VORLAGE ZU ABSCHNITT 3.13 DES BANDES 5B

Die Seite für die Eigentümerschaft

Der Bericht, den die Eigentümerschaft liest: eine Seite, höchstens fünf Zeilen, vier Spalten, und die Liste der Zusagen, die sie verbindet.

Kategorie: Vorlage (Bericht). Bezug im Buch: Abschnitt 3.13 (Das Prinzip, Was die Norm sagt, Rahmen in Deutschland, Österreich und der Schweiz); Norm: Klauseln 5.1, 7.4, 9.2 und 9.3 sowie Maßnahmen A.5.4, A.5.19 und A.5.31 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Bandes. Rechtsstand des Bandes: 28. September 2026.

Haus		**Nummer und Datum dieser Seite**	
Berichtszeitraum		**Abgestimmt mit der Leitung am**	

Die Entscheidungsseite

Nr.	Die Sache in einem Satz (beginnt mit dem, was passieren kann, nicht mit dem, was fehlt)	Die mögliche Folge in einer Größenordnung (Umsatz, Tage, Datensätze)	Die notwendige Entscheidung (keine Empfehlung)	Wer entscheidet

Weitergabe an die Eigentümerschaft bestätigt von		**am**	
Nummerierte Empfänger		**Ablage**	

Keine Klauselnummern, keine Reifegrade, keine Farben: eine Zeile je Thema, das jemanden außerhalb des Hauses etwas angeht. Die Seite enthält keine Empfehlung, was zu tun ist, sondern die Entscheidung, die ansteht: Eine Entscheidung muss man treffen oder ausdrücklich vertagen. Sie hat ein Datum und eine Nummer und wird nicht überschrieben; nach vier Quartalen sieht man auf einen Blick, welche Zeile zum vierten Mal dasteht. Der vollständige Teil für den Betrieb bleibt, mit Verweis, wo jedes Thema ausführlich steht; der Nachweis der Vollständigkeit steht in einer Tabelle im Anhang.

So nutzen Sie diese Vorlage

1. Nehmen Sie den letzten Auditbericht und markieren Sie die drei Feststellungen, die eine Entscheidung außerhalb des Hauses verlangen. Besorgen Sie für jede eine Größenordnung: fünf Minuten am Telefon mit der kaufmännischen Leitung genügen.
2. Fragen Sie: Wie viel Umsatz hängt an diesem Kunden? Was kostet ein Tag ohne dieses System? Wie viele Datensätze wären betroffen? Schreiben Sie jede Zeile so, dass sie mit dem beginnt, was passieren kann.
3. Stimmen Sie die Seite mit der Leitung ab, bevor der Bericht hinausgeht: Die Entscheidung, was auf die Seite kommt, ist selbst eine Bewertung, für die der Auditor geradesteht. Die Seite geht auf dem Weg der Leitung, nicht daran vorbei; verlangen Sie die Bestätigung der Weitergabe und legen Sie sie in die Akte.
4. Legen Sie die Seite der Quartalsunterlage bei, in der die Eigentümerschaft ohnehin liest, nicht dem Jahresbericht unter acht anderen Anhängen. Wo die Eigentümerschaft es nicht wissen will, geht die Seite an die Geschäftsführung des Betreibers.

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

Prüffragen vor dem Versand

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
1	Beginnt jede Zeile mit dem, was passieren kann? Steht in jeder Zeile eine Größenordnung? _____	Nicht «keine Zwei-Faktor-Authentisierung für Teilnehmerlisten», sondern: «Ein Konto mit Zugriff auf Teilnehmerlisten kann ohne zweiten Faktor übernommen werden; betroffen wären bis zu neuntausend Datensätze und ein Kunde mit elf Prozent Umsatzanteil.» Die zweite Fassung ist länger und wird gelesen.	**Methode** dieses Bandes.
2	Trennt der Bericht Konformität und Exposition, und steht nur die Exposition auf der ersten Seite? _____	Konformität ist die Frage, ob das System der Norm entspricht; Exposition ist die Frage, was das Haus treffen kann. Die Eigentümerschaft interessiert sich nicht für Konformität, sondern für Exposition: Was kann uns passieren, was kostet es, und wer entscheidet darüber.	**Methode** dieses Bandes.

