

TEMPLATE · TOMORIS TOOLBOX

Restore Test: Log Template for Backups and Systems

Fillable log for file, system and full restores as well as offline copies, with target-versus-actual comparison, findings, sign-off and annual plan

UPDATED

Oct 25, 2026

LENGTH

PDF, 11 pages

ONLINE

tomoris.com/en/downloads/wiederherstellungstest-protokoll

AT A GLANCE

4

Test types, from a single file to a full recovery

RTA

measured recovery time, compared with the RTO

4.2.6

Annex point: backup and redundancy testing

12 mo.

Minimum period of annual exercise planning (BSI)

WHO IT IS FOR

- IT administrators and IT managers who run backups and want to prove they can be restored
- IT service providers who manage backups for customers and run tests together with them
- Business continuity and information security officers who maintain exercise plans
- Management that approves test results and measures
- Essential and important entities that must document tests under the NISG 2026 (Austrian Network and Information Systems Security Act 2026)

WHAT THIS COVERS

A backup is only worth something once it can be restored. According to the BSI module CON.3, you must test regularly whether this works flawlessly and within a reasonable time; for essential and important entities, such tests have been mandatory since October 2026 under the NISG 2026 and the Annex to IR (EU) 2024/2690, including documentation of the results. This template provides a log for that purpose: test type and objective, preconditions, procedure with timestamps, achieved recovery time and data state against RTO and RPO, integrity check, findings with deadlines, sign-off and a test plan for the year. It is based on BSI Standard 200-4, the modules CON.3 and DER.4, and NIST SP 800-34.

Adapt this template to your company: test types, target values, frequencies and responsibilities depend on your business processes and systems. The structure and the marked recommendations are from TOMORIS. The template provides an overview and does not replace legal advice; the text of the law in its current version is decisive.

Usage: You may adapt this template for your own use; you may redistribute it only in unchanged form.

CONTENTS

01	Testing restores: recommendation and obligation	3
02	Four test types	4
03	Terms: target values and measured values	5
04	Test plan for the year	6
05	Part A: Test concept and preconditions	7
06	Part B: Procedure with timestamps	8
07	Part C: Measurement and integrity check	8
08	Part D: Result, findings and sign-off	9
09	Common mistakes	10
10	Sources	11

01 —

Testing restores: recommendation and obligation

Why a backup only counts once its restore has been tested, who requires such tests and how to use the template.

Backing up data regularly does not automatically ensure that it can be restored without problems (BSI IT-Grundschutz, module CON.3, threat 2.2). The module therefore requires, as a basic requirement, regular tests of whether backed-up data can be restored flawlessly and within a reasonable time (CON.3.A15). For Austrian companies, IT-Grundschutz is a recognized recommendation, not an obligation. The numbers refer to the Kompendium Edition 2023. According to the BSI, its successor Grundschutz++ can be certified from January 1, 2027, and IT-Grundschutz until November 30, 2031; its user catalog lists the restore test as NOT.4.16.1 (SHOULD, based on representative samples). Binding requirements arise from the NISG 2026 and, for personal data, from the GDPR:

Who requires or recommends restore tests

BASIS	APPLIES TO	WHAT IS REQUIRED
§ 32 para. 4 lit. c NISG 2026, in force since Oct 1, 2026	essential and important entities, unless equivalent sector-specific EU requirements apply (§ 27 NISG 2026; financial sector: DORA, § 4 para. 2)	Business continuity, such as backup management and disaster recovery, as a risk management measure.
Annex points 4.2.2, 4.2.3 and 4.2.6 Implementing Regulation (EU) 2024/2690, directly or via § 2 NISV 2026 (Austrian NIS Regulation 2026)	essential and important entities; directly for the providers named in Art. 1 of the Implementing Regulation (including cloud, data centers, managed services)	Backup plans with recovery times; regular integrity checks; regular testing of the restoration of backup copies and redundancies to ensure that they are reliable and cover all necessary copies, procedures and knowledge; document results and take corrective action where necessary.
Art. 32(1)(c) and (d) GDPR	Controllers and processors	The ability to restore the availability of personal data in a timely manner after an incident; a process for regularly testing the effectiveness of the measures.
BSI CON.3.A15 (basic), DER.4.A1 (standard), DER.4.A10 (elevated protection needs)	Recommendation for everyone	Regular restore tests (A15); use tests and exercises to check whether the measures in the emergency manual work as intended (A1); with elevated protection needs, test emergency plans regularly and when there is cause, and maintain an exercise plan (A10).

