Die Selbstprüfung vor Stufe 1

Ist das System prüfbar? Sechs Bereiche in der Reihenfolge, in der die erste Stufe sie ansieht, der Ordner, der den Tag in drei Stunden erledigt, und zwei Kennzahlen für die Managementbewertung.

Kategorie: Prüf-Checkliste. Bezug im Buch: Abschnitt 4.3 (Das Prinzip, Regeln eins bis sieben; Was die Norm sagt); Norm: Klauseln 4.3, 5.2, 6.1.2, 6.1.3, 7.5.2, 7.5.3, 9.2 und 9.3 sowie Anhang A (93 Maßnahmen) der ISO/IEC 27001:2022 mit Änderung 1:2024 und ISO/IEC 17021-1 mit ISO/IEC 27006-1, in den eigenen Worten des Buches. Rechtsstand des Bandes: 28. September 2026.

Haus / Standort		**Ausgefüllt von**	
Stichtag		**Termin Stufe 1**	
Geplante Stufe 2		**Land (DE / AT / CH)**	

So nutzen Sie diese Vorlage

1. Beginnen Sie wie der Auditor mit der Erklärung zur Anwendbarkeit: Versionsnummer und Freigabevermerk prüfen, die Spalte der Begründungen auf Wiederholungen durchsehen (Abschnitt 3).
2. Gehen Sie die Bereiche 1 bis 7 der Reihe nach durch. Jede Antwort «nein» oder «weiß nicht» ist ein Punkt für die Liste, die vor der zweiten Stufe abzuarbeiten ist.
3. Lassen Sie die Erklärung zeilenweise von den Personen beantworten, die die Maßnahme betrifft: Zutritt die Haustechnik, Personal die Personalabteilung, Lieferanten der Einkauf, Gastdaten der Empfang.
4. Lassen Sie die vier zentralen Dokumente freigeben (ein Vormittag), legen Sie internes Audit und Managementbewertung vor die zweite Stufe und stellen Sie den Ordner zusammen (Abschnitt 6).
5. Tragen Sie die beiden Kennzahlen ein und legen Sie sie der nächsten Managementbewertung vor; im Wiener Fall wird die Erklärung seither jedes Jahr im Frühjahr zeilenweise mit denselben Abteilungen durchgegangen.
6. Schönen Sie nichts: Die erste Stufe ist das einzige Audit, an dem man kostenlos scheitern kann; sie endet nicht mit Abweichungen, sondern mit Punkten, die vor der zweiten Stufe zu erledigen sind.

Spalte «Im Buch»: verlangt = von der Norm oder dem Regelwerk verlangt, wie der Band es in eigenen Worten wiedergibt (Klausel in Klammern); Methode dieses Bandes = Vorgehen des Bandes, keine Anforderung. Die erste Stufe prüft nicht, ob ein Haus sicher ist, sondern ob es etwas gibt, das man prüfen kann.

1 Der Anwendungsbereich

Frage	Antwort	Grund (aus dem Band)	Im Buch
Nennt der Anwendungsbereich alle Standorte (auch Nebenhaus, Verwaltungsbüro, Reservierungszentrale), die Tätigkeiten und die Schnittstellen zu ausgelagerten Funktionen, und nennt er sie vollständig?		Ein Anwendungsbereich, der die Orte verschweigt, an denen die Daten tatsächlich verarbeitet werden, ist kein enger Anwendungsbereich, sondern ein unrichtiger.	verlangt (Klausel 4.3: Schnittstellen und Abhängigkeiten zu Tätigkeiten anderer Organisationen); Vollständigkeit der Aufzählung: Methode
Ist der Anwendungsbereich jetzt richtig geschrieben, am Anfang, solange es nichts kostet?		Eine Erweiterung nach der Zertifizierung ist ein eigenes Verfahren mit eigenen Auditortagen; eine Berichtigung kann die Stelle veranlassen, über das Zertifikat zu entscheiden, bis hin zur Aussetzung.	Methode dieses Bandes

