TrustSpace

ISO 27001 Checkliste

Von der ersten Bestandsaufnahme bis zum Zertifikat: der vollständige Prüfpfad durch die Anforderungen der ISO/IEC 27001:2022 – in acht Phasen, praxisnah für den Mittelstand.

ISO/IEC 27001:2022 | inkl. Amendment 1:2024 | Kapitel 4–10 + Anhang A | Stand: August 2026

UMFANG

8 Phasen

Vom Projektaufsatz bis zum Zertifizierungsaudit, jede Phase mit abhakbaren Prüfpunkten.

ENTHÄLT

Pflichtdokumente

Alle von der Norm geforderten dokumentierten Informationen mit Klauselbezug.

ANHANG A

93 Maßnahmen

Die vier Themenbereiche im Überblick als Grundlage für Ihre Erklärung zur Anwendbarkeit.

FÜR WEN

KMU & Mittelstand

Für ISB, IT-Leitung und Geschäftsführung ohne eigenes Compliance-Team.

So arbeiten Sie mit dieser Checkliste

Die ISO/IEC 27001:2022 verlangt zweierlei: ein funktionierendes Managementsystem (Kapitel 4 bis 10) und die begründete Auswahl konkreter Sicherheitsmaßnahmen (Anhang A). Diese Checkliste folgt genau dieser Logik und führt Sie in acht Phasen durch beide Teile. Arbeiten Sie die Phasen der Reihe nach ab: Jede baut auf dem Ergebnis der vorherigen auf. Offene Punkte am Ende einer Phase sind Ihre Aufgabenliste, nicht ein Grund weiterzugehen.

Kästchen = ein prüfbarer Punkt, den Sie belegen können müssen **Kap.** = zugehörige Normklausel

1	**Projekt aufsetzen: Auftrag, Verantwortung, Ressourcen**	Kap. 5
2	**Kontext verstehen und Anwendungsbereich festlegen**	Kap. 4
3	**Risiken beurteilen und behandeln**	Kap. 6.1, 8.2, 8.3
4	**Maßnahmen auswählen und die Erklärung zur Anwendbarkeit erstellen**	Kap. 6.1.3, Anhang A
5	**Dokumentation und Nachweise aufbauen**	Kap. 7
6	**Maßnahmen im Betrieb umsetzen und wirksam halten**	Kap. 8
7	**Wirksamkeit prüfen: internes Audit und Managementbewertung**	Kap. 9
8	**Abweichungen schließen und Zertifizierungsaudit bestehen**	Kap. 10

Was diese Checkliste nicht ersetzt

Sie ersetzt weder den Normtext noch die Prüfung durch eine akkreditierte Zertifizierungsstelle. Der verbindliche Wortlaut der Anforderungen steht ausschließlich in der ISO/IEC 27001:2022 samt Amendment 1:2024; die Umsetzungsanleitung zu den Maßnahmen des Anhangs A liefert die begleitende ISO/IEC 27002:2022.

1 Projekt aufsetzen: Auftrag, Verantwortung, Ressourcen

Kapitel 5 – Führung

Ohne getragene Entscheidung der Leitung scheitert jedes ISMS an fehlender Zeit und fehlenden Befugnissen. Diese Phase schafft die formalen Voraussetzungen, bevor inhaltlich gearbeitet wird.

- [ ] **Ziel und Anlass sind schriftlich festgehalten** – Kundenanforderung, Ausschreibung, gesetzliche Pflicht oder Eigenmotivation.
- [ ] **Die oberste Leitung hat die Verantwortung übernommen** – nachweisbar, nicht nur mündlich (Kap. 5.1).
- [ ] **Eine Informationssicherheitspolitik ist verabschiedet und kommuniziert** – sie gibt den Rahmen vor und ist ein Pflichtdokument (Kap. 5.2).
- [ ] **Rollen, Verantwortlichkeiten und Befugnisse sind zugewiesen** – insbesondere die Rolle des Informationssicherheitsbeauftragten (Kap. 5.3).
- [ ] **Budget, Personal und Zeitrahmen sind freigegeben** – realistisch geplant, inklusive Auditkosten.
- [ ] **Ein Projektplan mit Meilensteinen liegt vor** – erfahrungsgemäß dauert der Weg zum Zertifikat sechs bis zwölf Monate.

2 Kontext verstehen und Anwendungsbereich festlegen

Kapitel 4 – Kontext der Organisation

Der Anwendungsbereich entscheidet darüber, was später geprüft wird. Er zu weit gefasst überfordert das Projekt, zu eng gefasst entwertet das Zertifikat gegenüber Kunden.

