Eine Feststellung: was ein Haus tun kann

Der Grad als Auftrag, nicht als Urteil: Tatsachen, Anforderung und Einstufung prüfen, Korrektur und Korrekturmaßnahme trennen, jede Zeile des Berichts einem Eigentümer geben, und den Weg für Einspruch und Beschwerde kennen.

Kategorie: Arbeitsblatt (Prüf-Checkliste mit Register). Bezug im Buch: Abschnitt 4.7 (Das Prinzip, Regeln eins bis sechs; Was die Norm sagt); Norm: Klauseln 5.3, 6.3, 8.1, 9.2 und 10.2 sowie Anhang A (Fassung 2022) 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		**Zertifizierungsstelle**	
Audit (Art, Datum)		**Feststellung Nr.**	
Grad (Haupt / Neben / Beobachtung)		**Eigentümer im Haus**	

So nutzen Sie diese Vorlage

1. Hören Sie in der Abschlussbesprechung einen Auftrag, kein Urteil. Fragen Sie nicht zuerst, ob das wirklich eine Hauptabweichung sein müsse; das kostet die Zeit, die der Ursachenanalyse fehlt.
2. Prüfen Sie Tatsachen, Anforderung und Einstufung (Abschnitt 2). Ein begründeter Einwand kann jeden der drei Punkte betreffen, und der richtige Zeitpunkt ist die Abschlussbesprechung, mit einem Nachweis, nicht mit einer Meinung.
3. Tragen Sie jede Zeile des Berichts in dasselbe Register ein, gleich welchen Grades, mit Eigentümer und Termin; bei einer Beobachtung lautet die Entscheidung «umsetzen bis …» oder «nicht umsetzen, weil …», unterschrieben (Empfehlung dieses Bandes, keine Pflicht).
4. Trennen Sie Korrektur (beseitigt den Zustand) und Korrekturmaßnahme (beseitigt die Ursache) und tragen Sie jede in ihr eigenes Feld ein (Abschnitt 3). Fragen Sie fünfmal «Warum?», bis die Ursache feststeht.
5. Wählen Sie die Abhilfe so klein, dass sie den Betrieb überlebt, und so genau, dass sie die Ursache trifft. Lassen Sie die Abhilfe weiterlaufen, während ein Einspruch oder eine Beschwerde geprüft wird (Abschnitt 4).
6. Lesen Sie den Bericht von hinten: Unter «Verbesserungspotenzial» steht, was jemand gesehen, aber nicht beanstandet hat.

Spalte «Im Buch»: verlangt = von Norm oder Regelwerk verlangt, wie der Band es in eigenen Worten wiedergibt (Klausel oder Quelle in Klammern); Methode dieses Bandes = Vorgehen oder Empfehlung des Bandes, keine Anforderung. Fristen, Nachweise und Verfahren legt jede Zertifizierungsstelle in ihren Regeln und im Vertrag fest; im Einzelfall gilt der Vertrag.

1 Die drei Grade und wozu sie verpflichten

Grad	Was er bedeutet (laut Buch)	Wozu er verpflichtet (in der Regel)	Im Buch
Hauptabweichung	Eine Anforderung ist nicht erfüllt, und dadurch ist die Fähigkeit des Systems berührt, die beabsichtigten Ergebnisse zu erreichen. Indizien: eine vollständig fehlende Maßnahme, ein sich wiederholendes Versagen, mehrere Nebenabweichungen mit demselben Muster, ein Mangel, den das System selbst hätte finden müssen. Kein Indiz entscheidet für sich; maßgeblich sind das betroffene Erfordernis, die objektiven Nachweise und die Auswirkung auf die Wirksamkeit.	Korrektur, Ursachenanalyse und Korrekturmaßnahme mit Nachweis innerhalb einer Frist, die die Stelle nach ihren Regeln und der Schwere des Falls setzt, gegebenenfalls Nachaudit vor Ort. Vor einer positiven Zertifizierungsentscheidung muss die Stelle Umsetzung und Wirksamkeit verifiziert und die Hauptabweichung geschlossen haben; ein Maßnahmenplan allein genügt nicht. Bei bestehendem Zertifikat entscheidet die Stelle über weitere Maßnahmen, gegebenenfalls bis zur Aussetzung oder zum Entzug.	verlangt (ISO/IEC 17021-1 in Verbindung mit ISO/IEC 27006-1; Einzelheiten: Regeln der Stelle und Vertrag)
Nebenabweichung	Ein einzelner Ausrutscher in einem im Übrigen wirksamen System.	Ein Maßnahmenplan, den die Stelle auf Angemessenheit prüft und annimmt; die Umsetzung verifiziert sie später, beim nächsten Audit oder durch Vorlage von Unterlagen.	verlangt (wie oben)
Beobachtung (Verbesserungschance)	Keine Abweichung: geschenkte Fachkenntnis von jemandem, der hundert Häuser gesehen hat, der einzige Teil des Berichts, der reine Auskunft ist.	Keine förmliche Antwort, keine Ursachenanalyse, kein Maßnahmenplan. Was ein Erfordernis tatsächlich verletzt, darf nicht als bloße Anregung abgelegt werden; steht etwas darunter, das eigentlich fehlt, ist es wie eine Abweichung zu behandeln und die Einstufung mit der Stelle zu klären.	Begriffe: verlangt (wie oben); Entscheidung je Zeile: Methode dieses Bandes