2 Die Risikobeurteilung

Frage	Antwort	Grund (aus dem Band)	Im Buch
Gibt es ein festgelegtes, wiederholbares Verfahren der Risikobeurteilung, und wurde die Beurteilung vor der Erklärung zur Anwendbarkeit durchgeführt?		Die Erklärung zur Anwendbarkeit ist das Ergebnis der Risikobeurteilung und nicht ihr Ersatz; die Umkehrung der Reihenfolge ist im Dokument sichtbar.	verlangt (Klausel 6.1.2)
Finden sich die Ergebnisse der Risikobeurteilung in der Erklärung zur Anwendbarkeit wieder?		Die Wiener Risikobeurteilung war gründlich gemacht und dann nicht benutzt worden: einer von sieben Punkten.	verlangt (Klauseln 6.1.2 und 6.1.3)
Lässt sich jede einbezogene Maßnahme auf die Risikobeurteilung zurückführen, und taucht jedes wesentliche Risiko in mindestens einer Maßnahme auf?		Zwei Sorten von Fehlern: Maßnahmen ohne Risiko, die aus der Vorlage stammen, und Risiken ohne Maßnahme, die aus der Wirklichkeit stammen; die zweite Sorte ist die wertvolle.	Methode dieses Bandes

3 Die Erklärung zur Anwendbarkeit

Frage	Antwort	Grund (aus dem Band)	Im Buch
Führt die Erklärung je Maßnahme die erforderliche Maßnahme, die Begründung der Einbeziehung, den Umsetzungsstand und, wo ausgeschlossen, die Begründung des Ausschlusses an?		Die Norm verlangt vier Angaben; das Wiener Dokument hatte eine.	verlangt (Klausel 6.1.3)

Frage	Antwort	Grund (aus dem Band)	Im Buch
Hat sie eine fünfte Spalte mit der Fundstelle des Nachweises (Verfahren, Aufzeichnung, Vertrag, Konfiguration)?		Die fünfte Spalte kostet beim Erstellen die meiste Zeit und spart in jedem Audit die meiste.	Methode dieses Bandes
Ist jede Begründung in eigenen Worten für diese Maßnahme geschrieben, ohne denselben Satz in mehreren Zeilen?		Eine Begründung, die für dreiundneunzig verschiedene Maßnahmen wörtlich passt, passt für keine.	Begründung: verlangt (Klausel 6.1.3); eigene Worte: Methode
Hat jede Zeile die Person beantwortet, die die Maßnahme betrifft, und nicht eine einzelne Person allein?		Eine Erklärung, die eine einzelne Person allein ausfüllt, beschreibt notwendigerweise das Wissen dieser Person.	Methode dieses Bandes
Ist jeder Ausschluss, wo eine Maßnahme nicht zutrifft, mit einem Satz begründet? Ist «machen wir nicht selbst» als Auslagerung geführt (Maßnahme bleibt anwendbar, Nachweis im Vertrag und in der Überwachung des Dienstleisters)?		Ausschlüsse sind vorgesehen und aussagekräftig; erwartet wird die Begründung, nicht eine bestimmte Zahl.	Begründung des Ausschlusses: verlangt (Klausel 6.1.3); Unterscheidung: Methode
Sind die mit Anhang A (Fassung 2022) neu aufgenommenen Maßnahmen (Erkenntnisse über Bedrohungen, Dienste aus der Cloud, Bereitschaft der Informations- und Kommunikationstechnik für die Betriebsfortführung) wirklich geprüft, bevor «umgesetzt» eingetragen wurde?		Bei diesen neuen Maßnahmen tragen Häuser erfahrungsgemäß «umgesetzt» ein, ohne es je geprüft zu haben.	Anhang A (Fassung 2022); Frage: Methode
Kennen die Menschen am Empfang, im Etagendienst und in der Haustechnik die Verfahren, die als Fundstelle genannt sind?		Die Erklärung in Baden war richtig, und das Haus kannte sie nicht; die erste Stufe prüft die Prüfbarkeit, nicht die Wirklichkeit.	Methode dieses Bandes (Gegenfall; weiter in Abschnitt 4.4)
Wer erhält die Erklärung? Gibt das Haus nach außen nur die Spalten Maßnahme, anwendbar und Umsetzungsstand weiter?		Das Dokument ist eine Landkarte der Lücken des Hauses; es gehört nicht auf die Webseite und nicht ungeschwärzt in jede Ausschreibung.	Methode dieses Bandes

