Der Prüfbericht über die Dienstleistungsorganisation

Was zu lesen ist, bevor man ihn ablegt, und die vier Dokumente, die nebeneinander gehören: eine Stunde statt eines Fragebogens mit Ja.

Kategorie: Checkliste. Bezug im Buch: Abschnitt 3.7 (Das Problem, Das Prinzip, Was die Norm sagt, Verifikationsnotiz); Norm: Klauseln 4.2, 5.3, 6.1.2 und 8.1 sowie Maßnahmen A.5.19 bis A.5.23 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Bandes. Rechtsstand des Bandes: 28. September 2026.

Haus		**Stand (Datum)**	
Anbieter und Dienst		**Geprüft von**	

So nutzen Sie diese Vorlage

1. Legen Sie vier Dokumente nebeneinander: die Zertifikatsurkunde mit ihrem Geltungsbereich, den Vertrag samt Anlagen, die Liste der Unterauftragnehmer und die letzte Störungsmeldung. Vier Dokumente, eine Stunde; die meisten Lücken zeigen sich im Vergleich, nicht in der Einzelprüfung.
2. Lesen Sie den Prüfbericht, bevor Sie ihn ablegen, und tragen Sie drei Angaben in die eigene Akte ein: geprüfter Zeitraum, Umfang, Ausnahmen oder Einschränkungen. Bei Auffälligkeiten holen Sie Rat.
3. Fragen Sie so, dass ein Dokument antwortet, nicht ein Ja. Wer nach vier Wochen keine Unterlagen hat, hat ein Ergebnis: Die Abhängigkeit ist unbelegt. Es gehört in die Risikobeurteilung und in die Managementbewertung, nicht in eine Mahnung.
4. Legen Sie die Prüfung des wichtigsten Lieferanten sechs Wochen vor die Kündigungsfrist des Vertrags, nicht irgendwann ins Jahr.

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

1 Der Prüfbericht: drei Angaben für die eigene Akte

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
1	Welcher Zeitraum wurde geprüft? _____	Die Aussagekraft eines Berichts über eine Dienstleistungsorganisation hängt vom geprüften Zeitraum und vom Prüfumfang ab; solche Berichte werden üblicherweise nach ISAE 3402 oder als SOC-2-Bericht erstellt.	**Methode** dieses Bandes.
2	Welcher Umfang wurde geprüft? Umfasst er den betriebenen Dienst (Betrieb der Plattform, Hosting, Rechenzentrum)? _____	In Linz umfasste das Zertifikat die Entwicklung am Firmensitz, nicht den Betrieb: echt, gültig, akkreditiert, und ohne Aussage über den Teil, der ausfiel.	**Methode** dieses Bandes.
3	Enthält der Bericht Ausnahmen oder Einschränkungen? (Was wurde nicht geprüft?) _____	Ein Hotelkoordinator muss den Bericht nicht fachlich bewerten; drei Angaben genügen. In der Karte des Abschnitts markiert die Fahne die Ausnahme: Rückspieltests von Kundendatenbanken waren nicht durchgeführt worden.	**Methode** dieses Bandes.
4	Auffälligkeit festgestellt? Bei wem wurde Rat geholt? _____	Wer die drei Punkte notiert und bei Auffälligkeiten Rat holt, hat mehr getan als neun von zehn Häusern.	**Methode** dieses Bandes.
5	Legt der Anbieter den unabhängigen Prüfbericht einmal jährlich vor? Wenn nicht: Wie wird der Nachweis sonst geführt (zum Beispiel Zertifikat des Rechenzentrumsbetreibers, dessen Geltungsbereich den Betrieb umfasst)? _____	Wenn er keinen hat, ist das keine Katastrophe, aber eine Information. Das Prüfrecht steht im Vertrag und wird selten genutzt.	**Methode** dieses Bandes.