2 Prüfen: Tatsachen, Anforderung, Einstufung

Frage	Antwort	Grund (aus dem Band)	Im Buch
Tatsachen: Stimmt der Sachverhalt, den der Auditor festhält? Welcher objektive Nachweis liegt ihm zugrunde?		Ein begründeter Einwand kann den Sachverhalt betreffen; er kommt mit einem Nachweis, nicht mit einer Meinung.	Methode dieses Bandes
Anforderung: Welche Anforderung ist zitiert (Klausel oder Maßnahme), und trifft sie auf diesen Sachverhalt zu?		Ein begründeter Einwand kann auch die zitierte Anforderung betreffen.	Methode dieses Bandes

Frage	Antwort	Grund (aus dem Band)	Im Buch
Einstufung, Auswirkung: Ist die Fähigkeit des Systems berührt, die beabsichtigten Ergebnisse zu erreichen? Wie wurde die Auswirkung auf die Wirksamkeit bewertet?		Der Grad richtet sich nicht nach der Größe des Lochs, sondern danach, ob das System um das Loch herum funktioniert hat.	verlangt (ISO/IEC 17021-1 in Verbindung mit ISO/IEC 27006-1)
Einstufung, Kette: War die Maßnahme beschrieben, in der Erklärung zur Anwendbarkeit als umgesetzt erklärt, intern geprüft, und im Vorjahr schon angesprochen?		Im Bremer Fall hatten vier Sicherungen nacheinander versagt; diese Kette, nicht die Zahl der offenen Konten, trug die Einstufung.	Methode dieses Bandes
Grauzone, drei Fragen: Fehlt die Maßnahme ganz, oder ist sie nur an dieser Stelle nicht befolgt worden? Hat das System den Mangel selbst gefunden oder erst der Auditor? Ist es das erste Mal?		Drei Antworten geben der Einstufung eine Richtung, ersetzen aber nicht die Bewertung nach Anforderung, Nachweisen und Wirksamkeit.	Methode dieses Bandes
Wiederholung: Ist dieselbe Feststellung im Vorjahr schon vorgekommen, und wurde damals nur die Korrektur geliefert?		Eine Wiederholung ist ein ernstes Indiz für eine Wirksamkeitslücke und kann bis zur Hauptabweichung führen.	Methode dieses Bandes

