

VORLAGE · TOMORIS TOOLBOX

Wiederherstellungstest: Protokollvorlage für Backups und Systeme

Ausfüllbares Protokoll für Datei-, System- und Komplett-Wiederherstellung sowie Offline-Kopien, mit Soll-Ist-Vergleich, Befunden, Freigabe und Jahresplan

STAND

25.10.2026

UMFANG

PDF, 11 Seiten

ONLINE

tomoris.com/downloads/wiederherstellungstest-protokoll

AUF EINEN BLICK

4

Testarten, von der Datei bis zum kompletten Wiederanlauf

RTA

gemessene Wiederanlaufzeit, verglichen mit der RTO

4.2.6

Nr. im DVO-Anhang: Tests von Sicherungen und Redundanzen

12 Mon.

Mindestzeitraum der Jahresübungsplanung (BSI)

FÜR WEN

- IT-Administration und IT-Leitung, die Sicherungen betreiben und deren Wiederherstellung nachweisen wollen
- IT-Dienstleister, die Backups für Kunden betreuen und Tests gemeinsam mit ihnen durchführen
- Notfall- und Informationssicherheitsverantwortliche, die Übungspläne führen
- Geschäftsführung, die Testergebnisse und Maßnahmen freigibt
- Wesentliche und wichtige Einrichtungen, die Tests nach NISG 2026 dokumentieren müssen

WORUM ES GEHT

Eine Sicherung ist erst etwas wert, wenn sie sich zurückspielen lässt. Ob das einwandfrei und in angemessener Zeit gelingt, muss nach dem BSI-Baustein CON.3 regelmäßig getestet werden; für wesentliche und wichtige Einrichtungen sind solche Tests seit Oktober 2026 nach NISG 2026 und dem Anhang der DVO (EU) 2024/2690 Pflicht, samt Dokumentation der Ergebnisse. Diese Vorlage gibt dafür ein Protokoll vor: Testart und Ziel, Vorbedingungen, Ablauf mit Zeitstempeln, erreichte Wiederanlaufzeit und Datenstand gegen RTO und RPO, Integritätsprüfung, Befunde mit Fristen, Freigabe und einen Testplan über das Jahr. Grundlage sind BSI-Standard 200-4, die Bausteine CON.3 und DER.4 sowie NIST SP 800-34.

Diese Vorlage ist an Ihr Unternehmen anzupassen: Testarten, Sollwerte, Häufigkeiten und Zuständigkeiten hängen von Ihren Geschäftsprozessen und Systemen ab. Aufbau und gekennzeichnete Empfehlungen stammen von TOMORIS. Die Vorlage gibt einen Überblick und ersetzt keine Rechtsberatung; maßgeblich ist der Gesetzestext in der jeweils geltenden Fassung.

Nutzung: Diese Vorlage dürfen Sie für den eigenen Gebrauch anpassen; weitergeben dürfen Sie sie nur in unveränderter Form.

INHALT

01	Wiederherstellung testen: Empfehlung und Pflicht	3
02	Vier Testarten	4
03	Begriffe: Sollwerte und gemessene Werte	5
04	Testplan über das Jahr	6
05	Teil A: Testkonzept und Vorbedingungen	7
06	Teil B: Ablauf mit Zeitstempeln	8
07	Teil C: Messung und Integritätsprüfung	9
08	Teil D: Ergebnis, Befunde und Freigabe	10
09	Häufige Fehler	11
10	Quellen	11

01

Wiederherstellung testen: Empfehlung und Pflicht

Warum ein Backup erst mit getesteter Wiederherstellung zählt, wer solche Tests verlangt und wie Sie die Vorlage nutzen.

