TOMORIS
MORE THAN IT

FREE DOWNLOAD

CHECKLIST · TOMORIS TOOLBOX

Backup Checklist: 3-2-1-1-0 with an Offline Copy and Tested Recovery

A data backup checklist, backed by BSI IT-Grundschutz CON.3, the BSI Ransomware Measures Catalog, and CISA

UPDATED	LENGTH	ONLINE
Oct 22, 2026	PDF, 5 pages	tomoris.com/en/downloads/backup-checkliste-3-2-1-1-0

AT A GLANCE

3-2-1-1-0
Rule with an offline copy and tested recovery

19
Checkpoints to tick off, each with a source

1× a year
Minimum recovery test (CISA CPG 2.0)

WHO IT IS FOR

- Executives and IT managers in small and medium-sized businesses
- Administrators who run or set up backups
- Anyone who has outsourced backups to a service provider and wants to check them

Redistribution in unchanged form permitted

WHAT THIS COVERS

> According to the US agency CISA, most ransomware attackers try to find reachable backups and delete or encrypt them. This checklist turns the 3-2-1 rule and its extension with an offline copy and verified recovery into items you can check off. It is based on module CON.3 Data Backup Concept of the BSI IT-Grundschutz Compendium, the BSI Ransomware Measures Catalog, and CISA recommendations.

This checklist summarizes the requirements and recommendations of the bodies named and does not replace a backup concept. Which frequency, retention, and recovery time suit your systems depends on your business processes.

CONTENTS

01 The Rule: 3-2-1-1-0 2
02 Concept and Plans 3
03 Store Separately and Securely 3
04 Test Recovery: Zero Errors 4
05 Sources 5

01

The Rule: 3-2-1-1-0

What the five digits mean and which body recommends which part.

3

Copies

Three copies of important data: the original and two backups (BSI aid for Standard 200-4, ENISA, CISA).

2

Storage media

On two different storage media (BSI aid for Standard 200-4, ENISA, CISA).

1

Copy at another location

One copy at another location, physically separated, ideally in a different fire compartment (BSI CON.3.A12, ENISA, CISA).

1

Copy offline

One copy offline: disconnected from all other systems after the backup (BSI Ransomware Measures Catalog, CISA #StopRansomware Guide).

0

Errors during recovery

Zero errors: recovery is tested, and the data comes back intact and on time (BSI CON.3.A15, CISA CPG 2.0).

> 3-2-1 is recommended by the BSI (aid for BCM Standard 200-4), the EU agency ENISA, and the US agency CISA. The extension to 3-2-1-1-0 is not a standard but a term coined by vendors. However, BSI and CISA explicitly recommend its two additions, an offline copy and verified recovery.

Data mirroring via RAID does not count as a backup (BSI CON.3, description). For entities covered by NIS2, backup management is explicitly one of the risk management measures (§ 32 para. 4 lit. c NISG 2026 (Austrian Network and Information Systems Security Act 2026)).

02

Concept and Plans

What is backed up, how often, for how long, and in which order it comes back.

- [ ] The framework conditions are recorded for every system: data to be backed up, storage and change volume, availability, confidentiality, legal requirements, deletion rules, and responsibilities (CON.3.A1).
- [ ] The type, frequency, and timing of backups are defined, as are storage media, transport, and retention (CON.3.A2).
- [ ] There is a backup plan for each system or group of systems: what is backed up, recovery order, procedure, retention period, protection against access and overwriting, and the hardware and software used (CON.3.A4).
- [ ] For every system, the maximum tolerable data loss is defined (Recovery Point Objective, CON.3.A6).
- [ ] The recovery plans are available even if the backup system itself fails, for example also on paper (CON.3.A6; threat 2.4 cites ransomware as the reason).
- [ ] All employees know the backup rules and their own tasks in them (CON.3.A5).
- [ ] Online storage is governed by contract: storage location, availability, sign-in, and encryption of stored and transmitted data (CON.3.A9).

