erforderliche Dokumentation, bieten Schulungen für Ihr Team an und unterstützen bei internen Audits sowie der finalen Audit-Vorbereitung.

Dank unserer langjährigen Erfahrung im Bereich Informationssicherheit sorgen wir dafür, dass Ihr ISMS technisch und organisatorisch solide aufgestellt ist – für einen reibungslosen Zertifizierungsprozess und nachhaltig gesteigerte Sicherheit in Ihrem Unternehmen.