- [ ] **Interne und externe Themen sind ermittelt** – Geschäftsmodell, Technologie, Regulierung, Marktumfeld (Kap. 4.1).
- [ ] **Die Relevanz des Klimawandels ist bewertet und dokumentiert** – seit Amendment 1:2024 ausdrücklich gefordert; auch ein begründetes „nicht relevant“ ist ein zulässiges Ergebnis.
- [ ] **Interessierte Parteien und ihre Anforderungen sind erfasst** – Kunden, Aufsicht, Mitarbeitende, Dienstleister (Kap. 4.2).
- [ ] **Der Anwendungsbereich ist schriftlich abgegrenzt** – Standorte, Organisationseinheiten, Prozesse, Systeme; Ausschlüsse sind begründet (Kap. 4.3).
- [ ] **Schnittstellen und Abhängigkeiten nach außen sind beschrieben** – insbesondere ausgelagerte IT und Cloud-Dienste.
- [ ] **Die ISMS-Prozesse und ihr Zusammenspiel sind festgelegt** – Kap. 4.4.

> **Praxishinweis zum Scope**
>
> Formulieren Sie den Anwendungsbereich so, dass ein Kunde ihn ohne Rückfrage versteht. Ein Zertifikat, dessen Geltungsbereich nur eine Abteilung umfasst, während der Kunde das ganze Unternehmen erwartet, führt in Lieferantenaudits regelmäßig zu Nachfragen.

3 Risiken beurteilen und behandeln

Kapitel 6.1 sowie 8.2 und 8.3 – Planung und Betrieb

Die Risikobeurteilung ist das Herzstück der Norm: Aus ihr leitet sich ab, welche Maßnahmen Sie brauchen und welche nicht. Auditoren prüfen hier besonders genau, ob Methode und Ergebnis zusammenpassen.

- [ ] **Eine Methode zur Risikobeurteilung ist festgelegt und dokumentiert** – inklusive Kriterien für Akzeptanz und Bewertung, damit Wiederholungen vergleichbar bleiben (Kap. 6.1.2).
- [ ] **Werte und Assets im Anwendungsbereich sind erfasst** – Informationen, Systeme, Dienstleister, Standorte.
- [ ] **Risiken sind identifiziert, analysiert und bewertet** – mit Eintrittswahrscheinlichkeit und Auswirkung.
- [ ] **Für jedes Risiko ist eine Behandlungsoption gewählt** – vermeiden, vermindern, übertragen oder bewusst akzeptieren (Kap. 6.1.3).
- [ ] **Ein Risikobehandlungsplan liegt vor** – mit Maßnahme, verantwortlicher Person, Frist und Status.
- [ ] **Die Risikoeigner haben Plan und Restrisiken freigegeben** – formale Freigabe, nicht stillschweigende Kenntnisnahme.
- [ ] **Die Ergebnisse von Beurteilung und Behandlung sind aufbewahrt** – als Nachweis gefordert (Kap. 8.2 und 8.3).
- [ ] **Informationssicherheitsziele sind messbar formuliert** – mit Verantwortlichen, Ressourcen und Terminen (Kap. 6.2).

4 Maßnahmen auswählen und die Erklärung zur Anwendbarkeit erstellen

Kapitel 6.1.3 d) – Anhang A

Die Erklärung zur Anwendbarkeit (Statement of Applicability, SoA) ist das meistgelesene Dokument im Audit. Sie verbindet Ihre Risiken mit den 93 Maßnahmen des Anhangs A.

- [ ] **Alle 93 Maßnahmen des Anhangs A sind geprüft** – keine darf unbeachtet bleiben.
- [ ] **Für jede Maßnahme ist entschieden: anwendbar oder nicht** – jeder Ausschluss ist nachvollziehbar begründet.
- [ ] **Der Umsetzungsstand je Maßnahme ist vermerkt** – umgesetzt, teilweise umgesetzt, geplant.
- [ ] **Jede anwendbare Maßnahme ist auf ein Risiko oder eine Anforderung zurückführbar**
- [ ] **Die SoA ist versioniert und freigegeben** – sie wird bei jeder Änderung des ISMS mitgeführt.

Anhang A: 93 Maßnahmen in vier Themenbereichen

Die Fassung 2022 hat die zuvor 114 Maßnahmen zu 93 zusammengeführt und in vier Themenbereiche neu geordnet. Elf Maßnahmen sind vollständig neu hinzugekommen, unter anderem zu Bedrohungsaufklärung, Cloud-Diensten, Datenmaskierung und Überwachungsaktivitäten. Nutzen Sie diese Übersicht, um Ihre Erklärung zur Anwendbarkeit zu strukturieren.

