Die Erklärung zur Anwendbarkeit, die ein Haus verteidigen kann

Die Entscheidung je Referenzmaßnahme mit ihrem Grund, die Zeilen aus Kassel und die Probe, die eine Auditorin anlegt, die von der ersten Zeile bis zur letzten liest.

Kategorie: Vorlage. Bezug im Buch: Abschnitt 1.9 (Leitfrage, Tabellen 1, 2, 3 und 4; als Register auch in der Excel-Datei zu Abschnitt 1.9); Norm: Klauseln 6.1.3, 8.2 und 8.3 der ISO/IEC 27001:2022 mit Änderung 1:2024 mit den dreiundneunzig Referenzmaßnahmen des Anhangs A, in den eigenen Worten des Bandes. Rechtsstand des Bandes: 27. September 2026.

Haus		**Stand der Erklärung (Datum)**	
Gebaut von (Risikoeigentümer, Systemverantwortliche)		**Unterschrieben von (befugt, den Betrieb zu verpflichten)**	

So nutzen Sie diese Vorlage

1. Lesen Sie zuerst nur die Gründe der ausgeschlossenen Maßnahmen (Teil 1). Könnte einer davon nicht von jemandem geschrieben sein, der durch Ihr Hotel gegangen ist, beschreibt das Dokument, das Ihre Eigentümerschaft unterschrieben hat, einen anderen Betrieb.
2. Beantworten Sie die acht Fragen (Teil 2) für jede Referenzmaßnahme in dieser Reihenfolge und tragen Sie die Antworten in das Register in Excel ein (dreiundneunzig Zeilen). Die Logik läuft vorwärts: von den Risiken und Pflichten des Hauses zur Maßnahme, dann der Abgleich mit der Liste, nicht ein Abhaken der Liste.
3. Die Zeilen aus Kassel (Teil 3) zeigen, was im Haus war, als die Erklärung ein Lager beschrieb. Sie sind Beispiel, keine Vorlage für Ihre Gründe.

Spalte «Im Buch»: verlangt = von der Norm verlangt, wie der Band sie in eigenen Worten wiedergibt (Klausel in Klammern); Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Die Probe der Leitfrage: nur die Gründe der Ausschlüsse lesen

Ausgeschlossene Referenzmaßnahmen (Anzahl)		**Gründe, die nur «nicht anwendbar» sagen oder allgemein bleiben**	
Gründe, die einen anderen Betrieb beschreiben		**Gründe, die schlicht falsch sind**	

«Nicht anwendbar» ist kein Grund, es ist ein Schluss; die Norm verlangt den Grund dahinter. Eine Begründung, die im Haus niemand hätte schreiben können, weil sie Räume beschreibt, die das Haus nicht hat, ist schlimmer als keine (Kassel: allgemeine, fremde und drei falsche Gründe). **Methode** dieses Bandes: das Zählen; **verlangt** ist der Grund für den Ausschluss (6.1.3 d).

