VORLAGE ZU ABSCHNITT 3.1 DES BANDES 5B

Das Auditprogramm, das die Information sucht, die niemand sieht

Ein Vorgang statt einer Abteilung: der interne Auditor folgt einer Veranstaltung von der Ankunft der Information bis zu ihrer Löschung.

Kategorie: Prüfliste (mit Anwendung in Schritten und häufigen Fehlern). Bezug im Buch: Abschnitt 3.1 (Das Prinzip, Operative Synthese); Norm: Klauseln 4.3, 6.1.2, 7.5, 8.1 und 9.2 sowie Maßnahmen A.5.9, A.5.12, A.5.13 und A.8.10 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**	
Datum		**Vorgang (Haus)**	

So nutzen Sie diese Vorlage

1. Wählen Sie keinen Prozess und keine Abteilung, sondern einen Vorgang, den das Haus tatsächlich bedient hat: eine Tagung, eine Hochzeit, eine Gruppenanreise. Das Haus sucht ihn aus, nicht der Auditor (3.1).
2. Folgen Sie der Information, die der Vorgang erzeugt hat, so wie ein Auditor in einem Werk einer Charge folgt: von der Stelle, an der sie ankommt, bis zu der Stelle, an der sie verschwindet. Stellen Sie an jeder Station dieselben vier Fragen (Teil 2).
3. Öffnen Sie erst danach ein Dokument des Managementsystems. Das Dokument kommt nach dem Vorgang.

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

1 Die Fragen, die im Audit alles tragen

Frage	Antwort	Grund (aus dem Band)	Im Buch
Welche Informationen hält dieses Haus?		Geprüft werden kann nur, was benannt ist, und benannt wird nur, was jemandem gehört.	verlangt (A.5.9)
Wer hat für jede von ihnen entschieden, wie sie behandelt wird?		Alle vier Maßnahmen (A.5.9, A.5.12, A.5.13, A.8.10) setzen keine Technik voraus, aber eine Entscheidung.	verlangt (A.5.9, A.5.12, A.5.13, A.8.10)
Woran würde man merken, dass die Entscheidung nicht eingehalten wird?		Das interne Audit liefert Information darüber, ob das System in der Wirklichkeit des Hauses wirksam verwirklicht ist, nicht ob die Dokumentation vollständig ist.	verlangt (9.2; 8.1)
Welche Information, die dieses Haus täglich bewegt, steht auf keiner Liste?		Die Prüfung der bekannten Werte kann nur bestätigen; erst die umgekehrte Frage macht das Audit wirksam.	Methode dieses Bandes

2 Der Weg der Information: dieselben vier Fragen an jeder Station

Frage an jeder Station	Grund (aus dem Band)	Im Buch
Was ist hier angekommen?	Die Liste kam als Anhang einer E-Mail an und lebte als Ausdruck weiter; in diesem Denken war sie kein Wert, sondern ein Arbeitsmittel.	Methode dieses Bandes
Wer hat es weitergegeben, und an wen?	Jede Weitergabe war der schnellste Weg, die Tagung gut zu bedienen; niemand tat etwas Falsches, und niemand führte Buch.	Methode dieses Bandes
Wo liegt es jetzt, in allen Kopien?	Das Haus fand neun Orte, darunter Papierkorb, Tablet und ein Laufwerk mit vier Jahrgängen.	Methode dieses Bandes
Und wann geht es weg?	Löschen verlangt eine Entscheidung, Behalten keine; die Frist fehlte.	verlangt (A.8.10); Form: Methode

Station (Ort, Person)	Angekommen	Weitergegeben von / an	Liegt jetzt (alle Kopien)	Geht weg am (Frist, Nachweis)

3 Zahlen, die ein Haus ohne zusätzliche Technik erheben kann

Zahl	Dieses Jahr	Vorjahr	Grund (aus dem Band)	Im Buch
Kopien des Vorgangs, die nach der Abreise noch bestehen			Zeigt, ob die Regel wirkt; sinkt die Zahl der Fundorte gegenüber dem Vorjahr nicht, wirkt die Regel nicht.	Methode dieses Bandes

Zahl	Dieses Jahr	Vorjahr	Grund (aus dem Band)	Im Buch
Tage nach der Veranstaltung, bis die letzte Kopie verschwindet			Sagt in der Managementbewertung mehr als der Anteil geschulter Personen.	Methode dieses Bandes
Wie oft in einem Jahr hat jemand eine Liste angefordert, die längst hätte gelöscht sein müssen?			Derselbe Weg einer Information ist der Weg, auf dem sich Wirksamkeit messen lässt.	Methode dieses Bandes
Zahl der Veranstaltungen mit Listen ab zehn Teilnehmenden, für die sich ohne Suche sagen lässt, welche Unterlagen noch bestehen und wo			Das Haus hatte nicht ein Problem mit einer Liste, sondern vierundsechzig Vorgänge, von denen einer sichtbar wurde.	Methode dieses Bandes