Dass Daten regelmäßig gesichert werden, gewährleistet nicht automatisch, dass sie sich problemlos wiederherstellen lassen (BSI IT-Grundschutz, Baustein CON.3, Gefährdung 2.2). Der Baustein verlangt deshalb als Basis-Anforderung regelmäßige Tests, ob gesicherte Daten einwandfrei und in angemessener Zeit zurückgespielt werden können (CON.3.A15). Für österreichische Unternehmen ist der IT-Grundschutz eine anerkannte Empfehlung, keine Pflicht. Die Nummern beziehen sich auf das Kompendium Edition 2023. Der Nachfolger Grundschutz++ ist laut BSI ab 1.1.2027 zertifizierbar, der IT-Grundschutz noch bis 30.11.2031; sein Anwenderkatalog führt den Restore-Test als NOT.4.16.1 (SOLLTE, anhand repräsentativer Stichproben). Verbindliche Vorgaben ergeben sich aus dem NISG 2026 und, für personenbezogene Daten, aus der DSGVO:

Wer Wiederherstellungstests verlangt oder empfiehlt

GRUNDLAGE	GILT FÜR	WAS VERLANGT WIRD
§ 32 Abs. 4 lit. c NISG 2026, in Kraft seit 1.10.2026	wesentliche und wichtige Einrichtungen, soweit nicht gleichwertige sektorspezifische EU-Vorgaben gelten (§ 27 NISG 2026; Finanzsektor: DORA, § 4 Abs. 2)	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, als Risikomanagementmaßnahme.
Anhang Nr. 4.2.2, 4.2.3 und 4.2.6 DVO (EU) 2024/2690, unmittelbar oder über § 2 NISV 2026	wesentliche und wichtige Einrichtungen; für die in Art. 1 DVO genannten Anbieter (u. a. Cloud, Rechenzentren, verwaltete Dienste) unmittelbar	Sicherungspläne mit Wiederherstellungszeiten; regelmäßige Integritätsprüfungen; regelmäßige Tests der Wiederherstellung von Sicherungskopien und Redundanzen, die sicherstellen, dass diese zuverlässig sind und alle nötigen Kopien, Verfahren und Kenntnisse abdecken; Ergebnisse dokumentieren, erforderlichenfalls Korrekturmaßnahmen.
Art. 32 Abs. 1 lit. c und d DSGVO	Verantwortliche und Auftragsverarbeiter	Fähigkeit, personenbezogene Daten nach einem Zwischenfall rasch wieder verfügbar zu machen; Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der Maßnahmen.
BSI CON.3.A15 (Basis), DER.4.A1 (Standard), DER.4.A10 (erhöhter Schutzbedarf)	Empfehlung für alle	Restore-Tests regelmäßig (A15); durch Tests und Übungen prüfen, ob die Maßnahmen des Notfallhandbuchs wie vorgesehen funktionieren (A1); bei erhöhtem Schutzbedarf Notfallpläne regelmäßig und anlassbezogen testen, Übungsplan führen (A10).

1

Testplan festlegen

Im Testplan (Abschnitt 04) für mindestens zwölf Monate eintragen, welches System wann mit welcher Testart geprüft wird; die Geschäftsführung gibt ihn frei (BSI-Standard 200-4, Kap. 13.3).

2

Je Test ein Exemplar ausfüllen

Teil A vor dem Test, Teil B währenddessen, Teil C und D danach. Befunde verfolgen Sie bis zum erfolgreichen Nachtest.

Aufbau und Felder sind eine Empfehlung von TOMORIS. Der BSI-Standard 200-4 sieht je Übung Übungskonzept, Übungsprotokoll und Übungsbericht vor und erlaubt, sie in einem Dokument zu sammeln (Kap. 13.2). Ersetzen Sie Platzhalter wie [System], [Name, Funktion] und [Datum] und füllen Sie die Felder „_____“ aus. Die DSGVO nennt den Test nicht ausdrücklich; aus Sicht von TOMORIS ist er ein naheliegender Weg, die Fähigkeit nach lit. c zu überprüfen.

