Was das Audit der Managementbewertung schuldet

Die Eingaben, die das interne Audit liefert: Abdeckung, Entwicklung und höchstens drei Entscheidungen, und das Protokoll, das sie festhält.

Kategorie: Vorlage (Beitrag zur Managementbewertung). Bezug im Buch: Abschnitt 3.15 (Das Prinzip, Was die Norm sagt, Rahmen in Deutschland, Österreich und der Schweiz); Norm: Klauseln 6.2, 6.3, 9.2, 9.3 und 10.1 sowie Maßnahme A.5.4 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Bandes. Rechtsstand des Bandes: 28. September 2026.

Haus		**Zyklus (von / bis)**	
Beitrag für die Bewertung vom		**Auditor/in**	

So nutzen Sie diese Vorlage

1. Legen Sie die Programme und Berichte der drei Jahre nebeneinander und lesen Sie sie als ein einziges Werk. Fragen Sie: Was habe ich noch nie geprüft?
2. Der Beitrag schuldet der Bewertung drei Dinge, und keines ist eine Zahl: erstens die Abdeckung (Teil 1), zweitens die Entwicklung (Teil 2), drittens die anstehenden Entscheidungen (Teil 3), höchstens drei.
3. Hängen Sie die Abdeckungsmatrix im Büro auf, nicht in eine Datei: Ein leerer Bereich an der Wand wird jeden Tag gesehen. Jede Anforderung und jede Maßnahme ohne Kreuz im laufenden Zyklus wandert ohne Diskussion in das Programm des nächsten Jahres.
4. Sitzen Sie bei Ihrem Tagesordnungspunkt im Raum, vor dem Budget. Das Protokoll hält Beschluss, Auftrag und Vertagung auseinander, jeweils mit Datum (Teil 4). Lassen Sie das Auditprogramm einmal im Zyklus von jemand anderem auditieren.

Spalte «Im Buch»: verlangt = von Norm oder Recht verlangt, wie der Band es nennt; Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Die Abdeckung: was über den Zyklus geprüft wurde und was nicht

Nr.	Anforderung oder Maßnahme	Jahr 1	Jahr 2	Jahr 3	Kein Kreuz: ins nächste Programm

Ein Kreuz, wo geprüft wurde; eine Seite, eine Stunde. Nicht die Zahl der Kreuze enttäuscht, sondern ihre Verteilung: Sie stehen in Reihen, und die Zwischenräume sind leer. Im Fall des Bandes waren über den Zyklus nie geprüft worden: der Kontext und die interessierten Parteien, die Kommunikation, die Planung von Änderungen, die Bewertung der Wirksamkeit von Maßnahmen und die Managementbewertung selbst. Wer häufig geprüft wird, gilt im Haus als problematisch, wer nie geprüft wird, als unauffällig: beides ist eine Folge der Programmwahl. Kennzahl: Zahl der Anforderungen ohne Kreuz im laufenden Zyklus; am Ende des Zyklus muss sie null betragen: _____ .

2 Die Entwicklung: drei Reihen über drei Jahre

Reihe	Jahr 1	Jahr 2	Jahr 3	Grund (aus dem Band)	Im Buch
Feststellungen, die sich wiederholen				Die aussagekräftigste Linie, weil sie das einzige Maß dafür ist, ob ein System lernt.	**Methode** dieses Bandes.
Dauer, die Punkte offen bleiben				Zahlen aus einem Jahr sagen nichts; dieselben Zahlen über drei Jahre sagen viel.	**Methode** dieses Bandes.
Maßnahmen, die nach ihrer Umsetzung noch einmal geprüft wurden				Ein Haus, dessen Feststellungen jedes Jahr andere sind, spricht für Fortschritte; sind sie jedes Jahr dieselben, ist zu prüfen, ob die Maßnahmen das Problem trafen.	**Methode** dieses Bandes.

