Die Prüfung der Wiederherstellung

Geprüft wird die Rückkehr, nicht die Sicherung: eine Probe mit Stoppuhr und Protokoll, und die Frage nach dem benutzbaren Zustand.

Kategorie: Arbeitsblatt (mit Protokoll der Probe). Bezug im Buch: Abschnitt 3.10 (Das Prinzip, Was die Norm sagt, Rahmen in Deutschland, Österreich und der Schweiz); Norm: Klauseln 6.1.2, 7.5, 8.1 und 9.1 sowie Maßnahmen A.5.9, A.5.29, A.5.30 und A.8.13 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Bandes. Rechtsstand des Bandes: 28. September 2026.

Haus		**Datum der Probe**	
Beauftragt von (Leitung)		**Auditor (Stoppuhr, Protokoll)**	

So nutzen Sie diese Vorlage

1. Fragen Sie nie, ob gesichert wird. Fragen Sie, wann zuletzt zurückgespielt wurde, und lassen Sie sich das Datum zeigen. Erst messen, dann planen.
2. Schreiben Sie vorher auf, was «arbeitsfähig» heißt. Halten Sie die Liste der gesicherten Systeme gegen die Liste der Systeme, die den Betrieb tragen. Legen Sie fest, wer die Testkopie löscht, wann und womit es nachgewiesen wird.
3. Spielen Sie auf Ersatzhardware oder in einer getrennten Umgebung zurück, in der ruhigsten Woche des Jahres, mit Stoppuhr und Protokoll. Der Auditor führt nicht durch und berät nicht: Er beobachtet und misst.
4. Staffeln Sie den Aufwand: im ersten Jahr die vollständige Probe mit Stoppuhr; in den Folgejahren eine Teilprobe (Datenbank zurückspielen, eine Schnittstelle prüfen); alle drei Jahre wieder vollständig. Am Ende steht eine einseitige Wiederanlaufkarte, gedruckt, an der Rezeption und in der Direktion hinterlegt.

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

1 Vor der Probe

Was heißt «arbeitsfähig»? Der Vorgang	Läuft?	Zeit (Stunden)	Grund (aus dem Band)
Ein Gast kann einchecken.	☐		Solange diese vier Vorgänge nicht laufen, ist das System nicht wiederhergestellt, auch wenn es startet: Die Datenbank ist nicht das System.
Eine Schlüsselkarte wird ausgegeben.	☐		Methode dieses Bandes; Beispiele für ein Hotel.
Eine Rechnung wird erstellt und bezahlt.	☐		
Eine Reservierung aus dem Portal kommt an.	☐		
	☐		Weitere Vorgänge des Hauses.

System (Frage: Was steht still, wenn dieses Gerät fehlt?)	In der Sicherungsliste?	Zuletzt zurückgespielt (Datum)	Eigentümer
Schließanlage (Server der Kodierstationen)			
Kassensysteme der Gastronomie			
Zeiterfassung			
Spa-Buchung			
Digitale Gästemappe			
Telefonanlage			

Die Liste schreibt nicht die IT, sondern die IT gemeinsam mit dem Betrieb. In jedem Hotel finden sich zwei bis vier Systeme, die in keiner Sicherung stehen: Systeme, die nicht wie Computer aussehen, fallen aus der Informationstechnik heraus. Auch die Schließanlage ist ein Wert mit einem Verantwortlichen (A.5.9). Die ersten sechs Zeilen nennt der Band als Beispiele.

2 Das Protokoll der Probe

Datenbank zurückgespielt nach (Stunden)		**Arbeitsfähig nach (Stunden)**	
Im Notfallplan angenommen (Stunden)		**Maximal hinnehmbarer Datenverlust (Stunden)**	

Nr.	Schritt (in der Reihenfolge der Ausführung)	Beginn	Ende	Wer, Telefon	Wo es hakte

Das Protokoll enthält nicht nur Zeiten, sondern die Reihenfolge der Schritte, die Telefonnummern, die verwendeten Passwörter in verschlossener Form und die Stelle, an der es hakte. Aus ihm entsteht in einer Stunde die einseitige Wiederanlaufkarte, die im Ernstfall tatsächlich benutzt wird. Testkopie gelöscht am _____ von _____ , Nachweis: _____