02

Vier Testarten

Von der einzelnen Datei bis zum kompletten Wiederanlauf, dazu die Probe der getrennten Kopie.

Testarten dieser Vorlage und ihre Grundlage

TESTART	WAS GEPRÜFT WIRD	GRUNDLAGE
Datei	Dateien, Ordner oder Datenbestände aus einer Sicherung zurückholen und öffnen: lesbar, vollständig, gewünschter Stand?	Lesbarkeits- und Restorationstests (BSI-Standard 200-4, Tabelle 34, Kap. 13.9.1); CON.3.A15
System	Server, virtuelle Maschine oder Datenbankserver samt Konfiguration auf Ersatz- oder Testhardware zurückspielen und in Betrieb nehmen; misst die Wiederanlaufzeit.	Wiederanlauftest (Tabelle 34); Wiederherstellung auf Ersatzplattform (NIST SP 800-34, 3.5.1); Konfigurationsdaten (DVO-Anhang Nr. 4.2.2 lit. b)
Kompletter Wiederanlauf	Alle zeitkritischen Systeme in der festgelegten Reihenfolge samt Abhängigkeiten wiederanlaufen lassen, bis der Fachbereich arbeiten kann.	Schwarzstart, d. h. Wiederanlauf aller Server und Systeme, planen und üben (BSI-Maßnahmenkatalog Ransomware, Kap. 2); vollständige Wiederherstellung bei Systemen hoher Schutzstufe (NIST, 3.5.4); Reihenfolge (CON.3.A4)
Offline- oder unveränderliche Kopie	Ist die Kopie wirklich getrennt oder gegen Löschen und Überschreiben gesperrt? Dann aus genau dieser Kopie wiederherstellen.	Trennung prüfen (Maßnahmenkatalog Ransomware, Kap. 2); Schutz vor Überschreiben (CON.3.A14); nicht im selben Netz (DVO Nr. 4.2.2 lit. c)

Oft genügt es, die zeitkritischen Teile in aufbauenden Stufen zu testen (BSI-Standard 200-4, Kap. 13.9); auch Stellvertretende sollen üben (Kap. 13.2). Probe für die Offline-Kopie: Ein (Domänen-)Administrator versucht, auf die getrennten Kopien zuzugreifen; das sollte nicht gelingen (Maßnahmenkatalog Ransomware, Kap. 2). Empfehlung von TOMORIS: Löschsperren nur an einer eigens angelegten Testsicherung prüfen. NIS2-Einrichtungen testen nach Nr. 4.2.6 DVO-Anhang auch Redundanzen, etwa das Umschalten zwischen redundant ausgelegten Systemen (BSI-Standard 200-4, Tabelle 34); dafür können Sie Teil B bis D sinngemäß verwenden.

03 —

Begriffe: Sollwerte und gemessene Werte

MTPD, RTO und RPO als Vorgaben, RTA und RPA als Messwerte, nach BSI-Standard 200-4 und NIST SP 800-34.

BSI-Standard 200-4, Kap. 7, 7.2.1, 8 und 8.2; NIST SP 800-34 Rev. 1, Abschnitt 3.2.1

