Fragen an einen Penetrationstest

Vor der Beauftragung zu stellen, nicht beim Lesen des Berichts: die Wegekarte, der Prüfumfang und zwei Sätze für den Auftrag.

Kategorie: Checkliste (mit Wegekarte). Bezug im Buch: Abschnitt 3.12 (Das Prinzip, Was die Norm sagt, Rahmen in Deutschland, Österreich und der Schweiz); Norm: Klauseln 4.3, 6.1.2, 8.1 und 9.1 sowie Maßnahmen A.5.19 bis A.5.23, A.8.8, A.8.9, A.8.20 und A.8.22 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Bandes. Rechtsstand des Bandes: 28. September 2026.

Haus		**Stand (Datum)**	
Prüffirma		**Ausgefüllt von**	

So nutzen Sie diese Vorlage

1. Zeichnen Sie zuerst die Wegekarte: ein Blatt, auf dem jeder Weg von außen nach innen steht, mit dem Verantwortlichen daneben. Sie entsteht in einer Stunde mit Haustechnik und Systemkoordination, hält zwei bis drei Jahre und ist die Grundlage jeder Beauftragung. Vergleichen Sie die Zahl der Wege mit dem Prüfumfang der letzten Berichte.
2. Schreiben Sie den Prüfumfang selbst; er gehört dem Haus, nicht dem Prüfer. Schicken Sie die Wegekarte vorab und fragen Sie: Was davon würden Sie zuerst prüfen, und warum?
3. Nehmen Sie in jeden Auftrag die beiden Sätze auf (Teil 2). Räumen Sie vor der Prüfung die Grundeinstellungen auf: Standardkennwörter, offene Verwaltungsoberflächen, veraltete Software, unnötige Zugänge.
4. Lesen Sie jeden Prüfbericht von hinten: Vorn steht, was gefunden wurde; hinten steht, worüber der Bericht nichts sagt. Rotieren Sie über drei Jahre und halten Sie fest, welcher Weg wann geprüft wurde.

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

1 Die Wegekarte und die fünf Grundfragen je Weg

Nr.	Weg von außen nach innen	Wer kommt herein, mit welchem Konto?	Kennwort geändert?	Zweiter Faktor?	Software zuletzt aktualisiert	Verantwortlicher im Haus · beim Lieferanten	Zuletzt geprüft (Jahr)

Wege von außen sind der Teil der Risikolandschaft, den ein Haus am besten kennen kann, weil er endlich und zählbar ist (Beurteilung der Risiken, 6.1.2). Bestandsaufnahme: Die fünf Fragen kosten pro Weg zwanzig Minuten und finden in der Praxis mehr als jeder Test, weil sie die Grundeinstellungen betreffen. Nicht jeder Weg braucht einen Penetrationstest. Zuständigkeit heißt hier nicht Betreuung, sondern Ansprechbarkeit: eine Zeile mit einem Namen, auch für den Aufzug. Beispiele des Bandes (Locarno, elf Wege): Website mit Buchungsstrecke, von einer Agentur betrieben; Mailserver; Wartungszugang des IT-Dienstleisters; Gäste-WLAN; Tagungs-WLAN; Schließanlage mit Fernwartung des Herstellers; Gebäudeleittechnik für Heizung, Lüftung und Spa mit Fernzugang; Zahlungsterminal; Schnittstelle zum Channel Manager; Verwaltungssystem in der Cloud mit Verwaltungsportal; private Geräte der Beschäftigten im Personalnetz. Zwei Wege kamen im Gespräch hinzu: die Agentur mit Zugang zur Website und der Steuerberater mit Zugriff auf die Buchhaltung.

2 Die Beauftragung: zwei Sätze und was zu klären ist

Satz im Auftrag	Im Auftrag enthalten?	Grund (aus dem Band)	Im Buch
«Bitte nennen Sie im Bericht ausdrücklich, was nicht geprüft wurde.»	☐	Er kostet nichts und verändert jeden Bericht. Kein Auftrag ohne diesen Satz.	**Methode** dieses Bandes.
«Bitte prüfen Sie die Behebung der Funde des Vorjahres.»	☐	In zwei der vier Berichte standen Funde mit Empfehlungen; ob sie behoben wurden, prüfte im Folgejahr niemand, weil der Folgetest von vorn begann.	**Methode** dieses Bandes.