4 Pflichten: was der Auditor braucht, ohne Jurist zu sein

Frage	Antwort	Grund (aus dem Band)	Im Buch
Welche Pflichten hat das Haus für sich selbst festgehalten?		Die Norm sagt, dass geltendes Recht einzuhalten ist; welches, sagt sie nicht. Für Luzern, Konstanz und Salzburg sind die Antworten verwandt, aber nicht gleich.	Methode dieses Bandes
Wer verantwortet jede dieser Pflichten (Name)?		Der Auditor braucht den Namen der Person je Pflicht.	Methode dieses Bandes
Wurde die Liste in den letzten zwölf Monaten gegen eine äußere Quelle geprüft; wann, und von wem?		Ob die Auslegung richtig ist, entscheidet nicht der Auditor; dass niemand sie geprüft hat, stellt er fest.	Methode dieses Bandes
Gilt für Gesundheitsangaben in der Bemerkungsspalte besonderer Schutz, und führt das Haus das Verzeichnis der Verarbeitungstätigkeiten, das dafür verlangt ist?		CH: besonders schützenswerte Personendaten (revDSG, seit 1. September 2023). DE und AT: besondere Kategorien der DSGVO; Verzeichnis, sobald solche Daten verarbeitet werden, unabhängig von der Betriebsgröße. Rechtsstand: 28. September 2026.	verlangt (Recht des Landes); Prüfung: Methode
Wer entscheidet im Ereignisfall über die Meldung, und welche Frist gilt an diesem Standort?		DE und AT: binnen zweiundsiebzig Stunden an die Aufsichtsbehörde, es sei denn, kein Risiko. CH: so rasch als möglich an den Beauftragten bei voraussichtlich hohem Risiko; eine feste Frist von zweiundsiebzig Stunden kennt das Schweizer Recht nicht. Rechtsstand: 28. September 2026.	verlangt (Recht des Landes)

5 Anwendung in Schritten

Schritt	Was zu tun ist (Operative Synthese des Abschnitts)	Erledigt
1 Sofort	Eine Veranstaltung der letzten drei Monate nehmen, die Liste suchen, die sie erzeugt hat, in allen Kopien, Papier eingeschlossen, und die gefundenen Orte aufschreiben.	☐
2 Planen	Das Informationsverzeichnis von den Informationen her aufbauen und nicht von den Geräten: eine verantwortliche Person je Kategorie im Betrieb und nicht in der IT, und für jede Kategorie eine Frist mit Grund.	☐
3 Überwachen	Einmal im Jahr denselben Weg mit einer anderen Veranstaltung gehen und die Zahl der Fundorte mit der des Vorjahres vergleichen.	☐
4 Regel für das Programm	Kein Audit beginnt mit einem Dokument. Es beginnt mit einem Vorgang, den das Haus aussucht.	☐
5 Feststellung	Die Feststellung gehört an die Stelle, an der die Regel fehlt, und das ist die Leitung, nicht das Officebrett.	☐

6 Häufige Fehler

Fehler (wie der Band ihn nennt)	Was der Band dagegen zeigt
Das Wort «Daten» meint Systeme; eine Liste als Anhang gilt als Arbeitsmittel, nicht als Information.	In einem Hotel entsteht der größte Teil der schützenswerten Information am Tresen, im Bankettbüro, am Telefon und im Gespräch, nicht in der IT.
Was vom Kunden kommt, wird als Auftrag behandelt, nicht als anvertrautes Gut.	Fragen, unter welchen Bedingungen der Kunde die Angaben erhoben hat und was er dem Haus damit übergab.
Gesundheitsangaben stehen in der Spalte «Bemerkungen» neben der Ankunftszeit.	Eine Unverträglichkeit und eine salzarme Kost nach einem Eingriff sind Gesundheitsangaben.
Keine Klassifizierung: Die Richtlinie spricht von vertraulich, sagt aber nicht, was, wer entscheidet und was folgt.	Zwei Stufen, die jeder benennen kann, und drei Regeln wirken besser als vier Stufen mit zwölf Regeln; Kennzeichnung nur auf Gästeunterlagen.
Das Inventar ist ein Geräteverzeichnis, das die IT lieferte; die Frage ging nur an die IT.	Dieselbe Frage an Bankett, Réception, Buchhaltung und Personalabteilung; das Verzeichnis beschreibt, was das Haus weiß, nicht was es besitzt.
Niemand hat entschieden, wie lange eine Liste bleibt.	Eine Frist je Kategorie; für den Übergang vom Arbeitsmittel zum Bestand braucht das Haus einen Begriff von Zeit.
Der Auditor prüft, was dokumentiert ist.	Ein System, das nur gegen seine eigenen Dokumente geprüft wird, kann nur bestätigen, dass das Vorhandene stimmt.
Eine Maßnahme gilt als umgesetzt, weil ein Dokument über sie existiert.	Der häufigste stille Fehler in der Erklärung zur Anwendbarkeit: Es fehlte die Zuordnung, welche Information in welche Klasse fällt.
Alles klassifizieren, kennzeichnen und mit Frist versehen (Gegenfall Chur).	Die Kennzeichnung wurde zum Stempel. Küche braucht die Diät, nicht den Namen; der Service den Platz, nicht die Diagnose.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch das Recht, das für Ihr Haus gilt; sie beurteilt nicht, ob eine Auslegung richtig ist. Sie ist keine Checkliste, die das Audit ersetzt: Sie gibt die Reihenfolge der Fragen, nicht ihre Antworten. Ein ausgefülltes Blatt ist kein Nachweis: Es zeigt, dass jemand einem Vorgang gefolgt ist, nicht dass die Entscheidungen im Haus getroffen und eingehalten werden. Rechtsstand des Bandes: 28. September 2026.