MTPD (MTA), maximal tolerierbare Ausfallzeit	Wie lange ein Geschäftsprozess höchstens ausfallen darf, bevor nicht tolerierbare Auswirkungen eintreten; ermittelt in der Business-Impact-Analyse (BSI). NIST nennt die entsprechende Größe MTD (Maximum Tolerable Downtime).
RTO (WAZ), geforderte Wiederanlaufzeit	BSI: vom Ausrufen des Notfalls bis zur geforderten Inbetriebnahme der Notfalllösung, etwa dem Zurücksetzen eines IT-Systems auf den letzten gesicherten Zustand; kürzer als die MTPD, weil die Reaktionszeit davon abgeht. NIST: wie lange eine Systemressource höchstens ausfallen darf, ohne unannehmbare Folgen für Prozesse und MTD.
RPO, maximal zulässiger Datenverlust	Wie alt verfügbare Daten höchstens sein dürfen, um im Notbetrieb sinnvoll zu arbeiten; daraus folgt der Sicherungszyklus (BSI). NIST: der Zeitpunkt vor dem Ausfall, auf den sich die Daten mit der jüngsten Sicherung zurückholen lassen.
RTA, tatsächliche Wiederanlaufzeit	Der real erreichbare Zeitraum vom Ausruf des Notfalls bis zur produktiv gesetzten Notfalllösung. Sie wird der RTO gegenübergestellt und lässt sich in Übungen und Tests ermitteln und nachweisen; ohne realistische Schätzung gilt sie als unbekannt (BSI).
RPA, tatsächlicher Datenverlust	Der Ist-Wert, mit dem die RPO zu vergleichen ist; zudem ist die RPO mit dem Sicherungszyklus abzugleichen (BSI, Kap. 8.2).
BAO-Reaktionszeit	BAO steht für die Besondere Aufbauorganisation, also die Notfallorganisation mit dem Notfallstab. Die BAO-Reaktionszeit reicht vom Eintreten des Schadensereignisses über Erkennen und Alarmieren bis zum Ausrufen des Notfalls; MTPD minus Reaktionszeit, gegebenenfalls minus Puffer, ergibt die RTO (BSI, Kap. 2, 5.5.1 und 7.2.1). Hinweis von TOMORIS: Ein Restore-Test misst sie nicht mit. Die tatsächliche Detektionszeit lässt sich nur schätzen oder aus realen Ereignissen ableiten (Kap. 13.10.2).

04

Testplan über das Jahr

Welche Testart wie oft, was der Jahresplan enthalten soll und eine Tabelle zum Ausfüllen.

Die Jahresübungsplanung soll mindestens zwölf Monate umfassen und je Übung Zeitraum, Art, Ziel und Umfang, Zuständige, Übende, Ressourcen und den erwarteten Einfluss auf den Normalbetrieb festhalten (BSI-Standard 200-4, Kap. 13.3). Bei NIS2-Einrichtungen müssen die Tests sicherstellen, dass Sicherungskopien und Redundanzen im Ernstfall zuverlässig sind und alle für eine wirksame Wiederherstellung nötigen Kopien, Verfahren und Kenntnisse abdecken; eine Häufigkeit nennt der DVO-Anhang nicht, nur „regelmäßig“ (Nr. 4.2.6). Die Musterrichtlinie in NIST SP 800-34 sieht jährliche Tests der Wiederherstellungsfähigkeit vor (Abschnitt 3.1). Die Häufigkeiten des BSI unten sind ein Beispiel, keine Vorgabe.

Häufigkeit: Beispiel des BSI und Empfehlungen von TOMORIS

TESTART	HÄUFIGKEIT	HERKUNFT
System	mindestens jährlich bei RTO unter 24 h, mindestens alle 3 Jahre bei RTO unter 5 Tagen	Beispiel des BSI für Funktionstests (Tabelle 37); für NIS2 siehe Hinweis unten
Datei	monatlich eine Stichprobe je Sicherungsauftrag, bei Daten hoher Kritikalität wöchentlich, zusätzlich sofort nach wesentlichen Änderungen; die Stichprobe wechselt zwischen den Kopien	Empfehlung von TOMORIS, angelehnt an das ENISA-Beispiel zu Nr. 4.2.6
Offline- oder unveränderliche Kopie	Trennung oder Sperre vierteljährlich prüfen; Datei-Stichproben regelmäßig auch aus dieser Kopie ziehen	Empfehlung von TOMORIS
Kompletter Wiederanlauf	mindestens jährlich, als Planbesprechung und als technischer Test in aufbauenden Stufen bis zur vollständigen Wiederherstellung auf einen bekannten Stand	Empfehlung von TOMORIS, gestützt auf Kap. 13.9 und ENISA zu Nr. 4.1.4
Anlassbezogen	nach erheblichen Sicherheitsvorfällen und wesentlichen Änderungen der Betriebsabläufe oder Risiken (DVO), nach System- oder Organisationsänderungen (NIST); Empfehlung von TOMORIS: auch nach Wechsel von Sicherungssoftware, Speicherziel oder Dienstleister	DVO Nr. 4.1.4 für den Notfallplan; NIST SP 800-34, 3.5; BSI-Standard 200-4, Kap. 13.2; DER.4.A10 (erhöhter Schutzbedarf)