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
1	Was ist der Prüfumfang, wer hat ihn geschrieben, und welche Wege der Wegekarte liegen außerhalb? _____	Ohne Wegekarte bestimmt der Anbieter den Prüfumfang, nach dem, was er gut kann und was das Budget hergibt. Was außerhalb liegt, ist nicht «in Ordnung», sondern «nicht betrachtet». In Locarno waren drei von elf Wegen geprüft, vier Jahre lang.	**Methode** dieses Bandes.
2	Hat sich das Haus seit dem letzten Auftrag verändert (System gewechselt, Buchungsstrecke neu aufgesetzt, Gewerk erneuert, Wechsel in die Cloud)? Ist danach geprüft worden? _____	Ein jährlicher Test mit unverändertem Umfang ist ein Prüfhinweis, dass die Festlegung nicht überdacht wurde; er genügt nur, wenn der Umfang begründet ist und sich das Haus nicht verändert hat. Wer ein System wechselt, prüft danach; wer nichts verändert hat, prüft turnusmäßig und rotierend.	**verlangt:** Festlegen, was überwacht und gemessen wird und wann (9.1).
3	Welche Wege stehen zuerst: Wege, über die Zahlungs- oder Gästedaten fließen; dann Wege in das Hausnetz; dann alles Übrige? _____	Nach dieser Regel stehen in einem Stadthotel im ersten Jahr Buchungsstrecke, Verwaltungsportal und Zahlungsterminal an, nicht die Website.	**Methode** dieses Bandes.
4	Rotieren die Wege über drei Jahre, und nennt der Bericht, welcher Weg wann geprüft wurde? _____	Der Nachweis gegenüber einer Zertifizierungsstelle ist damit besser als bei einem jährlichen Test desselben Ausschnitts.	**Methode** dieses Bandes.
5	Wurde vor der Prüfung aufgeräumt? (Standardkennwörter, offene Verwaltungsoberflächen, veraltete Software, unnötige Zugänge) _____	Sonst bezahlt man einen Spezialisten dafür, Dinge zu finden, die eine Checkliste gefunden hätte; in Lugano hatte der Bericht einundsechzig Funde, davon vierundvierzig triviale.	**verlangt:** Konfigurationsmanagement einschließlich Standardkennwörtern und Grundeinstellungen (A.8.9).

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
6	Ist der Auftrag schriftlich mit Umfang, Zeitraum, Ansprechpartnern und Notfallkontakt? Liegt die Zustimmung des Anbieters vor, wo dessen Systeme geprüft werden? _____	Bei Tests der Angreifbarkeit von Beschäftigten über Telefon oder E-Mail sind die arbeitsrechtlichen Regeln des Landes zu beachten.	**verlangt:** Recht des Landes (Rahmen des Abschnitts 3.12).
7	Kommt die Prüffirma einmal durch das Haus, oder läuft alles aus der Ferne? _____	Eine Firma, die durch das Haus geht, sieht die Kodierstation, das offene Netzwerkdöschen im Tagungsraum und den Bildschirm am Empfang, und stellt Fragen, die kein Auftrag enthält.	**Methode** dieses Bandes.
8	Gibt es für jeden Fund: Bewertung, Verantwortlichen, Frist, Nachweis der Behebung? Stehen die Funde im selben Register wie die Vorfälle? _____	Ohne diese vier Felder ist ein Testbericht eine Lektüre. Wer zwei getrennte Listen führt, hat zwei halb gepflegte.	**Methode** dieses Bandes.
9	Ist das Testprogramm ein gesteuerter Prozess mit Umfang, Rhythmus, Auswahl und Nachprüfung, und von der Verwaltung technischer Schwachstellen unterschieden? _____	Ein Test ist eine Momentaufnahme; der Umgang mit Schwachstellen ist ein Prozess aus Erkennen, Bewerten, Beheben und Nachweisen, mit Quellen, Rollen und Fristen. Ein Test kann darin vorkommen, er ist aber nicht der Prozess.	**verlangt:** Steuerung geplanter Prozesse (8.1); Verwaltung technischer Schwachstellen (A.8.8): Informationen beschaffen, Gefährdung bewerten, geeignete Maßnahmen ergreifen.
10	Sind Anwendungsbereich des Managementsystems und Prüfumfang des Tests auseinandergehalten? _____	Der Anwendungsbereich sagt, welche Teile der Organisation das System abdeckt; der Prüfumfang, was eine einzelne Prüfung betrachtet hat. Ein Test im Anwendungsbereich ersetzt keine Aussage über den Anwendungsbereich.	**verlangt:** Anwendungsbereich des Managementsystems (4.3).
11	Fragt die Bestellung bei jedem Gewerk mit Fernwartung: Wer greift von wo zu? Wie wird der Zugang geöffnet und geschlossen? Wer aktualisiert die Software, in welchem Rhythmus, zu welchen Kosten? _____	Diese drei Fragen sind billiger als jede spätere Nachrüstung. Die Bestellung geht nicht hinaus, bevor Zweck, Öffnungsverfahren, Verantwortlicher und Aktualisierungsrhythmus schriftlich festgehalten sind. Im Fall hatte der Hersteller das Wartungskennwort bei der Installation gesetzt und nie geändert; das Handbuch mit der Empfehlung lag acht Jahre im Technikbüro.	**verlangt:** Lieferantenbeziehungen (A.5.19 bis A.5.22); Konfigurationsmanagement (A.8.9).
12	Gibt es eine Tabelle der Lieferanten mit Fernzugang: Lieferant, Zweck, Zugangsart, Öffnungsverfahren, letzte Nutzung? _____	Fünf der elf Wege gehörten Lieferanten, in fünf Verträgen, betreut von drei Abteilungen. Die eine Tabelle hätte den ganzen Fall vorweggenommen.	**Methode** dieses Bandes.
13	Ist das Gäste-WLAN technisch vom Hausnetz getrennt? Sind Verwaltungsportale des Cloud-Systems mit zweitem Faktor gesichert? _____	Das Gäste-WLAN ist der einzige Zugang, den ein Haus Fremden absichtlich gewährt; in der Praxis ist die Trennung in jedem dritten geprüften Haus verletzt, weil ein Drucker, ein Fernseher oder eine Musikanlage «schnell mal» in dasselbe Netz gehängt wurde.	**verlangt:** Netzwerksicherheit und Trennung von Netzen (A.8.20, A.8.22); Sicherheit bei der Nutzung von Cloud-Diensten (A.5.23).
14	Welche Regeln der Kartenindustrie gelten für die Umgebung, in der Kartendaten verarbeitet werden? _____	Sie verlangen unter anderem Netzwerktrennung, geänderte Standardkennwörter und regelmäßige Prüfungen; Verstöße wirken über den Verlust der Akzeptanzvereinbarung. Vertraglicher Natur, in der jeweils geltenden Fassung des Regelwerks zu prüfen.	**verlangt:** Regeln der Kartenindustrie (vertraglich; Fassung zu prüfen).
15	Sind drei Zahlen für die Managementbewertung festgelegt: Zahl der Wege, Anteil der in den letzten drei Jahren geprüften Wege, Zahl der offenen Funde mit überschrittener Frist? _____	Die Wegekarte ist dokumentierte Information und gehört in dieselbe Lenkung wie alles andere: mit Datum, Verantwortlichem und Änderungshistorie.	**Methode** dieses Bandes.

