VORLAGE ZU ABSCHNITT 4.15 DES BANDES 5B

War das System zwischen den Audits wach?

Die Prüfung vor der Rezertifizierung: ob das System in drei Jahren wirksam war und ob es zu dem Haus noch passt, das man jetzt vor sich hat.

Kategorie: Prüfliste. Bezug im Buch: Abschnitt 4.15 (Rezertifizierung und das System, das wach bleiben muss); Norm: Klauseln 6.1.2, 6.1.3, 8.2, 9.3 und 10.1 sowie Maßnahmen des Anhangs A (Fassung 2022) der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Buches. Rechtsstand des Bandes: 28. September 2026.

Haus / Standort		**Ausgefüllt von**	
Zyklus von … bis …		**Datum**	
Zertifikat gültig bis		**Termin der Rezertifizierung**	

So nutzen Sie diese Vorlage

1. Eine Rezertifizierung ist keine größere Überwachung. Sie fragt nicht, ob das System befolgt wird, sondern ob es noch das System dieses Hauses ist. Bereiten Sie nicht ein Audit vor, sondern eine Bestandsaufnahme.
2. Beginnen Sie mit Teil 1 und 2 und legen Sie beide Ergebnisse nebeneinander: die Zeilen, die sich geändert haben, und die Dinge, die das Haus in drei Jahren eingeführt, abgeschafft oder verändert hat. Gehen Sie dann Teil 3 bis 5 durch.
3. Der Termin wird zwölf Monate vorher gesetzt, rückwärts vom Ablaufdatum des Zertifikats, nicht aus dem Kalender des Hauses (Teil 6).

1 Die drei Fassungen der Risikobeurteilung nebeneinander

Methode dieses Bandes. Legen Sie die Fassungen des Zyklus nebeneinander und zählen Sie die geänderten Zeilen, nach oben wie nach unten. Dreimal dasselbe Ergebnis, während sich der Gegenstand ändert, ist ein Prüfhinweis; ein gleiches Ergebnis kann nach einer echten Bewertung herauskommen, ohne jede Spur einer Bewertung ist es abgeschrieben (6.1.2: «wiederholbar» heißt, dass das Verfahren wiederholt angewandt werden kann).

Fassung (Datum, Version)	Zeilen gesamt	unverändert	geändert	entfallen	neu hinzugekommen	Beleg der Bewertung (Protokoll, Teilnehmende)

Beispiel aus Abschnitt 4.15: In drei Fassungen dieselben 42 Risiken, in derselben Reihenfolge, mit denselben Werten; geändert hatten sich nur Datum und Versionsnummer. Die neue Beurteilung (ein Vormittag, vier Personen aus vier Bereichen) ergab von 42 Zeilen 28 unverändert, 7 geändert, 7 entfallen und 13 neue. Das Maß des Bandes: Die Beurteilung soll jedes Jahr an einigen Stellen anders aussehen und insgesamt ungefähr gleich lang bleiben; wächst sie nur, fehlt meist das Streichen. Ein Nachbarhaus war von 32 auf 114 Zeilen gewachsen.

2 Was wurde in drei Jahren eingeführt, abgeschafft oder verändert?

Methode dieses Bandes. Die Antwort steht nicht in den Unterlagen des Systems, sondern in vier Quellen; wer sie einmal im Zyklus durchsieht, findet nach dem Band zuverlässig zwei bis fünf Dinge, die nirgends im Managementsystem vorkommen. Verlangt (8.2): Risiken werden in geplanten Abständen und bei wesentlichen Änderungen beurteilt, die vorgeschlagen werden oder eintreten.

Quelle	Eingeführt, abgeschafft, verändert (Dienst, Verfahren, Gerät)	Wann	In der Risikobeurteilung?	Vier Fragen beantwortet?
Investitionsanträge			☐ ja ☐ nein	☐ ja ☐ nein
Verträge			☐ ja ☐ nein	☐ ja ☐ nein
Projektlisten des Marketings			☐ ja ☐ nein	☐ ja ☐ nein
Rechnungen			☐ ja ☐ nein	☐ ja ☐ nein

Beispiel aus Abschnitt 4.15: Handyschlüssel (vor vierzehn Monaten), digitaler Check-in mit Ausweisbild und Gesichtsabgleich (vor elf Monaten), automatisierter Gästedialog (vor sieben Monaten). In der Risikobeurteilung kam keines davon vor: drei Dienste, null Zeilen. Abschnitt 8.2 war dreimal ausgelöst und dreimal nicht angewandt worden.