Für NIS2-Einrichtungen: Die ENISA-Umsetzungshilfe zur DVO (Technical Implementation Guidance, Juni 2025, nicht rechtsverbindlich) nennt zu Nr. 4.2.6 als Beispiel wöchentliche Prüfungen für Daten hoher Kritikalität, monatliche für mittlere und niedrige und eine Prüfung sofort nach wesentlichen Änderungen. Zu Nr. 4.1.4 rät sie, Notfall- und Wiederanlaufpläne mindestens jährlich zu testen, auch als Planbesprechung, und die vollständige Wiederherstellung auf einen bekannten Zustand in die Tests des Wiederanlaufplans aufzunehmen.

Testplan [Datum] bis [Datum], freigegeben am [Datum] durch [Name, Funktion]

ZEITRAUM	TESTART, SYSTEM, ZIEL	ZUSTÄNDIG, ÜBENDE	RESSOURCEN, EINFLUSS AUF BETRIEB	ERLEDIGT AM
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

05

Teil A: Testkonzept und Vorbedingungen

Vor dem Test: was mit welcher Sicherung getestet wird, woran Erfolg gemessen wird und was bereitstehen muss.

Testkonzept (nach BSI-Standard 200-4, Kap. 13.4 und 13.9.1, und NIST SP 800-34, 3.5.1)

ANGABE	EINTRAG
Test-Nr.; Testart: Datei, System, kompletter Wiederanlauf, Offline- oder unveränderliche Kopie	_____
Getestetes System, Dienst oder Datenbestand; Sollwerte RTO, RPO und MTPD siehe Teil C	[System]
Ziel und messbare Erfolgskriterien, z. B. RTA höchstens RTO, Fachbereich bestätigt die Funktion	_____
Datum, Beginn, Ende; angekündigt ja oder nein; Umgebung: abgeschottete Testumgebung, Ersatzhardware oder Produktion	[Datum], __:__ bis __:__; _____
Übungsleitung; Durchführende, Protokoll, Beobachtung mit Rolle und Name; Dienstleister	[Name, Funktion]
Verwendete Sicherung: Auftrag, Zeitstempel des Datenstands, Kopie oder Medium, Standort	_____

- ☐ Risikoeinschätzung, risikosenkende Maßnahmen und Abbruchkriterien festgelegt, der Weg zurück in den Ausgangszustand vorbereitet; Freigabe der Geschäftsführung, falls der Test den Betrieb beeinträchtigen kann (BSI-Standard 200-4, Kap. 13.9.1).
- ☐ Testumgebung realitätsnah, aber vom Produktionsbetrieb abgekapselt; Aufbau und Rückbau geplant (Kap. 13.9.1).
- ☐ Die Wiederherstellungsanleitung liegt auch außerhalb des Sicherungssystems vor, etwa auf Papier, und wird im Test verwendet (CON.3.A6, Gefährdung 2.4).