1

Define the test plan

In the test plan (Section 04), enter for at least twelve months which system is tested when and with which test type; management approves it (BSI Standard 200-4, ch. 13.3).

2

Fill out one copy per test

Part A before the test, Part B during it, Parts C and D afterward. Track findings until a successful retest.

The structure and fields are a TOMORIS recommendation. BSI Standard 200-4 provides for an exercise concept, an exercise log and an exercise report for each exercise and allows them to be combined in one document (ch. 13.2). Replace placeholders such as [System], [Name, role] and [MM/DD/YYYY] and fill in the “_____” fields. The GDPR does not mention the test explicitly; in TOMORIS’s view, it is an obvious way to verify the ability under lit. c.

02

Four test types

From a single file to a full recovery, plus the check of the separated copy.

Test types in this template and their basis

TEST TYPE	WHAT IS TESTED	BASIS
File	Restore files, folders or data sets from a backup and open them: readable, complete, desired state?	Readability and restoration tests (BSI Standard 200-4, Table 34, ch. 13.9.1); CON.3.A15
System	Restore a server, virtual machine or database server including its configuration to replacement or test hardware and put it into operation; measures the recovery time.	Recovery test (Table 34); recovery to an alternate platform (NIST SP 800-34, 3.5.1); configuration data (Implementing Regulation Annex point 4.2.2(b))
Full recovery	Bring all time-critical systems back up in the defined order, including dependencies, until the business unit can work.	Plan and practice a black start, i.e. recovery of all servers and systems (BSI ransomware catalog of measures, ch. 2); full restoration for high-impact systems (NIST, 3.5.4); sequence (CON.3.A4)
Offline or immutable copy	Is the copy truly separated or locked against deletion and overwriting? Then restore from exactly this copy.	Check the separation (ransomware catalog of measures, ch. 2); protection against overwriting (CON.3.A14); not in the same network (Implementing Regulation point 4.2.2(c))

It is often sufficient to test the time-critical parts in incremental stages (BSI Standard 200-4, ch. 13.9); deputies should practice too (ch. 13.2). Check for the offline copy: a (domain) administrator tries to access the separated copies; this should fail (ransomware catalog of measures, ch. 2). TOMORIS recommendation: test deletion locks only on a test backup created specifically for this purpose. Under point 4.2.6 of the Implementing Regulation Annex, NIS2 entities also test redundancies, for example failover between redundantly designed systems (BSI Standard 200-4, Table 34); you can use Parts B to D accordingly for this.

03 —

Terms: target values and measured values

MTPD, RTO and RPO as targets, RTA and RPA as measured values, according to BSI Standard 200-4 and NIST SP 800-34.

BSI Standard 200-4, ch. 7, 7.2.1, 8 and 8.2; NIST SP 800-34 Rev. 1, Section 3.2.1

MTPD (MTA), maximum tolerable period of disruption	The maximum time a business process may be down before intolerable impacts occur; determined in the business impact analysis (BSI). NIST calls the corresponding value MTD (Maximum Tolerable Downtime).
RTO (WAZ), required recovery time	BSI: from the declaration of the emergency to the required commissioning of the emergency solution, such as resetting an IT system to the last backed-up state; shorter than the MTPD, because the response time is subtracted from it. NIST: the maximum time a system resource can be unavailable without unacceptable consequences for processes and the MTD.
RPO, maximum acceptable data loss	The maximum age of available data that still allows meaningful work in emergency operations; the backup cycle follows from it (BSI). NIST: the point in time before the outage to which data can be recovered with the most recent backup.
RTA, actual recovery time	The actually achievable period from the declaration of the emergency to the emergency solution being put into production. It is compared with the RTO and can be determined and demonstrated in exercises and tests; without a realistic estimate, it is considered unknown (BSI).
RPA, actual data loss	The actual value against which the RPO is compared; in addition, the RPO must be aligned with the backup cycle (BSI, ch. 8.2).
BAO response time	BAO stands for Besondere Aufbauorganisation (special organizational structure), meaning the emergency organization with the crisis team. The BAO response time runs from the occurrence of the damaging event through detection and alerting to the declaration of the emergency; MTPD minus response time, minus a buffer where applicable, gives the RTO (BSI, ch. 2, 5.5.1 and 7.2.1). TOMORIS note: a restore test does not measure it. The actual detection time can only be estimated or derived from real events (ch. 13.10.2).