2 Die vier Dokumente nebeneinander

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
6	Was genau ist zertifiziert? (Geltungsbereich der Urkunde, nicht die Überschrift) _____	Ein Zertifikat beantwortet «was wurde geprüft», nicht «ist mein Teil dabei». Das Risiko liegt meist in dem Teil, den das Zertifikat nicht erwähnt.	**verlangt:** Steuerung extern bereitgestellter Prozesse, Produkte und Dienstleistungen (8.1); «gesteuert» heißt nicht «eingekauft».
7	Wer steht hinter dem Anbieter? (Unterauftragnehmer in der Anlage zum Vertrag; wer betreibt das Rechenzentrum?) Wurde die Genehmigung gelesen, die das Haus erteilt hat? _____	Zwischen Hotel und Gästedaten standen zwei Unternehmen, das zweite im Haus namentlich unbekannt. Die Genehmigung in der Anlage war eine Entscheidung; wer sie nicht liest, entscheidet trotzdem, nur ohne es zu wissen.	**verlangt:** Maßnahme A.5.21 (Lieferkette der Informations- und Kommunikationstechnik: der Blick hinter den direkten Lieferanten); Unterauftragnehmer nur mit Genehmigung, der Auftragsverarbeiter haftet (Datenschutz-Grundverordnung).
8	Welche Zusagen enthalten Vertrag und Anlagen zu Sicherheitsmaßnahmen, Verfügbarkeit und Rückgabe der Daten am Vertragsende? _____	Der Vertrag ist selten das Problem, die Anlagen sind es: Dort steht, was der Betrieb spürt.	**verlangt:** Vertrag mit bestimmtem Inhalt, darunter Sicherheitsmaßnahmen, Löschung oder Rückgabe am Ende, Nachweise und Duldung von Prüfungen (Datenschutz-Grundverordnung); Schweiz: revidiertes Datenschutzgesetz.
9	Was sagt die letzte Störungsmeldung über Ursache, Sicherung und Überwachung? (zum Beispiel: Alarm in einem Postfach, das niemand liest) _____	Der Linzer Bericht nannte ein Stromereignis, ein fehlerhaftes Umschalten, einen Sicherungslauf, der seit sechs Wochen nur teilweise lief, und einen Alarm im ungelesenen Postfach.	**Methode** dieses Bandes.
10	Stehen die vier Fragen beantwortet da: Wo liegen die Sicherungen? Stehen sie in einem zweiten Rechenzentrum? Wie oft wird die Wiederherstellung geprobt? Welcher Datenverlust ist zugesagt? (Datum der letzten vollständigen Probe · Dauer · Datenverlust) _____	Der Fragebogen fragte «Führen Sie Sicherungen?» und bekam ein wahres Ja. Besser: «Wann haben Sie zuletzt vollständig wiederhergestellt, wie lange dauerte es, welchen Datenverlust hätte es bedeutet?»	**Methode** dieses Bandes.
11	Ist der maximal tolerierbare Datenverlust im Vertrag vereinbart, zusätzlich zum Verfügbarkeitsziel (Stunden)? (Stunden Verfügbarkeit · Stunden Datenverlust) _____	Verfügbarkeit ohne maximal tolerierbaren Datenverlust ist eine halbe Zusage; für ein Hotel ist der Datenverlust der schmerzhaftere Teil. Wer den Wert nicht vereinbart, hat ihn dem Anbieter überlassen.	**Methode** dieses Bandes.
12	Wie viele Menschen beim Anbieter haben Zugriff auf die Datenbank dieses Hauses? _____	Im Haus hätte niemand eine Zahl nennen können; es war auch nie jemand auf die Idee gekommen zu fragen.	**Methode** dieses Bandes.

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
13	Wie viele Ihrer Kunden haben diese Unterlagen im letzten Jahr angefordert? _____	Anbieter, die sie regelmäßig liefern, haben Prozesse dafür; bei Anbietern, bei denen ein Hotel der erste Frager ist, ist die langsame, unvollständige Lieferung selbst eine Information.	**Methode** dieses Bandes.
14	Sitzen Rechenzentrum oder Supportteam außerhalb des Europäischen Wirtschaftsraums? Welche Grundlage besteht, und wurde ihre Wirksamkeit geprüft? (auch Fernwartung) _____	Fernwartung aus einem Drittland ist eine Übermittlung, auch wenn die Daten physisch bleiben, wo sie sind.	**verlangt:** Datenschutz-Grundverordnung (Übermittlung in Drittländer); Schweiz: revidiertes Datenschutzgesetz.