Recht laut Band. Keine Norm und kein Gesetz verlangt einen Penetrationstest; verlangt werden angemessene Maßnahmen und ihre regelmäßige Überprüfung. Schweiz: angemessene technische und organisatorische Maßnahmen, gemessen an Stand der Technik, Zweck und Risiko; die Ausführungsverordnung nennt Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit und verlangt, die Maßnahmen zu überprüfen (revidiertes Datenschutzgesetz). Deutschland und Österreich: Datenschutz-Grundverordnung mit der Pflicht, die Wirksamkeit regelmäßig zu überprüfen, zu bewerten und zu evaluieren. Eine gesetzliche Zahl für die Häufigkeit gibt es nicht. Rechtsstand des Bandes: 28. September 2026.

Häufige Fehler (aus dem Band)

Nr.	Fehler	Was der Band daraus macht
1	Bericht und Aussage über das Haus verwechselt	Ein Prüfbericht sagt etwas über seinen Prüfumfang.
2	Die Wiederholung des Auftrags	Derselbe Auftrag drei Jahre in Folge, weil er im Vorjahr erteilt worden war; niemand fragte, ob sich das Haus verändert hat.
3	Die Zusammenfassung für die Geschäftsleitung	«Keine kritischen Schwachstellen» ist wahr und wird von jedem Leser als Aussage über das Haus verstanden. Der Leser fragt: Sind wir sicher? Der Prüfer antwortet: Was habe ich in diesem Rahmen gefunden?
4	Die fehlende Wegekarte	Ohne die Liste der Wege lässt sich kein Prüfumfang bestimmen.
5	Die Systeme der Gewerke	Schließanlage und Gebäudeleittechnik sind in jedem Haus die am schlechtesten gepflegten Systeme mit der längsten Laufzeit.
6	Test und Schwachstellenmanagement verwechselt	Schwachstellen entstehen täglich; der Prozess aus Erkennen, Bewerten, Beheben und Nachweisen fehlte vollständig.
7	Das Fehlen der Wiederholungsprüfung	Der Folgetest begann von vorn; ob die Funde behoben waren, prüfte niemand.
8	Ein Jahresrhythmus ohne Verbindung zu Änderungen	In vier Jahren hatte sich das Haus erheblich verändert; es gab nur den Jahresrhythmus.
9	Ungeputzt prüfen lassen	Wer ungeputzt prüfen lässt, bezahlt dafür, dass ihm jemand die Staubschicht beschreibt.

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 keine Empfehlung für eine Prüffirma und keine Leistungsbeschreibung für einen Test, und sie ersetzt keinen Penetrationstest. Ein Penetrationstest ist keine Prüfung des Managementsystems und ersetzt kein Audit. Die Wegekarte ist am Tag ihrer Erstellung richtig und ein Jahr später unvollständig. Rechtsstand des Bandes: 28. September 2026.