3 Abhilfe: Korrektur, Ursache, Korrekturmaßnahme

Frage	Antwort	Grund (aus dem Band)	Im Buch
Korrektur: Welchen Zustand beseitigt sie, bis wann, mit welchem Nachweis? (Eigentümer und Termin im Register)		Die Korrektur beseitigt den Zustand, nicht die Ursache; Häuser liefern regelmäßig nur sie und tragen sie in das Feld der Korrekturmaßnahme ein.	verlangt (Klausel 10.2: reagieren und korrigieren); Register: Methode
Ursache: Wie lautet die Antwort auf fünf aufeinanderfolgende «Warum?», und wo hört die Kette bei einem Prozess, einem Formular, einem Vertrag auf?		Die Ursachenanalyse braucht keine Methodik, sondern Hartnäckigkeit.	verlangt (Klausel 10.2: Ursachen ermitteln); fünf Fragen: Methode
Korrekturmaßnahme: Beseitigt sie die Ursache, damit der Zustand nicht wieder entsteht? Ist sie so klein, dass sie den Betrieb überlebt, und so genau, dass sie die Ursache trifft?		In Bremen war es eine Zeile auf einem Formular, in Oldenburg waren es vierzehn Unterschriften; ein Verfahren mit mehr Beteiligten als nötig erzeugt Unterschriften statt Handlungen.	verlangt (Klausel 10.2); Maßstab: Methode
Gleichartiges: Wo im Haus könnten gleichartige Nichtkonformitäten bestehen oder auftreten?		Der letzte Halbsatz von Klausel 10.2 entscheidet die Qualität der Abhilfe.	verlangt (Klausel 10.2)
Wirksamkeit: Wer bewertet, wann und womit, ob die Korrekturmaßnahme wirkt, und wo ist es dokumentiert? Prüft das interne Audit Daten statt Dokumente?		Ein internes Audit, das Dokumente gegen Dokumente prüft, bestätigt die Beschreibung der Welt und nicht die Welt; der Entzug von Berechtigungen ist ein Prozess mit hoher Bedeutung.	verlangt (Klauseln 10.2 und 9.2)
Zuständigkeiten: Wer informiert wen und wann, wenn mehrere Stellen im Haus und ein externer Dienstleister beteiligt sind? Gibt es eine Rückmeldung des Dienstleisters in einer Frist?		Solange nicht festgelegt ist, wer wen wann informiert, ist die Anforderung nicht erfüllt, auch wenn jede Stelle ihre Arbeit gut macht; ein Prozess ohne Auftrag, Frist und Rückmeldung ist nicht gesteuert.	verlangt (Klauseln 5.3 und 8.1)
Fristen: Welche Frist hat die Stelle gesetzt, ist ein Nachaudit vor Ort vorgesehen, und gilt der Vertrag?		Die Frist setzt die Stelle nach ihren Regeln und der Schwere des Falls; Einzelheiten stehen im Vertrag, nicht im Buch.	verlangt (Regeln der Stelle und Vertrag)
Bericht: Hat jede Zeile des Berichts, auch jede Beobachtung, einen Eigentümer, einen Termin und eine Entscheidung?		Zwischen dem Satz im Bericht und der Hauptabweichung des Folgejahres lag das Versäumnis, ihn jemandem zuzuteilen.	Methode dieses Bandes (Empfehlung, keine Pflicht für jede Beobachtung)

Beispiel aus Abschnitt 4.7 (Bremen, drei Konten ausgeschiedener Beschäftigter): Die Korrektur bestand aus drei Deaktivierungen, einem Kennwortwechsel und der Rückgabe zweier Generalschlüssel. Die Korrekturmaßnahme bestand aus einer Zeile auf dem Austrittsformular mit drei Empfängern, fünf Fristen anstelle des Wortes «unverzüglich», einer Übersicht der Zugänge je Person, einer Vereinbarung mit dem IT-Dienstleister über schriftliche Rückmeldung und dem Quartalsabgleich der aktiven Konten gegen die Personalliste. Die Hauptabweichung war in elf Tagen korrigiert und in drei Monaten erledigt.

4 Der Weg für Einspruch und Beschwerde

Schritt	Was zu tun ist	Grund (aus dem Band)	Im Buch
1 Gespräch	Das Gespräch mit dem Auditteam in der Abschlussbesprechung führen und der Feststellung widersprechen: der Tatsache, der zitierten Anforderung, der Bewertung der Auswirkung oder dem Grad selbst. Mit Nachweis.	Das Gespräch ist vom förmlichen Einspruch und von der Beschwerde zu trennen; nach der Abschlussbesprechung wird aus der Feststellung ein Bericht (Abschnitt 4.5).	Methode dieses Bandes
2 Weg wählen	Einspruch, wenn er sich gegen eine Entscheidung der Zertifizierungsstelle richtet; Beschwerde, wenn sie sich gegen ihr Verhalten oder das eines Auditors richtet. Beide werden von Personen bearbeitet, die an der beanstandeten Sache nicht beteiligt waren.	Ein Haus, das diesen Weg nicht kennt, nimmt eine Feststellung hin, gegen die es hätte vorgehen können (Glossar: Einspruch und Beschwerde).	verlangt (ISO/IEC 17021-1 in Verbindung mit ISO/IEC 27006-1; Verfahren der Stelle)
3 Verfahren der Stelle lesen	Das förmliche Verfahren in den Bedingungen und im Vertrag der Stelle nachlesen: Form, Ansprechstelle, Fristen. Der Band nennt dafür keine Fristen und keine Ansprechstelle: Die Felder unten bleiben leer, bis sie aus dem Vertrag stammen.	Es gibt bei jeder Zertifizierungsstelle ein förmliches Verfahren für Einspruch und Beschwerde; jede Stelle regelt den Ablauf selbst.	verlangt (Verfahren je Stelle: Vertrag)

