TOMORIS
MORE THAN IT

FREE DOWNLOAD

CHECKLIST · TOMORIS TOOLBOX

NIS2 Risk Management: The Measures Under § 32 NISG 2026 as a Checklist

The minimum contents under § 32 para. 4 NISG 2026 with the Annex of Implementing Regulation (EU) 2024/2690, evidence ideas, management body duties and self-declaration

UPDATED	LENGTH	ONLINE
Oct 25, 2026	PDF, 11 pages	tomoris.com/en/downloads/nis2-risikomanagement-checkliste

AT A GLANCE

10
minimum contents under § 32 para. 4 lit. a to j NISG 2026

13
points in the Annex of IR (EU) 2024/2690

annually
management reviews the security policy

2027
self-declaration by Sep 30, 2027

WHO IT IS FOR

- Information security officers and CISOs of essential and important entities under the NISG 2026
- Managing directors, executive boards and other management bodies that must ensure and oversee implementation
- IT management, compliance and internal audit who collect evidence and prepare the self-declaration

Redistribution in unchanged form permitted

WHAT THIS COVERS

Since October 1, 2026, essential and important entities must implement risk management measures under § 32 NISG 2026. What the ten minimum contents require in detail is set out in the Annex of IR (EU) 2024/2690; § 2 NISV 2026 extends it to all essential and important entities to which it does not already apply. This checklist maps each letter of § 32 para. 4 to the points of the Annex, summarizes the core of each requirement and lists evidence you should keep on hand. It also covers the duties of the management bodies under § 31, proportionality and compensating measures, and the self-declaration, audits and deadlines under § 33.

These checklists are a TOMORIS recommendation and do not replace legal advice. The NISG 2026 and NISV 2026 as currently in force, the Annex of Implementing Regulation (EU) 2024/2690 (via § 2 NISV 2026 in the version at the time of its entry into force) and the cybersecurity authority's requirements for the self-declaration are authoritative. The evidence ideas are examples; the ENISA guidance is not binding.

CONTENTS

01 What this is about and what is binding 3
02 Mapping: § 32 para. 4 NISG 2026 and the Annex of the Implementing Regulation 3
03 Checklist 1: policies, risk, incidents, operations 4
04 Checklist 2: supply chain, procurement, operations 5
05 Checklist 3: training, access, assets, environment 6
06 Duties of the management bodies (§ 31 NISG 2026) 7
07 Proportionality and compensating measures 8
08 Self-declaration, audits and deadlines (§ 33 NISG 2026) 9
09 Common mistakes 10
10 Sources 11

01

What this is about and what is binding

Ten minimum contents in the NISG 2026, details in the Annex of the Implementing Regulation, evidence ideas as a recommendation.

Since October 1, 2026, essential and important entities must implement appropriate and proportionate technical, operational and organizational risk management measures (§ 32 paras. 1 and 2 NISG 2026). They are based on an all-hazards approach and include at least the ten contents of § 32 para. 4 lit. a to j, which transpose Art. 21(2) of the NIS2 Directive.

- Binding: §§ 31 to 33 NISG 2026 with management duties, minimum contents and evidence.
- Binding: the Annex of Implementing Regulation (EU) 2024/2690 with thirteen points, directly for digital providers such as cloud and managed services, and for all other entities via § 2 NISV 2026.
- Not binding: the ENISA guidance (June 2025) and the FAQ of the Austrian Federal Office for Cybersecurity (BCS).
- Exception: equivalent EU sector-specific law such as DORA displaces § 32 to that extent (§ 27 NISG 2026).

> How to read the tables: the “core of the requirement” is binding; where the Annex says “where appropriate, applicable or feasible”, you may deviate only with documented reasons (Art. 2(2) IR).

02

Mapping: § 32 para. 4 NISG 2026 and the Annex of the Implementing Regulation

Which points of the Annex specify the ten letters of § 32 para. 4 NISG 2026.

§ 32 para. 4 NISG 2026 (Art. 21(2) NIS2 Directive) and Annex points by headings and introductory sentences

POINT	MINIMUM UNDER § 32 PARA. 4 NISG 2026	ANNEX POINT
a	Policies on risk analysis and information system security	1, 2
b	Incident handling	3
c	Business continuity: backup, recovery, crisis management	4, 13.1
d	Supply chain security, including with direct suppliers	5
e	Acquisition, development, maintenance; vulnerability handling and disclosure	6, 13.2
f	Assessing the effectiveness of risk management measures	7
g	Basic cyber hygiene and training	8
h	Cryptography and, where appropriate, encryption	9

i	Human resources security, access control, asset management	10 to 12, 13.3
j	MFA or continuous authentication; secured communications	11 (11.7)

03

Checklist 1: policies, risk, incidents, operations

Points (a) to (c), Annex points 1 to 4: policy, roles, risks, incidents, contingency, backup and crisis.