A.5

Organisatorische Maßnahmen — 37

Richtlinien, Rollen, Lieferantenbeziehungen, Umgang mit Sicherheitsvorfällen, Kontinuität, rechtliche Anforderungen und Klassifizierung von Informationen.

A.6

Personenbezogene Maßnahmen — 8

Eignungsprüfung vor der Einstellung, Vertragsbedingungen, Sensibilisierung und Schulung, Disziplinarverfahren, Regelungen für mobiles Arbeiten.

A.7

Physische Maßnahmen — 14

Sicherheitsbereiche, Zutrittskontrolle, Schutz vor Umgebungseinflüssen, Verkabelung, sichere Entsorgung von Datenträgern, aufgeräumter Arbeitsplatz.

A.8

Technologische Maßnahmen — 34

Zugriffsrechte, Kryptografie, Härtung, Protokollierung und Überwachung, Schutz vor Schadsoftware, Handhabung technischer Schwachstellen, sichere Entwicklung.

Prüfpunkte zur Maßnahmenauswahl

- [ ] **Neue Maßnahmen der Fassung 2022 sind bewertet** – insbesondere Bedrohungsaufklärung, Informationssicherheit für Cloud-Dienste, Bereitschaft für Kontinuität, Überwachungsaktivitäten, Datenmaskierung, Verhinderung von Datenabfluss, Löschung von Informationen, Konfigurationsmanagement, Web-Filterung, sichere Programmierung.
- [ ] **Für Maßnahmen aus Anhang A ist die Umsetzungsanleitung der ISO/IEC 27002:2022 herangezogen**
- [ ] **Jede umgesetzte Maßnahme hat einen belegbaren Nachweis** – Richtlinie, Konfiguration, Protokoll, Schulungsnachweis oder Vertragsklausel.
- [ ] **Ausgelagerte Leistungen sind über Verträge abgesichert** – Anforderungen an Dienstleister sind vereinbart und werden überwacht.

5 Dokumentation und Nachweise aufbauen

Kapitel 7 – Unterstützung

Die Norm verlangt eine überschaubare Zahl dokumentierter Informationen. Alles Weitere ergänzen Sie nur, wenn Ihre Organisation es tatsächlich braucht. Prüfen Sie jede Zeile: Existiert das Dokument, ist es aktuell, ist es freigegeben?

	Kapitel	Dokumentierte Information
☐	4.3	Anwendungsbereich des ISMS
☐	5.2	Informationssicherheitspolitik
☐	6.1.2	Prozess der Informationssicherheitsrisikobeurteilung
☐	6.1.3	Prozess der Informationssicherheitsrisikobehandlung
☐	6.1.3 d)	Erklärung zur Anwendbarkeit (Statement of Applicability)
☐	6.2	Informationssicherheitsziele
☐	7.2	Nachweise über Kompetenz und Schulung
☐	7.5	Lenkung dokumentierter Informationen (Version, Freigabe, Verfügbarkeit, Schutz)
☐	8.1	Nachweise, dass die Prozesse wie geplant durchgeführt wurden
☐	8.2	Ergebnisse der Risikobeurteilungen
☐	8.3	Ergebnisse der Risikobehandlung
☐	9.1	Nachweise über Überwachung, Messung, Analyse und Bewertung
☐	9.2	Auditprogramm und Ergebnisse der internen Audits
☐	9.3	Ergebnisse der Managementbewertung
☐	10.2	Nichtkonformitäten, Korrekturmaßnahmen und deren Ergebnisse

Ergänzend prüfen Sie die weiteren Anforderungen aus Kapitel 7:

- ☐ **Erforderliche Ressourcen sind bereitgestellt** – Kap. 7.1.
- ☐ **Kompetenzanforderungen je Rolle sind definiert und erfüllt** – Kap. 7.2.
- ☐ **Mitarbeitende sind sensibilisiert und kennen ihren Beitrag** – Kap. 7.3, nachweisbar über Schulungen.
- ☐ **Interne und externe Kommunikation ist geregelt** – was, wann, an wen, durch wen (Kap. 7.4).