2 Die acht Fragen, je Referenzmaßnahme in dieser Reihenfolge

Nr.	Frage	Grund (aus dem Band)	Im Buch	Eintrag
1	Aus welchem Risikoszenario oder welcher Pflicht des Hauses folgt die Maßnahme?	Die Erklärung ist das Ergebnis der eigenen Risikobehandlung des Hauses; die Referenzliste kommt danach, zum Abgleich.	**verlangt:** Maßnahmen aus der Risikobehandlung bestimmt (6.1.3 b); jede einbezogene Maßnahme lässt sich zurückführen.	☐ erledigt _____
2	Ist jede der dreiundneunzig Referenzmaßnahmen geprüft, mit Ergebnis?	Der Abgleich sorgt dafür, dass nichts Nötiges übersehen wird; die Liste ist nicht einzeln verpflichtend und keine Checkliste zum Abhaken.	**verlangt:** Abgleich mit der Referenzliste (6.1.3 c). Ein förmlicher Gap-Analyse-Bericht ist nicht verlangt.	☐ erledigt _____
3	Warum ist die Maßnahme einbezogen, in den Worten des Hauses?	Ein Grund nennt ein Risiko, ein Gesetz oder einen Kundenvertrag; eine Standardformel sagt nichts über dieses Haus.	**verlangt:** Begründung der Einbeziehung (6.1.3 d). Eine Standardformel je Maßnahme ist nicht verlangt.	☐ erledigt _____
4	Ist sie umgesetzt: ja, teilweise oder geplant mit Datum? Welcher Nachweis steht hinter jedem Ja?	Bei etwa einem Fünftel der einbezogenen Maßnahmen stand Ja, wo die ehrliche Antwort «teilweise» oder «noch nicht» gewesen wäre; umgesetzt heißt: sie wirkt.	**verlangt:** Stand der Umsetzung (6.1.3 d). Ein Reifegradwert je Maßnahme ist nicht verlangt.	☐ erledigt _____
5	Warum ist die Maßnahme ausgeschlossen, mit einem Grund, den nur schreiben konnte, wer das Haus kennt?	Ein Ausschluss, weil die Maßnahme schwierig wirkt, ist keiner; ein Grund muss das Haus beschreiben, keinen anderen Betrieb.	**verlangt:** Begründung des Ausschlusses (6.1.3 d). Eine Ausschlussrichtlinie ist nicht verlangt.	☐ erledigt _____
6	Welche guten Gewohnheiten des Hauses stehen nicht auf der Liste und sind trotzdem Maßnahmen?	Ein Haus, das nicht erklärt, was es gut macht, hört irgendwann damit auf, wenn das Personal wechselt.	**verlangt:** weitere Maßnahmen, wo nötig; die Referenzliste ist nicht abschließend (6.1.3). Die vollständige Abbildung eines anderen Rahmenwerks ist nicht verlangt.	☐ erledigt _____
7	Wer hat die Erklärung gebaut, und wer hat sie nach der Lektüre unterschrieben?	Sie wird von den Risikoeigentümern und der Person, der das System gehört, gemeinsam gebaut und von jemandem unterschrieben, der befugt ist, den Betrieb zu verpflichten, weil sie genau das tut.	**verlangt:** Die Risikoeigentümer genehmigen den Behandlungsplan (6.1.3). **Methode:** wer baut, wer unterschreibt.	☐ erledigt _____

Nr.	Frage	Grund (aus dem Band)	Im Buch	Eintrag
8	Was hat sich seit der letzten Fassung bei Systemen, Lieferanten oder Abläufen geändert, und hat jemand die Erklärung dazu wieder geöffnet?	Das Verwaltungssystem zog zu einem gehosteten Dienst, eine Check-in-App kam hinzu, das Spa übernahm eine Buchungsplattform: Keine Änderung veranlasste jemanden, die Erklärung zu öffnen.	**verlangt:** Die Erklärung muss die heute nötigen Maßnahmen widerspiegeln (8.2, 8.3).	☐ erledigt _____

Die Logik der Fragen ist die der Norm (Tabelle 2 des Bandes): Ausgangspunkt sind die Risikoszenarien und Pflichten des Hauses, nicht die Liste; Ausschlüsse sind, was das Haus nachweislich nicht braucht, nicht, was schwierig wirkt; eigene Maßnahmen werden erklärt und geführt.

3 Die Zeilen aus Kassel: dieselbe Referenzmaßnahme, einmal falsch, einmal mit Grund

Beispiel aus Abschnitt 1.9 (Tabelle 1; Kassel, 210 Zimmer, Rezertifizierung): Die Erklärung war aus der eines Logistikunternehmens gebaut worden. Rechts steht, was ein Grund aus dem Haus selbst gesagt hätte.