04

Test plan for the year

Which test type how often, what the annual plan should contain and a table to fill in.

Annual exercise planning should cover at least twelve months and record for each exercise the period, type, objective and scope, responsible persons, participants, resources and the expected impact on normal operations (BSI Standard 200-4, ch. 13.3). For NIS2 entities, the tests must ensure that backup copies and redundancies are reliable in an emergency and cover all copies, procedures and knowledge required for effective recovery; the Implementing Regulation Annex does not specify a frequency, only “regularly” (point 4.2.6). The sample policy in NIST SP 800-34 provides for annual tests of recovery capability (Section 3.1). The BSI frequencies below are an example, not a requirement.

Frequency: BSI example and TOMORIS recommendations

TEST TYPE	FREQUENCY	ORIGIN
System	at least annually for an RTO under 24 h, at least every 3 years for an RTO under 5 days	BSI example for functional tests (Table 37); for NIS2, see the note below
File	one sample per backup job monthly, weekly for highly critical data, and also immediately after significant changes; the sample alternates between the copies	TOMORIS recommendation, based on the ENISA example for point 4.2.6
Offline or immutable copy	check separation or lock quarterly; regularly draw file samples from this copy as well	TOMORIS recommendation
Full recovery	at least annually, as a tabletop review and as a technical test in incremental stages up to full restoration to a known state	TOMORIS recommendation, based on ch. 13.9 and ENISA on point 4.1.4
Event-driven	after significant security incidents and significant changes to operations or risks (Implementing Regulation), after system or organizational changes (NIST); TOMORIS recommendation: also after a change of backup software, storage target or service provider	Implementing Regulation point 4.1.4 for the contingency plan; NIST SP 800-34, 3.5; BSI Standard 200-4, ch. 13.2; DER.4.A10 (elevated protection needs)

For NIS2 entities: the ENISA implementation guidance on the Implementing Regulation (Technical Implementation Guidance, June 2025, not legally binding) gives as an example for point 4.2.6 weekly checks for highly critical data, monthly checks for medium and low criticality, and a check immediately after significant changes. For point 4.1.4, it recommends testing contingency and recovery plans at least annually, including as a tabletop review, and including full restoration to a known state in the recovery plan tests.

Test plan [MM/DD/YYYY] to [MM/DD/YYYY], approved on [MM/DD/YYYY] by [Name, role]

PERIOD	TEST TYPE, SYSTEM, OBJECTIVE	RESPONSIBLE, PARTICIPANTS	RESOURCES, IMPACT ON OPERATIONS	COMPLETED ON
-----	-----	-----	-----	-----

_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

05

Part A: Test concept and preconditions

Before the test: what is tested with which backup, how success is measured and what must be ready.

Test concept (based on BSI Standard 200-4, ch. 13.4 and 13.9.1, and NIST SP 800-34, 3.5.1)

ITEM	ENTRY
Test no.; test type: file, system, full recovery, offline or immutable copy	_____
System, service or data set tested; target values RTO, RPO and MTPD, see Part C	[System]
Objective and measurable success criteria, e.g. RTA no more than RTO, business unit confirms functionality	_____
Date, start, end; announced yes or no; environment: isolated test environment, replacement hardware or production	[MM/DD/YYYY], __:__:__ to __:__:__
Exercise lead; performers, logging, observation with role and name; service providers	[Name, role]
Backup used: job, timestamp of the data state, copy or medium, location	_____

- ☐ Risk assessment, risk-reducing measures and abort criteria defined, the way back to the initial state prepared; management approval if the test may affect operations (BSI Standard 200-4, ch. 13.9.1).
- ☐ Test environment realistic but isolated from production; setup and teardown planned (ch. 13.9.1).
- ☐ The restore instructions are also available outside the backup system, for example on paper, and are used in the test (CON.3.A6, threat 2.4).
- ☐ Keys for encrypted backups are available from separate storage (CON.3.A13, elevated protection needs); replacement or test hardware is ready (NIST SP 800-34, 3.5.1); with online storage, the backup system and network connection achieve the permissible recovery time (CON.3.A9).
- ☐ Procedure coordinated with service providers that operate backup or recovery, tested jointly where appropriate (DER.4.A16, elevated protection needs); for NIS2 entities, the ENISA implementation guidance on point 4.2.6 also recommends involving suppliers in tests.
- ☐ Deputies practice too (BSI Standard 200-4, ch. 13.2, there for the roles of the emergency organization). TOMORIS recommendation: where possible, the deputy performs the restore following the documented instructions.