- ☐ Schlüssel verschlüsselter Sicherungen sind aus getrennter Ablage verfügbar (CON.3.A13, erhöhter Schutzbedarf); Ersatz- oder Testhardware steht bereit (NIST SP 800-34, 3.5.1); bei Online-Speicher schaffen Sicherungssystem und Netzanbindung die zulässige Wiederherstellungszeit (CON.3.A9).
- ☐ Ablauf mit Dienstleistern abgestimmt, die Sicherung oder Wiederherstellung betreiben, wenn angemessen gemeinsam getestet (DER.4.A16, erhöhter Schutzbedarf); für NIS2-Einrichtungen rät auch die ENISA-Umsetzungshilfe zu Nr. 4.2.6, Lieferanten in Tests einzubeziehen.
- ☐ Auch Stellvertretende üben (BSI-Standard 200-4, Kap. 13.2, dort für die Rollen der Notfallorganisation). Empfehlung von TOMORIS: Den Restore führt, wo möglich, die Vertretung nach der dokumentierten Anleitung aus.

06

Teil B: Ablauf mit Zeitstempeln

Während des Tests: jeder Schritt mit Uhrzeit, Person und Ergebnis, vom Teststart T0 bis zur Übergabe T1.

Das Protokoll soll prägnant und für sachverständige Dritte verständlich sein (BSI-Standard 200-4, Kap. 13.2). Empfehlung von TOMORIS: alle Zeitstempel von derselben Uhr, T0 vorab festlegen.

Ablaufprotokoll zum Ausfüllen

UHRZEIT	SCHRITT	WER	ERGEBNIS, BEMERKUNG
__:__:__	T0: Teststart, steht für den Ausruf des Notfalls und den angenommenen Ausfall	_____	_____
__:__:__	Sicherung ausgewählt und bereitgestellt: Auftrag, Zeitstempel des Datenstands, Kopie	_____	_____
__:__:__	Sicherung vor dem Einspielen auf Schadsoftware und Beschädigung geprüft	_____	_____
__:__:__	Wiederherstellung gestartet	_____	_____
__:__:__	Wiederherstellung abgeschlossen; Datenmenge, reine Dauer	_____	_____
__:__:__	Integrität und Funktion geprüft (Teil C)	_____	_____
__:__:__	T1: System an den Fachbereich zur Nutzung übergeben	_____	_____
__:__:__	Abweichung, Unterbrechung oder Eingriff	_____	_____
__:__:__	Rückbau abgeschlossen, Ausgangszustand hergestellt	_____	_____

Bei unbeabsichtigten Auswirkungen auf den Betrieb nach den festgelegten Kriterien abbrechen und den Ausgangszustand schnellstmöglich herstellen (Kap. 13.9.1); die Übungsleitung prüft die Abbruchkriterien fortlaufend (Tabelle 36). Alles eigens für den Test Geschaffene wird danach rückgängig gemacht (Kap. 13.9.1).

07

Teil C: Messung und Integritätsprüfung

Erreichte Wiederanlaufzeit und Datenstand gegen RTO und RPO, dann prüfen, ob die Daten vollständig und unversehrt sind.

So rechnen Sie (Empfehlung von TOMORIS, abgeleitet aus den Begriffen des BSI-Standards 200-4, Kap. 7 und 8): T0 steht im Test für den Ausruf des Notfalls, also den Beginn der Wiederherstellung; Erkennen und Alarmieren (BAO-Reaktionszeit) sind darin nicht enthalten. Die erreichte Wiederanlaufzeit (RTA) reicht von T0 bis zur Übergabe T1 an den Fachbereich. Für den Datenverlust gilt T0 zugleich als angenommener Ausfallzeitpunkt: Die RPA ist der Abstand zwischen dem Zeitstempel des jüngsten vollständig zurückgekommenen Datenstands und T0.