3 Die vier Fragen vor dem Start jedes neuen gästenahen Dienstes

Frage	Antwort	Grund (aus dem Band)	Im Buch
Welche Daten entstehen?		Vier Fragen, eine halbe Stunde; sie gehören in dieselbe Vorlage, in der Preis, Anbindung und Kündigungsfrist stehen.	Methode dieses Bandes
Zu welcher Kategorie gehören sie? Ist es eine besondere Kategorie, etwa biometrische Daten zur eindeutigen Identifizierung?		Ein Verfahren, das biometrische Daten erzeugt, ist in den meisten Häusern das einzige seiner Art, und deshalb gibt es niemanden, der es erkennt.	Methode dieses Bandes; Recht: siehe unten

Frage	Antwort	Grund (aus dem Band)	Im Buch
Auf welcher Grundlage werden sie verarbeitet?		Bei besonderen Kategorien braucht die Verarbeitung eine tragfähige Grundlage; in der Hotellerie ist das die ausdrückliche Einwilligung, und sie muss freiwillig sein.	Methode dieses Bandes; Recht: siehe unten
Wie lange bleiben sie, bei uns und beim Anbieter?		Bilder, die nach der Prüfung keinen Zweck mehr haben, bleiben, wenn niemand eine Frist vereinbart; der Vertrag sagte nichts.	Methode dieses Bandes
Bei besonderer Kategorie: Ist eine Folgenabschätzung erforderlich und begründet? Gibt es einen gleichwertigen Weg ohne den digitalen (Tresen, ohne Aufpreis, ohne Nachteil)?		Eine Einwilligung trägt nur, wenn es eine echte Alternative gibt; eine gleiche Dauer lässt sich nicht in jeder Lage versprechen, wohl aber eine Behandlung, die die Wahl nicht bestraft.	Methode dieses Bandes; Recht: siehe unten

Die drei Sätze im Vertrag des neuen Dienstes	Vereinbart?	Fundstelle
Löschfristen für jede Datenart	☐ ja ☐ nein	
Verbot der Verwendung für eigene Zwecke des Anbieters, einschließlich der Verbesserung seiner Dienste	☐ ja ☐ nein	
Nennung der Unterauftragnehmer mit Mitteilungspflicht	☐ ja ☐ nein	

Methode dieses Bandes. Wer diese drei Sätze verhandelt, erfährt binnen einer Woche, mit welcher Art von Anbieter er es zu tun hat. Der Handyschlüssel wird wie jedes Zugangsmittel behandelt: Liste der gültigen Berechtigungen je Zimmer, automatischer Entzug bei Abreise, Weg für den sofortigen Entzug bei Verlust, Regel für Begleitpersonen, Türprotokoll mit Frist und begrenztem Zugriff.

4 Die Managementbewertung und die Erklärung zur Anwendbarkeit

Frage	Antwort	Grund (aus dem Band)	Im Buch
Stehen die Änderungen bei internen und externen Themen als Eingabe in der Managementbewertung, und folgen daraus Entscheidungen in den Ergebnissen?		Die Einführung dreier Dienste ist eine Änderung interner Themen; sie gehört in die Eingabe, und was daraus folgt, in die Ergebnisse.	verlangt (9.3)
Wurde der Satz «weiterhin angemessen» geprüft, bevor er geschrieben wurde?		Er ist eine Feststellung, die geprüft werden kann; dreimal geschrieben, hat er dreimal verhindert, dass jemand nachsah.	Methode dieses Bandes (Anker: 9.3)
Wurde die Erklärung zur Anwendbarkeit nach der neuen Beurteilung überarbeitet?		Sie folgt der Beurteilung; bleibt die Beurteilung stehen, bleibt auch die Erklärung stehen, und beide altern unbemerkt gemeinsam.	verlangt (6.1.3)
Ist das System nicht nur wirksam, sondern noch geeignet?		Ein System kann wirksam sein und zugleich ungeeignet werden, weil das Haus ein anderes geworden ist.	verlangt (10.1: Eignung, Angemessenheit, Wirksamkeit)

5 Die Zyklusbilanz: drei Veränderungen je Jahr

Methode dieses Bandes. Nicht drei Feststellungen, nicht drei Dokumente: drei Veränderungen im Betrieb, die durch das Managementsystem anders geworden sind. Wer neun Dinge nennen kann, hat ein System; wer keine nennen kann, hat eine Urkunde erneuert.