06

Part B: Procedure with timestamps

During the test: every step with time, person and result, from test start T0 to handover T1.

The log should be concise and understandable to expert third parties (BSI Standard 200-4, ch. 13.2). TOMORIS recommendation: take all timestamps from the same clock and define T0 in advance.

Procedure log to fill in

TIME	STEP	WHO	RESULT, REMARK
__:__:__	T0: test start, represents the declaration of the emergency and the assumed outage	_____	_____
__:__:__	Backup selected and provided: job, timestamp of the data state, copy	_____	_____
__:__:__	Backup checked for malware and damage before restoring	_____	_____
__:__:__	Restore started	_____	_____
__:__:__	Restore completed; data volume, net duration	_____	_____
__:__:__	Integrity and functionality checked (Part C)	_____	_____
__:__:__	T1: system handed over to the business unit for use	_____	_____
__:__:__	Deviation, interruption or intervention	_____	_____
__:__:__	Teardown completed, initial state restored	_____	_____

In case of unintended impact on operations, abort according to the defined criteria and restore the initial state as quickly as possible (ch. 13.9.1); the exercise lead checks the abort criteria continuously (Table 36). Everything created specifically for the test is reversed afterward (ch. 13.9.1).

07

Part C: Measurement and integrity check

Achieved recovery time and data state against RTO and RPO, then check whether the data is complete and intact.

How to calculate (TOMORIS recommendation, derived from the terms in BSI Standard 200-4, ch. 7 and 8): in the test, T0 stands for the declaration of the emergency, i.e. the start of recovery; detection and alerting (BAO response time) are not included. The achieved recovery time (RTA) runs from T0 to handover T1 to the business unit. For data loss, T0 also counts as the assumed time of the outage: the RPA is the interval between the timestamp of the most recent fully restored data state and T0.

Target-versus-actual comparison (BSI Standard 200-4, ch. 8.2, Tables 28 and 29; last row: TOMORIS recommendation)

METRIC	TARGET	ACTUAL	MET
Recovery time: RTA = T1 minus T0	RTO ____ h	____ h ____ min	yes / no
Data loss: RPA = T0 minus timestamp of the data state	RPO ____ h	____ h	yes / no
Backup cycle according to the backup plan	no more than RPO	____ h	yes / no
RTA plus BAO response time	below MTPD ____ h	____ h	yes / no

- ☐ Before restoring, checked whether the backup might already contain malware; worked with a copy of the backup or with write protection (BSI ransomware catalog of measures, ch. 2).
- ☐ Data fully restored and at the state of the last available backup (NIST SP 800-34, 4.4); verification method, e.g. count, size, checksums: _____
- ☐ Configuration data and data stored in cloud services restored (Implementing Regulation Annex point 4.2.2(b)); encrypted backup decrypted with the key from separate storage (CON.3.A13, elevated protection needs).
- ☐ All functions checked, ready for normal operations (NIST SP 800-34, 4.4); confirmed by [Name, role] from the business unit.
- ☐ Offline copy: access attempt with (domain) administrator rights failed (ransomware catalog of measures, ch. 2). Immutable copy: deletion or overwriting of a test backup rejected (overwriting: CON.3.A14; deletion: TOMORIS recommendation).
- ☐ The instructions were understandable, complete and technically correct; deviations are recorded in Part D (BSI Standard 200-4, ch. 13.9).

08

Part D: Result, findings and sign-off

Result per tested resource, measures with owner and deadline, signatures up to management.

Per tested resource: successful, partially successful or not successful (BSI Standard 200-4, ch. 13.9.2, Table 40). Overall result: passed / failed, because under ISO 22398 a test is an exercise with an objectively measured result (ch. 13). An error-free exercise is not a success criterion; an exercise is also successful if a need for correction is identified and used for improvement (ch. 13.10).