Soll-Ist-Vergleich (BSI-Standard 200-4, Kap. 8.2, Tabellen 28 und 29; letzte Zeile: Empfehlung von TOMORIS)

KENNGRÖSSE	SOLL	IST	ERFÜLLT
Wiederanlaufzeit: RTA = T1 minus T0	RTO ____ h	____ h ____ min	ja / nein
Datenverlust: RPA = T0 minus Zeitstempel des Datenstands	RPO ____ h	____ h	ja / nein
Sicherungszyklus laut Datensicherungsplan	höchstens RPO	____ h	ja / nein
RTA plus BAO-Reaktionszeit	unter MTPD ____ h	____ h	ja / nein

- ☐ Vor dem Einspielen geprüft, ob die Sicherung schon Schadsoftware enthalten könnte; gearbeitet mit einer Kopie der Sicherung oder einem Schreibschutz (BSI-Maßnahmenkatalog Ransomware, Kap. 2).
- ☐ Daten vollständig zurück und auf dem Stand der letzten verfügbaren Sicherung (NIST SP 800-34, 4.4); Prüfweg, etwa Anzahl, Größe, Prüfsummen: _____
- ☐ Konfigurationsdaten und in Cloud-Diensten gespeicherte Daten zurückgekommen (DVO-Anhang Nr. 4.2.2 lit. b); verschlüsselte Sicherung mit dem Schlüssel aus getrennter Ablage entschlüsselt (CON.3.A13, erhöhter Schutzbedarf).
- ☐ Alle Funktionen geprüft, bereit für den Normalbetrieb (NIST SP 800-34, 4.4); bestätigt durch [Name, Funktion] aus dem Fachbereich.
- ☐ Offline-Kopie: Zugriffsversuch mit (Domänen-)Administratorrechten gescheitert (Maßnahmenkatalog Ransomware, Kap. 2). Unveränderliche Kopie: Löschen oder Überschreiben einer Testsicherung abgewiesen (Überschreiben: CON.3.A14; Löschen: Empfehlung von TOMORIS).

- ☐ Die Anleitung war verständlich, vollständig und fachlich richtig; Abweichungen stehen in Teil D (BSI-Standard 200-4, Kap. 13.9).

08

Teil D: Ergebnis, Befunde und Freigabe

Ergebnis je getesteter Ressource, Maßnahmen mit Verantwortung und Frist, Unterschriften bis zur Geschäftsführung.

Je getesteter Ressource: erfolgreich, teilweise erfolgreich oder nicht erfolgreich (BSI-Standard 200-4, Kap. 13.9.2, Tabelle 40). Gesamtergebnis: bestanden / nicht bestanden, denn ein Test ist nach ISO 22398 eine Übung mit objektiv gemessenem Ergebnis (Kap. 13). Eine fehlerfreie Übung ist kein Erfolgskriterium; erfolgreich ist sie auch, wenn Korrekturbedarf erkannt und zur Verbesserung genutzt wird (Kap. 13.10).

Ergebnis und Maßnahmen je Ressource (nach BSI-Standard 200-4, Tabelle 40)

RESSOURCE, TEST-AKTIVITÄT	ERGEBNIS	BEFUND, URSACHE	KORREKTURMASSNAHME	VERANTWORTLICH, FRIST
_____	_____	_____	_____	[Name, Funktion], [Datum]
_____	_____	_____	_____	[Name, Funktion], [Datum]
_____	_____	_____	_____	[Name, Funktion], [Datum]
_____	_____	_____	_____	[Name, Funktion], [Datum]

NIS2-Einrichtungen dokumentieren Testergebnisse und ergreifen erforderlichenfalls Korrekturmaßnahmen (DVO-Anhang Nr. 4.2.6); die Lehren aus Tests fließen in die Pläne ein (Nr. 4.1.4). Das BSI empfiehlt, Ursachen zu ermitteln, Verbesserungen zu überwachen und Verzögerungen der Leitung zu melden (DER.4.A14, erhöhter Schutzbedarf). Empfehlung von TOMORIS: einen Befund erst nach erfolgreichem Nachtest schließen. Gilt der Anhang für Sie über § 2 NISV 2026 und können Sie Nr. 4.2.6 vorübergehend oder wegen Ihrer Größe nicht erfüllen, verlangt § 4 NISV 2026 kompensierende Maßnahmen, begründet dokumentiert und mindestens jährlich auf Wirksamkeit geprüft.