Points (a) to (c): Annex points 1 to 4 of Implementing Regulation (EU) 2024/2690; evidence ideas based on ENISA

ANNEX POINT	CORE OF THE REQUIREMENT (BINDING)	EVIDENCE IDEAS (RECOMMENDATION)
1.1 Policy	Policy on the security of network and information systems with objectives, resources, roles and metrics, formally approved by the management bodies and reviewed at least annually (1.1).	Policy with approval date; acknowledgment by employees; review minutes.
1.2 Roles	Responsibilities defined and communicated to management; at least one person reports directly to the management bodies (1.2).	Dated organizational chart with reporting line; formal appointment to the roles.
2.1 Risks	Methodology and criteria; identify and assess risks using an all-hazards approach; treatment plan; residual risks accepted; reviewed at least annually (2.1); categories under § 3 NISV 2026.	Methodology; risk register; treatment plan; approval of residual risks.
2.2, 2.3 Review	Review compliance regularly and report to management; independent review at planned intervals, internally only by people who do not report to the area under review, otherwise alternative measures for impartiality (2.2, 2.3).	Audit plan and audit reports; list of approved exceptions.
3.1, 3.2 Incidents	Policy for detection, containment, recovery and reporting, aligned with the contingency plan; monitoring and protected logs (3.1, 3.2).	Incident categories; escalation plan; logging settings.
3.3 to 3.6 Response	Simple reporting channel for employees, suppliers and customers; assessment based on predefined criteria; check quarterly for recurring incidents (3.4.2(b), otherwise § 7 NISV 2026 by analogy); response following documented procedures; tests; document lessons learned (3.3 to 3.6).	Reporting channels; playbooks; list of reporting obligations and deadlines; test records.
4.1 Contingency	Contingency plan based on the risk assessment; business impact analysis; plan tested at planned intervals (4.1).	Contingency plan; analysis with recovery objectives; test reports.
4.2 Backup, redundancy	Backup plans with recovery times; copies not on the same network and sufficiently distant; regular integrity checks; at least partial redundancy of systems, assets, staff and communication channels; recovery tests with documented results (4.2).	Backup plan; backup logs; test reports with times achieved.
4.3 Crisis	Crisis management with roles, means of communication with the authorities and security measures; plan tested (4.3).	Crisis team with deputies; crisis communication plan; exercise reports.

04

Checklist 2: supply chain, procurement, operations

Points (d) to (f), Annex points 5 to 7: supply chain, acquisition, changes, patches, network and effectiveness.

Points (d) to (f): Annex points 5 to 7 of Implementing Regulation (EU) 2024/2690; evidence ideas based on ENISA

ANNEX POINT	CORE OF THE REQUIREMENT (BINDING)	EVIDENCE IDEAS (RECOMMENDATION)
5.1 Supply chain	Policy with selection criteria for direct suppliers; contracts, where appropriate, with security requirements, incident reporting, audit rights and obligations at contract termination (5.1).	Policy; contracts with the clauses from 5.1.4; list of incidents at suppliers.
5.2 Suppliers	Current register of direct suppliers with contact point and the ICT products, services and processes supplied (5.2).	Register with change history; classification by criticality.
6.1, 6.2 Acquisition	Security requirements when acquiring ICT products and services, including updates throughout the lifetime; rules for secure development, including outsourced development (6.1, 6.2).	Tender templates; development rules; separate test environment.
6.3, 6.4 Changes	Define and enforce secure configurations; document changes and test them beforehand; justify emergency changes afterwards (6.3, 6.4).	Baseline configuration with exceptions; change logs; rollback plans.
6.5, 6.6 Patches	Plan security testing based on risk; patches within a reasonable time, tested, from a trusted source; not applying a patch documented and justified (6.5, 6.6).	Penetration test reports; patch history; justification when a patch is not applied.
6.7, 6.8 Network	Network architecture documented; unnecessary services disabled; remote access controlled; plans for new network protocols and email standards; zones based on risk (6.7, 6.8).	Network diagrams; firewall rule sets; zone model.
6.9, 6.10 Malware, vulnerabilities	Protection against malware and unauthorized software; remediate critical vulnerabilities without undue delay; coordinated disclosure procedure (6.9, 6.10).	EDR settings; scan logs; evidence of remediation.
7 Effectiveness	Define what is measured and analyzed, how, when and by whom; review at planned intervals (7).	Metrics; reports to the management bodies.

05

Checklist 3: training, access, assets, environment

Points (g) to (j), Annex points 8 to 13: training, cryptography, staff, access, MFA, assets, environment.