3 Die Entscheidungen: höchstens drei Zeilen

Nr.	Frage, mit Ja oder Nein zu beantworten	Folge bei Ja	Folge bei Nein	Wer entscheidet

Nr.	Frage, mit Ja oder Nein zu beantworten	Folge bei Ja	Folge bei Nein	Wer entscheidet

Die Begrenzung auf drei ist eine Zumutung an die Auditorin: Sie zwingt zu einer Rangfolge, und eine Rangfolge ist ein fachliches Urteil, für das man einsteht. Wer achtzehn Feststellungen vorlegt, bekommt eine Kenntnisnahme; wer drei Entscheidungen vorbereitet, bekommt drei Antworten. Die Entscheidungsvorlage ist in der Bewertung kürzer als die Seite für die Eigentümerschaft aus Abschnitt 3.13.

4 Das Protokoll: Beschluss, Auftrag, Vertagung

Punkt	Art (Beschluss · Auftrag · Vertagung)	Datum	Verantwortlicher	Betrag	Grund bei Vertagung, nächste Vorlage

Ein Beschluss ist eine Entscheidung mit Wirkung; ein Auftrag die Anweisung, eine Entscheidung vorzubereiten; eine Vertagung die bewusste Verschiebung mit Grund und Datum. Was nicht beschlossen wurde, gehört ebenfalls hinein, mit dem Grund. «Zur Kenntnis genommen» ist keine gültige Erledigung. Beispiel des Bandes: «Vertagt wegen Umbau des Tagungsbereichs, erneute Vorlage im Folgejahr» ist die Beschreibung einer Abwägung.