03

Store Separately and Securely

Dedicated media, another location, one copy offline, and no overwriting by unauthorized parties.

- [ ] Backups are always stored on dedicated storage media, not only on the system being backed up (CON.3.A2).
- [ ] The media are stored physically separated from the backed-up systems, ideally in a different fire compartment (CON.3.A12).
- [ ] At least one copy is offline and disconnected from all other systems after the backup (BSI Ransomware Measures Catalog; CON.3.A2 for media requiring special protection).

- [ ] Separation test: a domain administrator tries to access the separated copies as a test. This must fail (BSI Ransomware Measures Catalog).
- [ ] Backups cannot be overwritten, either intentionally or by accident; only authorized backup and administration processes have write access (CON.3.A14).
- [ ] Backups are encrypted, the keys are backed up separately, and encrypted data can still be restored even after a long time (CON.3.A13, for elevated protection needs).

> Automatic synchronization to the cloud is not an adequate backup on its own: if an attacker encrypts the local files, the encrypted versions are synchronized as well (CISA #StopRansomware Guide).

04

Test Recovery: Zero Errors

Regularly, at least once a year, completely, and within a reasonable time.

- [ ] Regular tests check whether backed-up data can be restored intact and within a reasonable time (CON.3.A15).
- [ ] Recovery is tested at least once a year (CISA CPG 2.0; WKO guide on technical and organizational measures).
- [ ] The recovery of data and entire systems is practiced, not just the backup (BSI Ransomware Measures Catalog).
- [ ] The recovery order follows the importance of the services (CON.3.A4; CISA #StopRansomware Guide).
- [ ] Regular checks confirm that the backup concept is implemented as described (CON.3.A6).
- [ ] The result and duration of every test are documented; errors are fixed and tested again.

> The last item is a TOMORIS recommendation: only a documented, successful test shows that the zero in 3-2-1-1-0 has been achieved.

NEXT STEP

Check It Yourself or Put It into Practice Together

DISCUSS IMPLEMENTATION

Get in Touch
tomoris.com/en/contact

contact@tomoris.com

05

Sources

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

1 **BSI IT-Grundschutz Compendium, module CON.3 Data Backup Concept, 2023 edition**
Requirements A1, A2, A4, A5, A6, A9, A12 to A15, threats 2.4 and 2.10
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...

2 **BSI: Ransomware Measures Catalog, version 1.0 of February 23, 2022**
Offline copy, separation test, practicing recovery
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Th...

3 **BSI: Proposals for Business Continuity Strategies, aid for BSI Standard 200-4 (Community Draft 2.0)**
Chapter 3.1, 3-2-1 rule
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmi...

4 **ENISA: Threat Landscape for Ransomware Attacks (July 2022)**
Chapter 6.1
www.enisa.europa.eu/sites/default/files/publications/ENISA%20Th...

5 **CISA: #StopRansomware Guide**
Offline and encrypted backups, cloud synchronization, recovery by priority
www.cisa.gov/resources-tools/resources/stopransomware-guide

6 **CISA: Cross-Sector Cybersecurity Performance Goals 2.0**
Offline backups, test at least once a year
www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0

7 **CISA/US-CERT: Data Backup Options**
3-2-1 rule
www.cisa.gov/sites/default/files/publications/data_backup_optio...

8 **WKO it-safe: Guide to technical and organizational measures under the GDPR**
Section 3.7, annual recovery test
www.wko.at/oe/it-sicherheit/leitfaden-massnahmen-dsgvo-1.pdf

9 **NISG 2026, BGBl. I No. 94/2025, § 32 para. 4 lit. c**
www.ris.bka.gv.at/eli/bgbl/i/2025/94

10 **Veeam: 3-2-1 Backup Rule (origin of the term 3-2-1-1-0)**
www.veeam.com/blog/321-backup-rule.html