6 Maßnahmen im Betrieb umsetzen und wirksam halten

Kapitel 8 – Betrieb

- [ ] **Die geplanten Prozesse laufen im Alltag und werden gesteuert** – Kap. 8.1.
- [ ] **Geplante Änderungen werden gesteuert, ungeplante bewertet** – mit Rückfalloption.
- [ ] **Ausgelagerte Prozesse sind bestimmt und werden überwacht**
- [ ] **Die Risikobeurteilung wird in festgelegten Abständen wiederholt** – und zusätzlich bei wesentlichen Änderungen (Kap. 8.2).
- [ ] **Der Risikobehandlungsplan wird nachgehalten** – offene Maßnahmen haben Termin und Verantwortliche (Kap. 8.3).

7 Wirksamkeit prüfen: internes Audit und Managementbewertung

Kapitel 9 – Bewertung der Leistung

- [ ] **Es ist festgelegt, was überwacht und gemessen wird** – mit Methode, Zeitpunkt und Zuständigkeit (Kap. 9.1).
- [ ] **Ein internes Auditprogramm existiert und wurde durchgeführt** – alle Normkapitel und anwendbaren Maßnahmen sind über den Zyklus abgedeckt (Kap. 9.2).
- [ ] **Die internen Auditoren sind unabhängig vom geprüften Bereich**
- [ ] **Auditergebnisse sind dokumentiert und an die Leitung berichtet**
- [ ] **Die Managementbewertung hat stattgefunden** – mit allen von Kap. 9.3 geforderten Eingangsgrößen und dokumentierten Ergebnissen.

8 Abweichungen schließen und Zertifizierungsaudit bestehen

Kapitel 10 – Verbesserung

- [ ] **Nichtkonformitäten sind erfasst, ursachenbezogen analysiert und behoben** – mit dokumentiertem Ergebnis (Kap. 10.2).
- [ ] **Die fortlaufende Verbesserung ist belegbar** – Kap. 10.1.
- [ ] **Eine akkreditierte Zertifizierungsstelle ist ausgewählt und beauftragt**
- [ ] **Stufe 1 (Dokumentenprüfung) ist bestanden** – Feststellungen daraus sind vor Stufe 2 abgearbeitet.
- [ ] **Stufe 2 (Umsetzungsprüfung vor Ort) ist terminiert und vorbereitet** – Ansprechpartner, Nachweise und Zugänge stehen bereit.
- [ ] **Der Folgezyklus ist eingeplant** – das Zertifikat gilt drei Jahre, in den beiden Folgejahren stehen Überwachungsaudits an, danach die Rezertifizierung.

Fünf Stolpersteine, die Zertifizierungen verzögern

Diese Punkte tauchen in Erstaudits im Mittelstand immer wieder auf. Wer sie früh adressiert, spart sich Nachaudits und Korrekturschleifen.

01 Der Anwendungsbereich wird nachträglich verändert

Wird der Scope erst im Projektverlauf erweitert, müssen Risikobeurteilung, Erklärung zur Anwendbarkeit und interne Audits nachgezogen werden. Legen Sie ihn früh fest und begründen Sie Ausschlüsse sauber.

02 Die Erklärung zur Anwendbarkeit passt nicht zur Risikobeurteilung

Maßnahmen ohne zugehöriges Risiko und Risiken ohne zugehörige Maßnahme sind die häufigste Feststellung. Beide Dokumente müssen sich gegenseitig erklären.

03 Nachweise existieren nur als Absichtserklärung

Eine Richtlinie belegt nicht, dass danach gehandelt wird. Der Auditor sucht Protokolle, Tickets, Freigaben und Schulungsnachweise aus dem laufenden Betrieb.

04 Das interne Audit wird zur Formalie

Ein internes Audit ohne Feststellungen ist ein Warnsignal, kein gutes Zeichen. Es soll Lücken finden, solange sie intern korrigierbar sind.

05 Nach dem Zertifikat schläft das System ein

Überwachungsaudits prüfen den laufenden Betrieb. Wiederkehrende Risikobeurteilung, Managementbewertung und Maßnahmenverfolgung müssen im Kalender stehen, nicht im Projektplan.

Von der Checkliste zum belegbaren ISMS

TrustSpace verbindet Software und Beratung: In TrustSpaceOS hängen Assets, Risiken, Maßnahmen und Nachweise zusammen, Aufgaben haben Verantwortliche und Fristen, und die Erklärung zur Anwendbarkeit entsteht aus den gepflegten Daten statt aus einer separaten Tabelle. Unsere Beraterinnen und Berater begleiten Sie bis ins Zertifizierungsaudit.

Zur ISO 27001-Beratung trustspace.io/isms-software