5 Prüffragen

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
1	Welcher Satz steht in den Protokollen der letzten drei Managementbewertungen zum internen Audit? Ist er jedes Jahr derselbe? _____	In Bern stand dreimal: «Der Bericht der internen Auditorin wurde zur Kenntnis genommen.» Keine Entscheidung, keine Ressource, keine Frist, kein Auftrag. Das Protokoll ist der einzige Teil der Bewertung, der das Jahr überdauert.	**Methode** dieses Bandes.
2	Folgen aus der Bewertung Entscheidungen zu Verbesserungsmöglichkeiten und zu Änderungsbedarf am System? _____	Eine Bewertung ohne Ergebnisse erfüllt den Abschnitt nicht: Die Eingaben werden sorgfältig zusammengestellt, weil sie sich abhaken lassen; die Ergebnisse werden vergessen, weil sie Arbeit im Raum verlangen.	**verlangt:** Managementbewertung mit festgelegten Eingaben und mit Ergebnissen: Entscheidungen zu Verbesserungsmöglichkeiten und zu Änderungsbedarf (9.3).
3	Sind die Eingaben vollständig? (Status von Maßnahmen vorheriger Bewertungen · Änderungen bei externen und internen Themen · Rückmeldungen interessierter Parteien · Auditergebnisse · Erfüllung von Zielen) (Beitrag des Audits zu jeder Eingabe) _____	Der Band nennt diese Eingaben ausdrücklich; die Liste ist nicht abschließend («darunter»).	**verlangt:** Eingaben der Managementbewertung (9.3).
4	Berücksichtigt das Programm die Bedeutung der Prozesse und die Ergebnisse vorheriger Audits, mit Bezug auf das vorhergehende Programm? Ist die Auswahl begründet? _____	Ein Programm, das drei Jahre lang gleich lautet, ist ein Prüfhinweis: Es erfüllt beide Wendungen nur, wenn die gleiche Auswahl jedes Jahr begründet ist und die Ergebnisse der Vorjahre erkennbar berücksichtigt wurden. Nach drei Jahren beschreibt es sonst die Gewohnheit der Auditorin.	**verlangt:** Auditprogramm: Häufigkeit, Methoden, Verantwortlichkeiten, Planungsanforderungen, Berichterstattung; Bedeutung der Prozesse und Ergebnisse vorheriger Audits berücksichtigen (9.2).
5	Wurden die Änderungen des Hauses neben die Bestätigung gelegt, Risiken und Ziele seien weiterhin angemessen? (Cloud, Schließanlage, digitale Gästemappe, IT-Dienstleister) _____	Vier wesentliche Änderungen in drei Jahren sind für ein Hotel dieser Größe viel; in den Bewertungen war von ihnen nirgends die Rede. Gleichlautende Texte beweisen für sich nichts; ein Satz, der nicht geprüft werden kann, ist keine Feststellung, sondern eine Überschrift.	**verlangt:** Informationssicherheitsziele überwacht, kommuniziert, bei Bedarf aktualisiert (6.2); Änderungen am Managementsystem geplant durchführen (6.3).
6	Stützt sich die Aussage zur Verbesserung auf benennbare Veränderungen? _____	Verbesserung ist kein Zustand, den man behauptet, sondern eine Folge von Veränderungen, die sich benennen lassen. Wo drei Jahre dieselben Sätze protokolliert werden, fehlt der Nachweis.	**verlangt:** Fortlaufende Verbesserung der Eignung, Angemessenheit und Wirksamkeit (10.1).
7	Ist der Beitrag eine Entscheidungsvorlage oder eine Folie mit Zahlen? _____	Eine Folie mit Zahlen ist eine Statusmeldung; auf gute Nachrichten (fünfzehn von achtzehn Feststellungen geschlossen) folgt kein Beschluss. Gefragt ist: Was wissen wir jetzt, was wir vorher nicht wussten, und was ist zu entscheiden?	**Methode** dieses Bandes.
8	Ist die Auditorin bei ihrem Tagesordnungspunkt im Raum, und steht er vor dem Budget? _____	Wer nicht im Raum ist, kann nicht gefragt werden; ein Beitrag, der nur als Dokument erscheint, wird wie ein Dokument behandelt. In Bern stand das Audit an neunter Stelle von elf, nach dem Budget. Entscheidungen kosten Geld; ein Budget, das ohne sie beschlossen wurde, macht sie für ein weiteres Jahr unmöglich.	**Methode** dieses Bandes.
9	Auf welcher Ebene wird bewertet, im Haus oder in der Gruppe? Welche Punkte gehen an die Gruppe, und wann werden sie dort behandelt? _____	Eine Gruppenbewertung ersetzt die Bewertung im Haus nicht, wenn die Häuser eigene Gesellschaften sind; eine Bewertung im Haus ist wertlos, wenn die Entscheidungen in der Gruppe fallen. In Bern betraf das die Verträge mit dem IT-Dienstleister und Investitionen oberhalb eines festgelegten Betrags.	**Methode** dieses Bandes.
10	Wurde das Auditprogramm selbst auditiert, von jemand anderem, einmal im Zyklus? _____	Das Auditprogramm ist ein Prozess des Managementsystems. In kleinen Gesellschaften tauschen die Häuser die Auditoren: zwei Tage, und es findet regelmäßig mehr als jede externe Prüfung. In Thun: Die Nachverfolgung bestand aus der Bestätigung der Abteilung und keiner eigenen Prüfung.	**Methode** dieses Bandes.
11	Wird die Zahl der Entscheidungen je Bewertung und die Zahl der zum zweiten oder dritten Mal vorgelegten Punkte geführt und in die nächste Bewertung genommen? _____	Beide Zahlen gehören in die nächste Bewertung; eine vertagte Zeile taucht im nächsten Jahr wieder auf.	**Methode** dieses Bandes.
12	Sagt der Bericht, dass die Zahl der Feststellungen die Güte des Audits nicht misst? _____	Ein Audit ohne Nichtkonformitäten kann gut sein, wenn die Kriterien geeignet, die Nachweise ausreichend und die Schlussfolgerungen nachvollziehbar sind; eine Quote an Mängeln ist kein Maßstab. Im Sinne der Auditterminologie gehört auch die festgestellte Konformität zu den Ergebnissen.	**Methode** dieses Bandes.