Jahr des Zyklus	Veränderung 1	Veränderung 2	Veränderung 3
1			
2			
3			

6 Der Zeitplan: zwölf Monate rückwärts vom Ablaufdatum

Reihenfolge	Schritt	Geplant bis	Erledigt am
1	Durchsicht der vier Quellen		
2	Neue Risikobeurteilung: jede Zeile bleibt unverändert, ändert sich oder entfällt; danach die Frage, was fehlt		
3	Überarbeitung der Erklärung zur Anwendbarkeit		
4	Vollständiges internes Audit		
5	Managementbewertung		

Methode dieses Bandes: Wer in dieser Reihenfolge arbeitet, geht mit einem System in die Rezertifizierung, das er selbst schon geprüft hat; wer es umgekehrt macht, lässt sich von einem Fremden erklären, was sich in seinem Haus verändert hat. Die Rezertifizierung findet vor dem Ablauf des Zertifikats statt; wer zu spät beginnt, riskiert eine Lücke zwischen zwei Zertifikaten, die in Ausschreibungen wie ein Entzug aussieht. Inhalt und Zeitpunkt folgen ISO/IEC 17021-1 in Verbindung mit ISO/IEC 27006-1.

7 Häufige Fehler

Die Risikobeurteilung als Dokument statt als Arbeit.	Zweiundvierzig Zeilen, jährlich mit neuem Datum; ein Verzeichnis, das nichts auslöst, ist ein Beleg. Stillstand schützt sich selbst: Wer die erste Zeile ändert, stellt die anderen in Frage.

Wachstum ohne Bereinigung.	Keine Zeile kam hinzu, keine fiel weg: Die Fähigkeit, ein Risiko zu streichen, ist das sicherste Zeichen dafür, dass jemand die Liste liest.
Der Ausweis im Bild.	Der automatische Abgleich erzeugt biometrische Daten; das Verfahren wurde wie eine Zahlungsart geprüft: Bedienbarkeit, Preis, Anbindung.
Die fehlende Löschung.	Der Anbieter hatte getan, was der Vertrag sagte, und der Vertrag sagte nichts.
Der Handyschlüssel ohne Betrachtung.	Entzug, Geschwindigkeit, Liste der Berechtigungen, Verlust, Begleitpersonen, Türprotokoll: alles, was das Haus für seine Karten längst beantwortet hatte.
Der Gästedialog.	Gäste schreiben dem Assistenten, was sie einer Rezeption nicht sagen würden; eine Klausel zur Verwendung der Verläufe macht den Anbieter insoweit zu mehr als einem Auftragsverarbeiter.
Der Satz in der Managementbewertung: «weiterhin angemessen».	Dreimal geschrieben, während sich das Haus veränderte.

Recht laut Buch (Rechtsstand des Bandes: 28. September 2026.): Biometrische Daten zur eindeutigen Identifizierung sind eine besondere Kategorie personenbezogener Daten; in der Hotellerie regelmäßig allein auf Grundlage einer ausdrücklichen, freiwilligen Einwilligung. Datenschutz-Folgenabschätzung: Art. 35 DSGVO (hohes Risiko; Listen der Aufsichtsbehörden; keine Automatik); Schweiz: Art. 22 des revidierten Datenschutzgesetzes (seit 1. September 2023). Ein bloßes Ausweisfoto ist nicht allein deshalb ein biometrisches Datum. Meldewesen Deutschland: seit 1. Januar 2025 entfällt die besondere Meldepflicht für Gäste mit deutscher Staatsangehörigkeit; für andere Gäste bleiben Meldeschein mit eigenhändiger Unterschrift, Vorlage des Reisedokuments und Abgleich; die Unterschrift kann unter den Voraussetzungen des § 29 Abs. 5 BMG elektronisch ersetzt werden, ein gewöhnlicher digitaler Check-in ersetzt sie nicht von selbst. Österreich: Meldegesetz; Schweiz: kantonale Regelungen. Stand und Fassung sind vor Anwendung im Einzelfall zu prüfen.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch ISO/IEC 17021-1 oder ISO/IEC 27006-1; sie beurteilt nicht, ob ein Haus rezertifizierungsreif ist, und die Entscheidung trifft die Zertifizierungsstelle. Ein ausgefülltes Blatt ist kein Nachweis: Ausbleibender Schaden beweist weder Wirksamkeit noch das Gegenteil; geprüft wird die Übereinstimmung zwischen dem, was ein Haus tut, und dem, was es aufgeschrieben hat.