4 Die Freigabe der vier zentralen Dokumente

Frage	Antwort	Grund (aus dem Band)	Im Buch
Trägt jedes der vier Dokumente einen nachvollziehbaren Freigabestatus: Version ab eins, Datum, benannte Verantwortliche, Genehmigung durch die Leitung?		Entscheidend ist nicht die Nummer, sondern der Freigabestatus; dieser Fehler war in zehn Minuten zu beheben gewesen.	verlangt (Klauseln 5.2, 7.5.2, 7.5.3: Kennzeichnung, Genehmigung, Versionskontrolle); Form der Genehmigung: Methode

Dokument	Version	Datum der Freigabe	Verantwortliche/r	Genehmigt durch (Leitung)
Anwendungsbereich				
Leitlinie (Informationssicherheitspolitik)				
Risikobeurteilung				
Erklärung zur Anwendbarkeit				

5 Internes Audit und Managementbewertung

Frage	Antwort	Grund (aus dem Band)	Im Buch
Hat das interne Audit stattgefunden, und liegt sein Bericht vor? (Datum eintragen)		Ein System, das noch nie selbst geprüft wurde, hat keinen Nachweis dafür, dass es betrieben wird.	verlangt (Klausel 9.2)
Hat die Managementbewertung stattgefunden, und liegt ihr Protokoll vor? (Datum eintragen)		Die Stelle bewertet schon in der ersten Stufe, ob beide geplant und durchgeführt werden; sie sind keine späteren Pflichten.	verlangt (Klausel 9.3)
Liegen beide vor der zweiten Stufe und nicht nach ihr?		Wo beide für September nach der zweiten Stufe vorgesehen waren, fehlten genau die beiden Nachweise, ohne die ein System nicht als betriebsbereit gilt.	Methode dieses Bandes

6 Der Ordner für den Tag

	Unterlage	Ablageort (Ordner oder Verzeichnis)	Im Buch
☐	Anwendungsbereich		Methode dieses Bandes
☐	Leitlinie		Methode dieses Bandes
☐	Risikobeurteilung		Methode dieses Bandes
☐	Erklärung zur Anwendbarkeit		Methode dieses Bandes
☐	Verzeichnis der dokumentierten Information		Methode dieses Bandes
☐	Bericht des internen Audits		Methode dieses Bandes

	Unterlage	Ablageort (Ordner oder Verzeichnis)	Im Buch
☐	Protokoll der Managementbewertung		Methode dieses Bandes

Grund: Ein Ordner, digital oder auf dem Tisch, mit diesen Unterlagen deckt den größten Teil des Tages ab; Häuser mit Ordner erleben eine erste Stufe von drei Stunden, Häuser, die suchen, einen langen Tag mit wenig Ertrag (Regel sieben).