3 Das eigene Haus

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
15	Ist die Maßnahme zur Sicherheit bei der Nutzung von Cloud-Diensten (A.5.23) in der Erklärung zur Anwendbarkeit als anwendbar geführt? _____	Eine Prüfung von zwei Minuten, die oft überrascht: In Häusern, deren System seit Jahren in der Cloud läuft, steht dort häufig «nicht anwendbar», weil die Erklärung aus der Zeit stammt, als das System im Keller stand.	**verlangt:** A.5.23; die Erklärung zur Anwendbarkeit.
16	Welche Person führt Vertrag, Zertifikat, Nachweise und Störungen zusammen? (Name) _____	Der Vertrag gehört dem Einkauf, das Zertifikat der Qualitätsstelle, die Schnittstelle der IT, der Ausfall dem Empfang: Solange niemand für das Ganze zuständig ist, liegt die Lücke zwischen den Teilen.	**verlangt:** Zuständigkeiten zugewiesen (5.3).
17	Kommt das Haus ohne diesen Dienst zwei Stunden aus? Hat er Gästedaten? → Beides Nein: Prüfung alle drei Jahre; eines Ja: jährlich; beides Ja: jährlich mit Nachweisdokumenten. _____	Kein Haus kann alle Lieferanten prüfen; in einem Stadthotel bleiben nach dieser Regel vier bis sechs übrig, nicht vierzig.	**Methode** dieses Bandes.
18	Was kostet ein Tag ohne Kernsystem? (Zahl, eine Stunde mit der Buchhaltung) _____	Ohne diese Zahl gibt es keinen Maßstab für die Frage, wie viel Vorsorge angemessen ist; dann gewinnt jedes Jahr die günstigste Variante.	**Methode** dieses Bandes.
19	Gibt es ein geschriebenes, geprobtes Verfahren für die Rückkehr? (Reihenfolge der Nachführung, benannte Personen: zuerst Anreisen des laufenden Tages, dann Abreisen, dann Zahlungen, dann alles Übrige) _____	Notfallpläne beschreiben fast immer den Ausfall und fast nie die Rückkehr; ein Plan, der bei «System ist wieder da» endet, endet an der teuersten Stelle. Der beste Anbietervertrag ersetzt das Verfahren nicht.	**Methode** dieses Bandes.
20	Wann wurde der Notbetrieb zuletzt geübt? (eine Schicht, angekündigt, ohne Zugriff auf das Verwaltungssystem, danach eine halbe Stunde Auswertung) _____	Ein Notbetrieb, der nie geübt wurde, kostet in den ersten zwei Stunden mehr als der Ausfall selbst.	**Methode** dieses Bandes.
21	Liegt täglich ein Auszug der Reservierungen der nächsten vierzehn Tage im eigenen Haus? _____	Eine Maßnahme des Hauses in Wels: keine Sicherung im technischen Sinn, hätte aber in Linz die Woche Rekonstruktion auf einen Tag verkürzt.	**Methode** dieses Bandes.
22	Prüft jemand das Kernsystem, der nicht den Fragebogen entworfen oder den Vertrag betreut hat? (Name, zum Beispiel Kollege aus einem Schwesterhaus) _____	Wer Fragebogen entwirft und ihn später selbst auditiert, ist in kleinen Häusern unvermeidbar und muss ausgeglichen werden.	**Methode** dieses Bandes.
23	Steht die Verfügbarkeit des Dienstes in der Risikobeurteilung, und wird die unbelegte Abhängigkeit dort geführt? _____	Die Verfügbarkeit eines Cloud-Systems ist der klassische Fall eines Risikos, das außerhalb des Hauses liegt und im Haus wirkt. Ausgelagert ist die Verfügbarkeit, nicht die Verantwortung.	**verlangt:** Beurteilung der Risiken für Vertraulichkeit, Integrität und Verfügbarkeit (6.1.2); Erfordernisse interessierter Parteien, auch der Lieferanten und ihrer Unterauftragnehmer (4.2).

Häufige Fehler (aus dem Band)

Nr.	Fehler	Was der Band daraus macht
1	Zertifikat und Aussage verwechselt	Der Geltungsbereich steht nicht in der Überschrift, sondern im Geltungsbereich, und wird selten gelesen.
2	Den Ansprechpartner gekannt, nicht den Dienstleister	Telefonnummer, Vorname und Reaktionszeit stimmten; die Zahl der Menschen mit Zugriff kannte niemand.
3	Die Kette nicht gesehen	Der Anbieter war nicht der Betreiber; Maßnahme A.5.21 verlangt den Blick hinter den direkten Lieferanten.
4	Ein Fragebogen, auf den man mit Ja antwortet	Fragen, die mit Ja beantwortbar sind, erzeugen Ja; zweiundzwanzig Punkte, vier Jahre nahezu identisch. Ein Audit auf dem Papier ist so gut wie die Unbequemlichkeit seiner Fragen.
5	Den Anbieter geprüft, den man kennt, nicht das Risiko, das man trägt	Fünf Jahre Zuverlässigkeit erzeugen das Vertrauen, das die Prüfung ersetzt.
6	Die zweite Kennzahl fehlt	Der maximal tolerierbare Datenverlust gehört in jeden Vertrag, auch wenn er in keinem Standardfragebogen steht.
7	Wiederherstellbarkeit vertraut, nie geprüft	Sicherungen besitzen und sie zurückspielen können sind zwei Dinge; dazwischen liegen Reihenfolgen, Lizenzen, Schnittstellen und Zeit.
8	Der Notfallplan endet beim Ausfall	Das Nachführen der auf Papier erfassten Vorgänge war nicht beschrieben; dort entstand die Woche Arbeit.

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 bewertet weder Anbieter noch Prüfberichte fachlich und empfiehlt keinen Anbieter. Zertifikat und Prüfbericht antworten auf die Frage, die ihnen gestellt wurde; ob Ihr Teil dabei ist, beantwortet nur diese Prüfung, und nur Sie können sie stellen. Rechtsstand des Bandes: 28. September 2026.