Referenzmaßnahme	Was die Erklärung sagte	Was im Haus war	Entscheidung mit Grund aus dem Haus
Überwachung der physischen Sicherheit (A 7.4)	nicht anwendbar: Zutritt zum Lager nur für Logistikpersonal	Kameras in allen öffentlichen Bereichen, Rekorder im Technikraum	einbezogen: Kameras in allen öffentlichen Bereichen, Rekorder im Technikraum
Aufgeräumter Arbeitsplatz, gesperrter Bildschirm (A 7.7)	nicht anwendbar: keine Papierunterlagen mit empfindlicher Information	Meldescheine, Rechnungen, Zimmerlisten am Empfang; Rundgänge des Nachtdienstes	einbezogen: Meldescheine, Rechnungen und Zimmerlisten am Empfang; Rundgänge des Nachtdienstes
Sicherheit bei der Nutzung von Cloud-Diensten (A 5.23)	nicht anwendbar: keine Cloud-Dienste	gehostetes Verwaltungssystem, Spa-Plattform, Check-in-App	einbezogen: gehostetes Verwaltungssystem, Spa-Plattform, Check-in-App
Lieferantenbeziehungen (A 5.19, 5.20)	umgesetzt	Musterklausel in zwei von elf Verträgen	einbezogen; Stand «teilweise» oder «noch nicht», nicht «umgesetzt»: Musterklausel in zwei von elf Verträgen
Zweite Freigabe bei Änderung von Bankverbindungen (eigene Maßnahme, nicht auf der Liste)	nicht erwähnt	gelebt in der Buchhaltung, von niemandem geführt	als eigene Maßnahme erklärt und geführt, damit sie den Wechsel der Buchhalterin überlebt

Ein vollkommen guter Ausschluss, in den Worten des Bandes: Ein Hotel, das keine eigene Software entwickelt, braucht die Maßnahmen zur sicheren Programmierung nicht, und das in diesen Worten zu sagen, ist ein Grund, den nur dieses Haus so schreiben kann. Ebenfalls aus Kassel, nicht in der Erklärung geführt: Der Nachtdienst prüft bei jedem Rundgang, ob die Bildschirme im Backoffice gesperrt sind; die Etage bringt vergessene Dokumente in verschlossenen Umschlägen an den Empfang.

4 Unsere ausgeschlossenen Maßnahmen: die Probe, Zeile für Zeile

Referenzmaßnahme (Nr. im Anhang A)	Grund in den Worten des Hauses	Hat jemand, der durch das Haus gegangen ist, ihn geschrieben?	Geprüft von · am

Methode dieses Bandes: die Probe an jedem Ausschluss. **verlangt:** der Grund für jeden Ausschluss (6.1.3 d).

5 Woher die Maßnahmen stammen dürfen: Deutschland, Österreich, Schweiz

Die Norm erlaubt, Maßnahmen aus jeder Quelle zu nehmen (**verlangt** · 6.1.3 b): aus dem IT-Grundschutz-Kompendium des BSI, aus dem Österreichischen Informationssicherheitshandbuch oder aus dem IKT-Minimalstandard des Bundes (Schweiz). Was sie nicht erlaubt, ist, die Entscheidung selbst zu übernehmen: Was das Haus braucht und warum, bleibt beim Haus. In Deutschland führt der IT-Grundschutz auch zu einer eigenen Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz (Zertifikat des BSI); das gewöhnliche Zertifikat ist international vertrauter, der Grundschutz-Weg kann bei Häusern, die vor allem öffentliche Stellen beherbergen, ein Vorteil sein. Beides ist eine Entscheidung der Eigentümerschaft, keine ist eine Abkürzung (**Methode** dieses Bandes).

Quelle der Maßnahmen (falls nicht Anhang A) _____ **Entscheidung der Eigentümerschaft am** _____

Was diese Vorlage nicht ist

Dieses Blatt ersetzt weder die Norm noch eine Beratung oder Rechtsauskunft und ist kein Nachweis: Ein ausgefülltes Blatt ist keine Erklärung zur Anwendbarkeit, und die Erklärung ist erst dann ein Dokument des Hauses, wenn Menschen, die das Haus kennen, sie gebaut, gelesen und wissentlich unterschrieben haben. Die Zeilen aus Kassel sind Illustration und kein Muster für Ihre Gründe. Die Reihenfolge der acht Fragen, die Probe und die Spalte «Eintrag» sind Methode dieses Bandes, keine Anforderung; verlangt ist, was mit 6.1.3, 8.2 und 8.3 gekennzeichnet ist. Die Angaben zu Rahmenwerken geben den Stand des Bandes wieder (Rechtsstand des Bandes: 27. September 2026).