3 Prüffragen

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
1	Wann wurde zuletzt vollständig zurückgespielt, und wie lange dauerte es? (Datum · Stunden bis arbeitsfähig) _____	Die einzige belastbare Aussage über die Wiederherstellbarkeit eines Systems ist die Zeit, die eine echte Wiederherstellung zuletzt gebraucht hat. Alles, was vorher gesagt wurde, auch die Zusagen des Dienstleisters und die Angabe im Notfallplan, ist gegenstandslos. Das ist kein Misstrauen: Verfügbarkeit entsteht erst im Vollzug.	**Methode** dieses Bandes.
2	Sind die beiden Zahlen in Vertrag und Notfallplan festgelegt: die Zeit bis zur Arbeitsfähigkeit und der maximal hinnehmbare Datenverlust? Von der Leitung entschieden? _____	Beide sind Entscheidungen der Leitung, nicht Eigenschaften der Technik: Ein Haus kann entscheiden, dass achtundvierzig Stunden hinnehmbar sind, solange es den Notbetrieb dafür hat. Eine Reaktionszeit ohne Wiederherstellungszeit ist die Zusage, das Problem schnell zur Kenntnis zu nehmen.	**Methode** dieses Bandes.
3	Wurde die Probe vom Auditprogramm angestoßen und von der Leitung beauftragt, nicht vom Dienstleister? _____	Der Dienstleister hat keinen Anlass, der Betrieb keine Zeit. Der interne Auditor kann die Probe verlangen, ohne jemandem Misstrauen auszusprechen: nicht gegen den Dienstleister, sondern für das Haus. Wer sie beauftragt, besitzt auch die Deutung.	**Methode** dieses Bandes.
4	Wo liegen die Lizenzschlüssel, und sind sie ohne Anruf beim Hersteller erreichbar? _____	Im Fall lagen sie beim Hersteller und waren erst am nächsten Vormittag zu bekommen; danach folgten die Schnittstellen. Der Weg zurück führt durch Lizenzen, Schnittstellen, Reihenfolgen und Telefonnummern.	**Methode** dieses Bandes.
5	Wo liegt die Wiederanlaufanleitung? (nicht als Datei im ausgefallenen System) _____	Eine Wiederanlaufanleitung, die als Datei im ausgefallenen System liegt, ist ein Klassiker, in Audits erstaunlich leicht zu finden: Man muss nur fragen, wo sie liegt.	**verlangt:** Dokumentierte Information, die verfügbar sein muss, wenn die Systeme es nicht sind (7.5).
6	Wie viele Kopien liegen auf wie vielen Medien, und liegt eine außer Haus und möglichst nicht dauerhaft erreichbar? (Drei-Zwei-Eins) (Kopien · Medien · Ort) _____	Sicherungen im selben Gebäude sind gegen Festplattenausfall gut, gegen Feuer, Wasser und Verschlüsselungsangriffe nichts wert. Der letzte Halbsatz ist seit den Verschlüsselungsangriffen der wichtigste.	**Methode** dieses Bandes.
7	Läuft die Übertragung der Kopie außer Haus vollständig durch? Hat sich seit der letzten Probe etwas geändert, zum Beispiel die Internetleitung? _____	Nach dem Wechsel der Leitung lief die Kopie ins Rechenzentrum nur noch teilweise durch; der Bericht meldete grün, weil er den lokalen Auftrag bewertete. Änderungen gehen in Hotels durch die Buchhaltung, selten durch ein Änderungsverfahren.	**Methode** dieses Bandes.
8	Wer prüft, ob der Morgenbericht überhaupt noch zugestellt wird? _____	Ein Bericht, der vom Geprüften an den Prüfer geht und von dort in einen Ordner, hat keine Empfängerstelle; in einem Schwesterhaus erreichte er drei Monate lang niemanden, weil die Empfängeradresse nach einem Personalwechsel nicht mehr existierte. Ein grüner Bericht prüft, ob der Auftrag durchgelaufen ist, nicht, ob das Ergebnis brauchbar ist.	**Methode** dieses Bandes.
9	Hängt der Wiederanlauf von einer Person ab? Wie lange dauerte er ohne sie? _____	Ein Wiederanlauf, der von einer Person abhängt, ist ein Wiederanlauf mit einem Urlaubsrisiko.	**Methode** dieses Bandes.
10	Wann war die letzte Schicht im Notbetrieb: ausgedruckte Anreiseliste, Kassenblock, Schlüsselkartencodierung von Hand? Liegen Vordrucke für das Gästeblatt im Schrank? _____	Häuser, die das einmal geübt haben, verlieren die Angst vor dem Ausfall und gewinnen zwei Stunden im Ernstfall. Die melderechtlichen Pflichten bestehen auch bei Ausfall des Systems (Österreich: Gästeblätter weiterführen).	**Methode** dieses Bandes.
11	Wurde die Testkopie gelöscht, mit Regel, Datum und Nachweis? Wo lag sie? _____	Wer eine Wiederherstellung übt, erzeugt eine zweite vollständige Kopie echter Gästedaten. Ohne Regel schafft die Übung das Risiko, das sie mindern soll; die Daten lagen vier Tage auf einer gemieteten Maschine und wurden gelöscht, weil danach gefragt wurde.	**Methode** dieses Bandes.
12	Wird die gemessene Zeit bis zur Arbeitsfähigkeit als Kennzahl geführt, jährlich neu erhoben und in die Managementbewertung genommen? _____	Sie ist die aussagekräftigste Messgröße des Gebiets und von Jahr zu Jahr vergleichbar.	**verlangt:** Festlegen, was überwacht und gemessen wird (9.1); Angaben zur Wirksamkeit für die Managementbewertung.
13	Führt die Erklärung zur Anwendbarkeit die Sicherung als umgesetzt, weil Sicherungen erstellt werden? _____	Die Maßnahme verlangt, dass Sicherungskopien geführt und regelmäßig getestet werden; die Wiederherstellungsprobe ist die Form, die die ISO/IEC 27002 als Hinweis beschreibt. Zu Aufbewahrung und Schutz gibt sie Hinweise, keine zusätzlichen Pflichten.	**verlangt:** Sicherung von Informationen (A.8.13); Informationssicherheit während einer Störung (A.5.29); Bereitschaft der IKT für die Betriebskontinuität (A.5.30).
14	Welche Obliegenheiten verlangt die Cyberversicherung (getestete Sicherungen, Offline- oder unveränderlicher Speicher)? Liegen Testprotokolle vor? _____	Wer im Schadenfall keine Testprotokolle vorlegen kann, riskiert eine Kürzung, in dem Moment, in dem das Geld gebraucht wird. Obliegenheiten sind vertraglich und im Einzelfall zu prüfen.	**Methode** dieses Bandes.
15	Wie hoch ist der Umsatz eines Durchschnittstages in der Hauptsaison, geteilt durch vierundzwanzig? (Größenordnung) _____	Die Größenordnung der Frage, ob vier oder einunddreißig Stunden hinnehmbar sind.	**Methode** dieses Bandes.