Freigabe (sinngemäß nach DER.4.A14, erhöhter Schutzbedarf; NIS2: Leitung beaufsichtigt nach § 31 Abs. 1 NISG 2026)

ROLLE	NAME, FUNKTION	DATUM	UNTERSCHRIFT
Übungsleitung: durchgeführt und protokolliert	[Name, Funktion]	[Datum]	_____
IT-Verantwortung oder IT-Dienstleister	[Name, Funktion]	[Datum]	_____
Fachbereich: Funktion bestätigt	[Name, Funktion]	[Datum]	_____
Geschäftsführung: Ergebnis und Maßnahmen freigegeben	[Name, Funktion]	[Datum]	_____

09 —

Häufige Fehler

Was Wiederherstellungstests wertlos macht, mit der jeweiligen Fundstelle.

- Der Status „Sicherung erfolgreich“ ersetzt keinen Restore-Test (CON.3, Gefährdung 2.2).
- Anleitung und Schlüssel liegen nicht getrennt und fallen mit aus (Gefährdungen 2.4 und 2.8).
- Die Konfiguration fehlt in der Sicherung, nur Inhaltsdaten sind gesichert (DVO-Anhang Nr. 4.2.2 lit. b).
- Immer dieselbe Übungssituation erhöht die Gefahr von Betriebsblindheit (BSI-Standard 200-4, Kap. 13.2).

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Betroffenheitscheck

tomoris.com/tools/nis2-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

10 —

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **BSI IT-Grundschutz-Kompendium, Baustein CON.3 Datensicherungskonzept, Edition 2023**
Gefährdungen 2.2, 2.4, 2.8; A4, A6, A9, A13, A14, A15
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 2 **BSI IT-Grundschutz-Kompendium, Baustein DER.4 Notfallmanagement, Edition 2023**
Anforderungen DER.4.A1, A10, A14 und A16
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 3 **BSI-Standard 200-4 Business Continuity Management, Version 1.0 (2023)**
Kap. 2, 5.5.1, 7 bis 8.2, 13 bis 13.10; Tab. 28, 29, 34, 36, 37, 40
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Sta...
- 4 **BSI: Grundschutz++, Meilensteinplan**
Stand Oktober 2026, gelesen am 25.10.2026
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standa...
- 5 **BSI: Anwenderkatalog Grundschutz++ (GitHub)**
NOT.4.16.1; Stand 22.10.2026, Pilotphase
github.com/BSI-Bund/Stand-der-Technik-Bibliothek
- 6 **BSI: Maßnahmenkatalog Ransomware, Version 1.0 vom 23.02.2022**
Kap. 2 Backups
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Th...
- 7 **NIST SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems**
Abschnitte 3.1, 3.2.1, 3.5, 3.5.1, 3.5.4 und 4.4
nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-3...
- 8 **Durchführungsverordnung (EU) 2024/2690**
Art. 1; Anhang Nr. 4.1.4, 4.2.2, 4.2.3 und 4.2.6
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- 9 **ENISA: Technical Implementation Guidance, Version 1.0 (Juni 2025)**
Nr. 4.1.4, 4.2.3 und 4.2.6, S. 54, 57 und 59
www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical...
- 10 **NISV 2026, BGBl. II Nr. 290/2026**
§ 2 und § 4, kundgemacht am 1.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 11 **NISG 2026, BGBl. I Nr. 94/2025, RIS, Fassung vom 25.10.2026**
§ 4 Abs. 2, § 27 Abs. 1, § 31 Abs. 1, § 32 Abs. 4 lit. c, § 51 Abs. 2
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 12 **Verordnung (EU) 2016/679 (DSGVO)**
Art. 32 Abs. 1 lit. c und d
eur-lex.europa.eu/eli/reg/2016/679/oj/deu