Schritt	Was zu tun ist	Grund (aus dem Band)	Im Buch
4 Abhilfe weiterführen	Die Abhilfe nach Abschnitt 3 läuft weiter, auch wenn ein Einspruch oder eine Beschwerde läuft.	Das Verfahren dauert regelmäßig länger als die Abhilfe; ob es Pflichten oder Fristen aufschiebt, regeln die Bedingungen der Stelle; rechnen Sie nicht damit.	Methode dieses Bandes

Einspruch / Beschwerde		**Ansprechstelle der Stelle**	
Frist laut Vertrag		**Eingereicht am**	
Aufschiebende Wirkung laut Vertrag		**Ergebnis**	

5 Häufige Fehler laut Abschnitt

Fehler	Was der Abschnitt dazu sagt
«Unverzüglich» als einzige Vorgabe	Im Recht bedeutet es «ohne schuldhaftes Zögern» (§ 121 BGB); für den Betriebsablauf ist es unbestimmt. Wer ein Verfahren schreibt, konkretisiert es durch eine Zahl; dringende Sperren erfolgen sofort.
Der Prozess, der nur einen Fall kennt	Saisonkraft, fristlose Trennung, Freistellung, Wechsel innerhalb der Gesellschaft, Leiharbeitnehmer, Auszubildende: in einem Hotel sind das zusammen mehr Fälle als der beschriebene.
Keine Übersicht je Person	Das Haus wusste, wer Zugriff, wer einen Schlüssel und wer ein Postfach hatte; es wusste zu keinem Menschen, was er insgesamt hatte.
Der externe Dienstleister auf Zuruf	Ohne Auftrag, Frist und Rückmeldung gibt es zu keinem Austritt einen Nachweis, dass die Berechtigung entzogen wurde.
Das interne Audit prüft das Papier	Es hatte das Verfahren geprüft und nicht zwei Listen nebeneinandergelegt: Konten gegen Personalliste.
Die unbearbeitete Verbesserungschance	Sie war keine Abweichung, also ohne Pflicht, ohne Eigentümer, ohne Termin und vergessen; sie steht im Bericht an der schwächsten Stelle, hinten.
Die Reaktion im Raum	Die erste Frage nach der Einstufung lautete, ob das wirklich eine Hauptabweichung sein müsse; die Frage ist verständlich und kostet die Zeit, die der Ursachenanalyse fehlt.

Rahmen laut Buch: Wird ein ausgeschiedenes Konto tatsächlich genutzt, liegt eine Verletzung des Schutzes personenbezogener Daten vor, die der Aufsichtsbehörde grundsätzlich binnen 72 Stunden zu melden ist (Schweiz: so rasch als möglich). Der Abgleich von Konten- und Personallisten berührt Beschäftigtendaten und kann der Mitbestimmung unterliegen (DE: Betriebsverfassungsrecht; AT: Betriebsvereinbarung; CH: Art. 26 der Verordnung 3 zum Arbeitsgesetz, Art. 328b OR); er ist keine Verhaltensüberwachung, die Auswertung von Zugriffsprotokollen kann eine sein. 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 Regeln und den Vertrag Ihrer Zertifizierungsstelle: Grad, Fristen, Nachaudit, Aussetzung und das Verfahren für Einspruch und Beschwerde bestimmt die Stelle nach ihren Regeln; im Einzelfall gilt der Vertrag. Sie stuft keine Feststellung ein und prüft keinen Einspruch auf Erfolgsaussicht. Ein ausgefülltes Blatt ist kein Nachweis: Es zeigt, dass jemand die Feststellung geprüft und der Abhilfe einen Eigentümer gegeben hat, nicht dass die Abhilfe wirkt.