Result and measures per resource (based on BSI Standard 200-4, Table 40)

RESOURCE, TEST ACTIVITY	RESULT	FINDING, CAUSE	CORRECTIVE ACTION	OWNER, DEADLINE
_____	_____	_____	_____	[Name, role], [MM/DD/YYYY]
_____	_____	_____	_____	[Name, role], [MM/DD/YYYY]
_____	_____	_____	_____	[Name, role], [MM/DD/YYYY]
_____	_____	_____	_____	[Name, role], [MM/DD/YYYY]

NIS2 entities document test results and take corrective action where necessary (Implementing Regulation Annex point 4.2.6); lessons learned from tests are incorporated into the plans (point 4.1.4). The BSI recommends identifying causes, monitoring improvements and reporting delays to management (DER.4.A14, elevated protection needs). TOMORIS recommendation: close a finding only after a successful retest. If the Annex applies to you via § 2 NISV 2026 and you cannot meet point 4.2.6 temporarily or because of your size, § 4 NISV 2026 requires compensating measures, documented with reasons and reviewed for effectiveness at least annually.

Sign-off (by analogy with DER.4.A14, elevated protection needs; NIS2: management oversees under § 31 para. 1 NISG 2026)

ROLE	NAME, ROLE	DATE	SIGNATURE
Exercise lead: performed and logged	[Name, role]	[MM/DD/YYYY]	_____
IT owner or IT service provider	[Name, role]	[MM/DD/YYYY]	_____
Business unit: functionality confirmed	[Name, role]	[MM/DD/YYYY]	_____
Management: result and measures approved	[Name, role]	[MM/DD/YYYY]	_____

09

Common mistakes

What makes restore tests worthless, with the relevant reference for each.

- The status “Backup successful” does not replace a restore test (CON.3, threat 2.2).
- Instructions and keys are not stored separately and fail along with everything else (threats 2.4 and 2.8).
- The configuration is missing from the backup; only content data is backed up (Implementing Regulation Annex point 4.2.2(b)).
- Always using the same exercise scenario increases the risk of operational blindness (BSI Standard 200-4, ch. 13.2).

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

NIS2 applicability check (German)

tomoris.com/tools/nis2-check

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

10

Sources

All statements are supported by sources. Legislation applies in its current version.

- 1 **BSI IT-Grundschutz-Kompodium, module CON.3 Backup Concept, Edition 2023**
Threats 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-Kompodium, module DER.4 Business Continuity Management, Edition 2023**
Requirements DER.4.A1, A10, A14 and 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)**
Ch. 2, 5.5.1, 7 to 8.2, 13 to 13.10; Tables 28, 29, 34, 36, 37, 40
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Sta...
- 4 **BSI: Grundschutz++, milestone plan**
As of October 2026, accessed October 25, 2026
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standa...
- 5 **BSI: Grundschutz++ user catalog (GitHub)**
NOT.4.16.1; as of October 22, 2026, pilot phase
github.com/BSI-Bund/Stand-der-Technik-Bibliothek
- 6 **BSI: Ransomware catalog of measures, version 1.0 of February 23, 2022**
Ch. 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**
Sections 3.1, 3.2.1, 3.5, 3.5.1, 3.5.4 and 4.4
nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-3...
- 8 **Implementing Regulation (EU) 2024/2690**
Art. 1; Annex points 4.1.4, 4.2.2, 4.2.3 and 4.2.6
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- 9 **ENISA: Technical Implementation Guidance, version 1.0 (June 2025)**
Points 4.1.4, 4.2.3 and 4.2.6, pp. 54, 57 and 59
www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical...
- 10 **NISV 2026, BGBl. II No. 290/2026**
§ 2 and § 4, promulgated on October 1, 2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 11 **NISG 2026, BGBl. I No. 94/2025, RIS, version of October 25, 2026**
§ 4 para. 2, § 27 para. 1, § 31 para. 1, § 32 para. 4 lit. c, § 51 para. 2
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 12 **Regulation (EU) 2016/679 (GDPR)**
Art. 32(1)(c) and (d)
eur-lex.europa.eu/eli/reg/2016/679/oj/deu