Recht laut Band. Die Verordnung nennt Verfügbarkeit und Belastbarkeit der Systeme und die Fähigkeit, Verfügbarkeit und Zugang zu personenbezogenen Daten nach einem Zwischenfall rasch wiederherzustellen; ferner ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen (Datenschutz-Grundverordnung; Deutschland und Österreich unmittelbar). Schweiz: angemessene Datensicherheit mit denselben drei Zielen, die Ausführungsverordnung nennt die Wiederherstellbarkeit ausdrücklich. «Rasch» ist unbestimmt; die gemessene Zeit ist der beste Beleg. Rechtsstand des Bandes: 28. September 2026.

Häufige Fehler (aus dem Band)

Nr.	Fehler	Was der Band daraus macht
1	Sicherung mit Wiederherstellbarkeit verwechselt	Eine Sicherung ist eine Kopie; Wiederherstellbarkeit ist eine Eigenschaft des gesamten Weges zurück.
2	Die Überwachung der Überwachung fehlt	Das Ausbleiben eines Berichts fällt niemandem auf, weil nichts Rotes erscheint.
3	Der grüne Bericht	Er prüft, ob der Auftrag durchgelaufen ist; ob das Ergebnis brauchbar ist, zeigt nur eine Wiederherstellung.
4	Die Systemgrenze	Die Schließanlage war in keiner Sicherung, weil sie in der Vorstellung des Hauses zur Tür gehörte und nicht zur Informationstechnik.

Nr.	Fehler	Was der Band daraus macht
5	Die Zahl im Notfallplan	Vier Stunden waren angenommen, nicht gemessen; die Annahme stammte aus einem Angebot.
6	Die stille Änderung	Der Wechsel der Internetleitung unterbrach die Sicherungskette, weil niemand die Kette aufgezeichnet hatte.
7	Der Aufbewahrungsort	Sicherungen im selben Gebäude sind gegen Feuer, Wasser und Verschlüsselungsangriffe nichts wert.
8	Die Testdaten	Die Übung erzeugt eine zweite vollständige Kopie echter Gästedaten, ohne Regel für ihre Löschung.
9	Der ungeprüfte Notfallplan	Ein ungeprüfter Plan ist in der Wirkung dasselbe wie kein Plan, mit einem Unterschied: Er erzeugt Zuversicht. Der Notfallplan endet zudem beim Ausfall, nicht bei der Rückkehr.
10	Der zu große Plan	In Bad Hofgastein liegt ein Wiederanlaufkonzept mit einundzwanzig Seiten im Ordner und wurde nie geübt; ein einseitiges Blatt, zweimal im Jahr durchgespielt, ist mehr wert.

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 Notfallplan, führt keine Wiederherstellung durch und ersetzt nicht den Beschluss der Leitung über Zeit und Datenverlust. Sie legt weder eine Wiederherstellungszeit noch einen zulässigen Datenverlust fest: Beides entscheidet das Haus. Das Protokoll einer Probe gilt für den Tag der Probe. Rechtsstand des Bandes: 28. September 2026.