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
3	Sind die Feststellungen nach Bedeutung geordnet und nicht nach dem Aufbau der Norm? _____	Die Gliederung nach der Norm sichert Vollständigkeit und stellt Wichtiges und Belangloses nebeneinander: Feststellung neunundzwanzig stand auf Seite einundvierzig, zwischen der Beschriftung eines Serverschranks und der Aufbewahrung von Besucherausweisen.	**Methode** dieses Bandes.
4	Ist die Seite an die relevante Leitung gegangen, die über die Ressourcen verfügt, um zu handeln? _____	«Relevant» ist das entscheidende Wort. Der Auditor berichtet an die Leitung, die ihn beauftragt hat, nicht an die Eigentümerschaft an ihr vorbei; sonst bleibt er im nächsten Jahr ohne Zugang.	**verlangt:** Ergebnisse der Audits der relevanten Leitung berichten (9.2).
5	Sind Inhalt, Empfänger und Rhythmus der Berichtslinie festgelegt, oder hängt es davon ab, wer gerade einen Anhang weiterleitet? _____	Die Berichtslinie zur Eigentümerschaft braucht festgelegten Inhalt, Empfänger und Rhythmus. Wo der Managementvertrag Informationssicherheit nicht nennt, entscheidet der Betreiber allein, was die Eigentümerschaft erfährt; eine Vertragszeile genügt: einmal jährlich Bericht mit Angabe offener Entscheidungen.	**verlangt:** Festlegen, worüber, wann, mit wem und wie kommuniziert wird (7.4).
6	Berücksichtigt das Auditprogramm die Bedeutung der Prozesse und die Ergebnisse vorheriger Audits, und ist das erkennbar? _____	Ein Programm, das jedes Jahr denselben Umfang mit derselben Gewichtung und Berichtsform verwendet, ist ein Prüfhinweis; ohne begründete Auswahl kann ein Zertifizierungsauditor eine Feststellung gegen das interne Auditprogramm selbst schreiben.	**verlangt:** Auditprogramm berücksichtigt Bedeutung der Prozesse und Ergebnisse vorheriger Audits (9.2).
7	Welche Frist hat die Nachverfolgung zu den Feststellungen, und ist der Nachverfolgungsbericht nach Bedeutung sortiert? _____	Die Frist von neunzig Tagen für Feststellung neunundzwanzig verstrich, weil der Nachverfolgungsbericht nach Normabschnitten sortiert war und die offenen Punkte über achtzig Seiten verteilte. Zwischen Feststellung und Behebung sollen keine Monate verstreichen.	**Methode** dieses Bandes.
8	Wer unterschreibt Lieferantenfragebögen? Laufen sie vor der Unterschrift durch die Informationssicherheit? _____	Der Fragebogen war im Vertrieb ausgefüllt worden, ohne die Informationssicherheit. Ein ausgefüllter und unterschriebener Fragebogen ist Vertragsinhalt, seine Verletzung eine Vertragsverletzung. Im Fall: Unterschrift durch die Direktion nach Gegenzeichnung der Informationssicherheit.	**verlangt:** Zusicherungen gegenüber Kunden sind Vertragsinhalt (Vertragsrecht); Informationssicherheit in Lieferantenbeziehungen (A.5.19).
9	Enthalten unterschriebene Fragebögen Prüfrechte des Kunden? _____	Wer sie unterschreibt, akzeptiert unter Umständen, dass der Kunde oder ein von ihm Beauftragter das Haus prüft; ein Verband mit medizinischen Teilnehmerdaten prüft ernsthaft. Im Fall hatte das Haus zwei Kunden, die jederzeit hätten prüfen dürfen.	**Methode** dieses Bandes.
10	Wer ist bei Kongressen mit Gesundheitsbezug Verantwortlicher, wer Auftragsverarbeiter, und liegt der Vertrag darüber vor? _____	Verantwortlich ist zunächst der Verband, das Haus in der Regel Auftragsverarbeiter; der Vertrag liegt oft nicht vor, weil beide Seiten den anderen für zuständig halten.	**verlangt:** Rollenverteilung nach Datenschutz-Grundverordnung beziehungsweise revidiertem Datenschutzgesetz, im Einzelfall zu bestimmen und vertraglich festzuhalten.
11	Geht die Liste der Zusagen in die Managementbewertung, und wie viele davon wurden im Berichtszeitraum belegt oder zurückgenommen? _____	Die Bewertung enthält fast überall Auditergebnisse und fast nirgends Kundenzusagen, obwohl Rückmeldungen interessierter Parteien verlangt sind; ein Lieferantenfragebogen eines Großkunden ist eine solche Rückmeldung. Kennzahl: die Zahl der Zusagen ohne Nachweis.	**verlangt:** Managementbewertung mit bestimmten Eingaben, darunter Auditergebnisse, Rückmeldungen interessierter Parteien, Wirksamkeit von Maßnahmen zur Behandlung von Risiken (9.3).
12	Trifft die Leitung Entscheidungen, die dokumentiert sind? Sind Vertagungen sichtbar? _____	Die häufigste Feststellung eines erfahrenen Zertifizierungsauditors lautet nicht «keine Bewertung durchgeführt», sondern «keine Entscheidungen erkennbar». Eine Leitung, die nicht erfährt, was auf dem Spiel steht, kann Ressourcen und Wirkung nicht sicherstellen.	**verlangt:** Führung und Verpflichtung der obersten Leitung (5.1); Verantwortung der Leitung (A.5.4).
13	Ist die Seite vertraulich behandelt: nummerierte Empfänger, keine Sammelverteiler, Ablage im Direktionsbereich? _____	Eine Seite mit Beträgen und Kundennamen darf nicht in Umlauf geraten. Zahlen wegzulassen löst das Problem nicht, sondern nur die Wirkung.	**Methode** dieses Bandes.