7 Termin, Abstand und Kennzahlen

Frage	Antwort	Grund (aus dem Band)	Im Buch
Ist die erste Stufe als Dokumententermin vorbereitet und nicht als «Vorbesprechung» in den Kalender gestellt?		Die Verwechslung der ersten Stufe mit einem Vorgespräch ist der siebte Fehler des Abschnitts.	Methode dieses Bandes
Ist der Termin der zweiten Stufe aus dem Stand des Systems abgeleitet und nicht aus einer Frist von außen, etwa einer Ausschreibung?		In Wien kam zuerst der Termin und dann das System; ein Managementsystem lässt sich nicht dazu drängen, gewirkt zu haben.	Methode dieses Bandes
Liegt zwischen den Stufen ein angemessener Abstand, und sind die Ergebnisse der ersten Stufe bei der zweiten noch gültig?		Wird der Abstand zu groß, muss die erste Stufe teilweise wiederholt werden; wer ein Jahr verstreichen lässt, bezahlt sie zweimal.	verlangt (ISO/IEC 17021-1 in Verbindung mit ISO/IEC 27006-1)
Kennzahl 1: Wie viele Zeilen der Erklärung zur Anwendbarkeit haben keine Fundstelle?		Beide Kennzahlen gehören in die nächste Managementbewertung.	Methode dieses Bandes
Kennzahl 2: Wie viele einbezogene Maßnahmen haben kein zugehöriges Risiko?		Maßnahmen ohne Risiko stammen aus der Vorlage und nicht aus dem Haus.	Methode dieses Bandes

8 Häufige Fehler laut Abschnitt

Fehler	Was der Abschnitt dazu sagt
Die Erklärung als Liste statt als Entscheidungsdokument	Sie ist das Protokoll der Entscheidungen eines Hauses; wer sie aus einer Vorlage übernimmt, übernimmt die Entscheidungen eines fremden Hauses. Die Vorlage soll als Fragenkatalog dienen, nicht als Antwort.
Die Angst vor dem Ausschluss	«Nichts ausschließen, das sieht schlecht aus» ist der verbreitetste Satz und der falscheste; ohne Begründung sind dreiundneunzig Ja dreiundneunzig offene Nachweispflichten.
Die immer gleiche Begründung	Sie ist der sicherste Hinweis darauf, dass die Spalte ausgefüllt und nicht gedacht wurde.
Der Umsetzungsstand ohne Fundstelle	«Umgesetzt» ist eine Behauptung; «umgesetzt, siehe Verfahren E-04 und Schulungsnachweis vom 12. März» ist ein Nachweis.
Die fehlende Freigabe	Eine Fassung unter eins legt den Verdacht Entwurf nahe, entscheidend ist der Freigabestatus; die Wiener Leitlinie lag ebenfalls als Entwurf vor.
Der unrichtige Anwendungsbereich	«Hotelbetrieb, Standort Wien» ohne Dependance, Verwaltungsbüro, Reservierungszentrale und die beiden ausgelagerten Funktionen: der teuerste Fehler des Abschnitts.
Die erste Stufe als Vorgespräch	Internes Audit und Managementbewertung waren für nach der zweiten Stufe vorgesehen; damit fehlten die beiden Nachweise der Betriebsbereitschaft.

Rahmen laut Buch: Die Erklärung zur Anwendbarkeit ist ein Norm-Dokument und kein Rechtsdokument; gegenüber Aufsichtsbehörden zeigt sie die Abwägung geeigneter technischer und organisatorischer Maßnahmen (Rechenschaftspflicht und Sicherheit der Verarbeitung nach der Datenschutz-Grundverordnung; Österreich: Datenschutzgesetz; Deutschland: Bundesdatenschutzgesetz; Schweiz: revidiertes Datenschutzgesetz mit Verordnung). Das zweistufige Verfahren und der Abstand zwischen den Stufen folgen ISO/IEC 17021-1 in Verbindung mit ISO/IEC 27006-1. Rechtsstand des Bandes: 28. September 2026.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch die Regelwerke der Zertifizierung. Sie ist keine Probe der ersten Stufe und keine Zusage der Zertifizierungsstelle: Was die Stelle in der ersten Stufe bewertet und welchen Abstand zur zweiten sie verlangt, bestimmt sie nach ihren Regeln und ihrem Vertrag. Die Selbstprüfung prüft die Prüfbarkeit, nicht die Wirklichkeit; ein ausgefülltes Blatt ist kein Nachweis, sondern zeigt, dass jemand nachgesehen hat.