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
13	Wie lange werden die Protokolle aufbewahrt? _____	Sie sind dokumentierte Information im Sinne der Norm. Maßgeblich ist der Zertifizierungszyklus und im Streitfall die Verjährung von Ansprüchen; in der Praxis hat sich bewährt, sie unbefristet zu behalten, weil ihr Umfang gering ist und ihr Wert mit der Zeit steigt (nicht verlangt).	**Methode** dieses Bandes.

Recht laut Band. Die Managementbewertung ist in keinem der drei Länder rechtlich vorgeschrieben; verlangt wird sie von der Norm. Sie zeigt im Ernstfall, was die Leitung wusste und was sie daraufhin entschied; ein Protokoll mit «zur Kenntnis genommen» belegt zugleich, dass die Lücke bekannt war und keine Handlung auslöste. Die Datenschutz-Grundverordnung macht den Verantwortlichen für den Nachweis zuständig und berücksichtigt bei Geldbußen Vorsatz oder Fahrlässigkeit und ergriffene Maßnahmen; Schweiz: revidiertes Datenschutzgesetz (in Kraft seit 1. September 2023). Die Regelungen zur Netz- und Informationssicherheit siedeln die Verantwortung bei der Leitung an; deren Stand ist vor Anwendung im Einzelfall zu prüfen. Geschäftsleitung und Geschäftsführung: Sorgfaltspflichten nach schweizerischem, deutschem und österreichischem Gesellschaftsrecht in den Grundzügen; verlangt wird eine nachvollziehbare Auseinandersetzung mit bekannten Risiken. Rechtsstand des Bandes: 28. September 2026.

Häufige Fehler (aus dem Band)

Nr.	Fehler	Was der Band daraus macht
1	Das vererbte Programm	Ein Programm, über das niemand klagt, ist in den meisten Häusern ein Programm, das nichts Neues mehr berührt.
2	Die fehlende Abdeckung über den Zyklus	Ohne Matrix entstehen weiße Flecken, die niemand bemerkt, weil jedes einzelne Jahr vollständig aussieht; was nie geprüft wird, wird nie korrigiert.
3	Häufung mit Bedeutung verwechselt	Drei Viertel der Feststellungen betrafen drei Bereiche: ein Spiegel des Programms, keine Diagnose. Man findet dort, wo man sucht.
4	Die Form des Beitrags	Eine Folie mit Zahlen befriedigt das Bedürfnis nach einem Ergebnis, ohne eine Frage zu stellen.
5	Die Sprache des Protokolls	«Zur Kenntnis genommen» ist das Eingeständnis, dass nichts folgt.
6	Angemessenheit ohne Prüfung bestätigt	Dreimal derselbe Text im Formular, ohne dass die Änderungen des Hauses danebengelegt wurden.
7	Die Auditorin ist nicht im Raum	Die Reihenfolge einer Tagesordnung ist eine Aussage über Bedeutung.
8	Die Bewertung auf einen halben Tag verlängert	In Thun wurde sie zur Veranstaltung mit Präsentationen und ohne Beschlüsse; Länge erzeugt keine Entscheidungen, Vorbereitung tut es.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch das Recht oder die Regelwerke, die für Ihr Haus gelten. Ein ausgefülltes Blatt ist kein Nachweis: Es zeigt, dass jemand hingesehen hat, nicht dass der Zustand besteht, den es beschreibt. Sie ersetzt weder die Managementbewertung noch deren Protokoll und trifft keine Entscheidung: Das Audit liefert den Anlass, die Bewertung trifft die Wahl. Sie legt keine Zahl von Feststellungen als Maßstab fest, und die Zahl der Auditorentage bleibt Sache des Auditprogramms. Rechtsstand des Bandes: 28. September 2026.