Die Liste der Zusagen an Kunden

Nr.	Kunde	Wer hat was zugesagt (Aussage)	Wann, in welchem Dokument	Womit belegt	Stand (belegt · in Umsetzung, Termin · zurückgenommen)

Die Zusagen gehören in dieselbe Liste wie rechtliche Verpflichtungen und werden im Audit genauso behandelt: Wer hat was zugesagt, wann, in welchem Dokument, und womit wird es belegt? Kein Audit kann ohne diese Liste prüfen, ob sie eingehalten werden, und kein Vertrieb weiß, was er schon versprochen hat. Der Band nennt als typische Zusicherungen neun Punkte, die ein Haus einmal ehrlich beantwortet und belegt haben sollte (jeder mit: belegt, oder: in Umsetzung mit Termin):

Nr.	Typische Zusicherung in Lieferantenfragebögen	Belegt (Nachweis)	In Umsetzung (Termin)
1	Verschlüsselung im Ruhezustand und bei der Übertragung		
2	Mehrfaktoranmeldung		
3	Protokollierung und Aufbewahrung		
4	Löschfristen		
5	Jährliche Tests		
6	Schulung		
7	Meldefristen bei Vorfällen		
8	Unterauftragnehmerlisten		

Nr.	Typische Zusicherung in Lieferantenfragebögen	Belegt (Nachweis)	In Umsetzung (Termin)
9	Recht auf Prüfung		

Ein Haus, das drei Punkte ehrlich mit «in Umsetzung, Termin Quartal drei» beantwortet, bleibt im Rennen; ein Haus, das vier Punkte bejaht und keinen belegen kann, fliegt beim ersten Nachweisverlangen heraus. Der Verband kündigte nicht wegen der fehlenden Maßnahmen, sondern wegen der Diskrepanz. Rechtsstand des Bandes: 28. September 2026.

Häufige Fehler (aus dem Band)

Nr.	Fehler	Was der Band daraus macht
1	Die Gliederung nach der Norm	Für den Prüfer bequem, weil sie Vollständigkeit sichert, und für jeden Leser unbrauchbar.
2	Vollständigkeit erzeugt Abstumpfung	Wer jedes Jahr vierzig Feststellungen bekommt, von denen achtunddreißig belanglos sind, behandelt den Bericht als Rauschen.
3	Die Gleichbehandlung der Feststellungen	Einundvierzig Punkte in einer Liste: Eine war geschäftsrelevant, vierzig waren Hygiene.
4	Die Zusammenfassung in der Sprache der Konformität	«Wirksam, keine Hauptabweichung» sagt der Eigentümerschaft nichts über ihre Exposition.
5	Das Fehlen von Beträgen	Wer eine Sache ohne Größenordnung beschreibt, überlässt die Einschätzung dem Leser, und der Leser hat sie nicht.
6	Die Empfängerlogik	Die Betriebsleitung braucht alle Punkte; die Eigentümerschaft drei Sätze und eine Entscheidung.
7	Der Fragebogen im Vertrieb	Er kommt als Verkaufsunterlage an; dort entstehen Zusagen, die das eigene System nicht deckt.
8	Keine Verbindung zwischen Zusage und Nachweis	Niemand führte eine Liste der Zusicherungen an Kunden; die beiden Berichtswege (Vertrieb, Informationssicherheit) kreuzten sich nirgends.
9	Die Frequenz	Einmal im Jahr als Anhang unter acht anderen: Der Bericht konkurriert mit allem anderen.
10	Das Ampelblatt	In Braunschweig stand ein Blatt mit fünfzehn Kennzahlen vor jedem Bericht; Farben ohne Beträge sind eine Meinung.

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 ist kein Ersatz für den vollständigen Auditbericht und bewertet nicht die Bedeutung eines Themas für das Unternehmen: Das tut die Leitung. Die Größenordnungen sind Angaben der kaufmännischen Leitung, keine Berechnung des Auditors. Die Seite ist keine Vertragsvorlage; die Wirkung von Zusicherungen richtet sich nach dem jeweiligen Vertragsrecht. Rechtsstand des Bandes: 28. September 2026.