

Backup controls evidence

GAPS

validator-01 · NIS2 and ISO/IEC 27001 · November 2025 – August 2026

Period	2025-11-01 to 2026-08-31 (UTC)
Databases	4
Signed validations	0 of 0
Successful test restores	0
Controls	evidence has gaps (see Controls)

About this report

This report collects evidence from Restorly's signed validation reports for the backup controls of NIS2 and ISO/IEC 27001. Each validation restores the newest backup into an isolated container on your own systems and checks it; the results are signed and hash-chained when they are made.

It is evidence for an assessment, not a statement of compliance: controls marked "For review" depend on facts outside Restorly, and your auditor judges whether the evidence is sufficient.

Controls

Control	Requirement	Evidence in this report	Status
NIS2 CIR 4.2.2(a)	Recovery times	Restore time measured on every successful test restore; median and maximum per database below. Compare them with your recovery time objectives. Missing for: billing, crm, inventory, webshop.	Gaps
NIS2 CIR 4.2.2(b)	Backup copies complete and accurate	Restored copies passed consistency checks (such as table checks, row counts and schema drift); customer checks on 0 of 4 databases. Missing for: billing, crm, inventory, webshop.	Gaps
NIS2 CIR 4.2.2(c)	Safe location, separate network, sufficient distance	The backup location of each database is listed below. Whether it is outside the production network and far enough from the main site is your assessment. Copies and the 3-2-1 rule were not checked (module check.copies).	For review
NIS2 CIR 4.2.2(d)	Access controls to backup copies	Restorly reads backups with the credentials it is given and does not change them while validating. Encrypted backups: 0 of 4 databases. Access controls on the backup storage are outside this report.	For review
NIS2 CIR 4.2.2(e)	Restoring data from backup copies	0 successful test restores of 0 of 4 databases into isolated containers. Missing for: billing, crm, inventory, webshop.	Gaps
NIS2 CIR 4.2.2(f)	Retention periods	Retention of backups Restorly does not take is set by your backup software and is outside this report.	For review
NIS2 CIR 4.2.3	Regular integrity checks on backup copies	Every validation checks that the newest backup exists, is fresh and reads without errors (checksum files verified where present); longest time between validations allowed here: 8 days, counted from the period's start or, for a database added later, from its first validation ("Since"). Missing for: billing, crm, inventory, webshop.	Gaps
ISO 27001 A.8.13	Information backup: copies maintained and regularly tested	Backups were present and within their maximum age at the latest validation, and restored in tests during the period. Missing for: billing, crm, inventory, webshop.	Gaps
ISO 27001 A.5.30	ICT readiness for business continuity	Test restores with measured duration show the backups can be brought back. Continuity objectives and plans are yours. Missing for: billing, crm, inventory, webshop.	Gaps

Databases

Database	Location	Validations	Restores	Median / max restore	Longest gap Since	Latest
billing	nas (local)	0 (0 failed)	0	- / -	304 days start	no signed runs
crm	nas (local)	0 (0 failed)	0	- / -	304 days start	no signed runs
inventory	nas (local)	0 (0 failed)	0	- / -	304 days start	no signed runs
webshop	nas (local)	0 (0 failed)	0	- / -	304 days start	no signed runs

Failures

No signed validation failed in this period.

Requirements referred to

Directive (EU) 2022/2555 (NIS2), Article 21(2)(c): "business continuity, such as backup management and disaster recovery, and crisis management".

Commission Implementing Regulation (EU) 2024/2690, Annex, point 4.2.2: "Based on the results of the risk assessment carried out pursuant to point 2.1 and the business continuity plan, the relevant entities shall lay down backup plans which include the following: (a) recovery times; (b) assurance that backup copies are complete and accurate, including configuration data and data stored in cloud computing service environment; (c) storing backup copies (online or offline) in a safe location or locations, which are not in the same network as the system, and are at sufficient distance to escape any damage from a disaster at the main site; (d) appropriate physical and logical access controls to backup copies, in accordance with the asset classification level; (e) restoring data from backup copies; (f) retention periods based on business and regulatory requirements."

Point 4.2.3: "The relevant entities shall perform regular integrity checks on the backup copies."

The Implementing Regulation applies to digital infrastructure and digital provider entities, including managed service and managed security service providers; other entities can use it as a reference for Article 21(2)(c).

ISO/IEC 27001:2022, Annex A controls 8.13 (Information backup) and 5.30 (ICT readiness for business continuity). The standard's text is not reproduced here.

Evidence index

Every signed report used above, with the SHA-256 of its JSON file. The JSON reports are the evidence: check them at <https://restorly.eu/verify>, in a browser (nothing is uploaded or installed), or with `restorly report verify --key report-signing.pub <files>`; both also check the hash chain across reports.