Points (g) to (j) and point 13 (points (c), (e), (i)): Annex points 8 to 13 of Implementing Regulation (EU) 2024/2690; evidence ideas based on ENISA

ANNEX POINT	CORE OF THE REQUIREMENT (BINDING)	EVIDENCE IDEAS (RECOMMENDATION)
8.1 Hygiene	Awareness raising for all employees, including the management bodies, recurring and for new employees, on threats and cyber hygiene (8.1).	Program with dates; attendance lists; test results.
8.2 Training	Identify roles with security tasks and train them regularly; assess effectiveness (8.2).	Training plan per role; proof of attendance.
9 Cryptography	Policy on the type and strength of cryptography based on classification, approved algorithms and key management; reviewed against the state of the art (9).	Policy with algorithms and key lengths.
10 Staff	Duties known and binding; roles reviewed at least annually; background checks where feasible; duties after leaving; disciplinary procedure (10).	List of roles; confidentiality clauses; screening procedure.
11.1 to 11.4 Access	Access control policy; rights based on need-to-know and segregation of duties, in a register, reviewed regularly; dedicated administrative accounts with strong authentication (11.1 to 11.4).	Permissions register; review records; list of privileged accounts.
11.5 to 11.7 MFA	Unique identifiers per person; lockout after failed attempts; where appropriate, multiple factors or continuous authentication based on classification (11.5 to 11.7).	Sign-in logs; MFA configuration; approved exceptions.
12 Assets	Classification by confidentiality, integrity, authenticity and availability; rules through to deletion; removable media; current inventory (12).	Classification scheme; inventory with change history.
13 Environment	Protection against failure of supporting utilities such as power and telecommunications and against physical threats; physical access control; tests (13).	Environmental monitoring; list of people with physical access.
Point (j) communications	Secured voice, video and text communications and, where appropriate, secured emergency communication systems within the entity (§ 32 para. 4 lit. j). No separate point in the Annex; related are communication channels in the contingency plan (4.1.2(c)), redundant channels (4.2.4(d)), means of communication with the authorities (4.3.2(b)) and encryption of transmitted data (9.2(a)).	TOMORIS recommendation: define encrypted services; define and test a fallback channel for emergencies, because according to ENISA the usual channels may not be secure in a crisis.

06

Duties of the management bodies (§ 31 NISG 2026)

Ensure, oversee, approve, get trained: what executive management must do itself.

A management body is whoever is appointed by law, articles of association or contract to manage the business (§ 3 no. 11 NISG 2026); according to the BCS, this means, for example, the managing directors or the executive board, not the IT management or the CISO. The management bodies must ensure and oversee compliance with the risk management measures (§ 31 para. 1), according to the explanatory notes to the government bill including approval of the requirements (cf. Art. 20(1) NIS2 Directive), and must take part in cybersecurity training designed for them (§ 31 para. 2).

- [ ] Security policy approved and reviewed annually (IR Annex points 1.1.1(k), 1.1.2).
- [ ] Resources committed: staff, funding, processes and technologies (point 1.1.1(e)).
- [ ] At least one person is directly accountable to management for security (point 1.2.3).
- [ ] Risk assessment and residual risks accepted by management or authorized persons (point 2.1.1).
- [ ] Regular reports on the security status and on independent reviews (points 2.2.1, 2.3.3).
- [ ] Every member of executive management trained, attendance documented (according to the BCS, employee training is not sufficient); employees are offered training regularly (§ 31 para. 2).
- [ ] Management signs audit reports together with the auditors (§ 33 para. 3) and approves the self-declaration (recommendation).

Consequences: The district administrative authority may fine legal entities under § 45, as a priority according to the explanatory notes (§ 44 paras. 3 and 4). Liability under § 9 VStG remains for external representatives, such as managing directors, unless responsible agents are appointed; if the entity is penalized for the same violation, they must not be penalized (§ 44 para. 5). The explanatory notes and BCS state that NISG 2026 provides no separate penalties for management bodies; damages for negligent conduct remain possible. The authority may temporarily prohibit management functions at essential entities (§ 39 para. 4 no. 2).

07

Proportionality and compensating measures

How size and risk determine implementation and when you may deviate with reasons.

Proportionality takes into account the entity's exposure to risks and that of its services, its size, and the likelihood and severity of incidents, including their societal and economic impact (§ 32 para. 3 NISG 2026, Art. 2(2) IR). According to the explanatory notes to the NISV 2026, the Annex is a framework, not a specific implementation description. An example from the BCS: in a micro-enterprise, keeping the inventory and supplier register in a spreadsheet may still be feasible.

Two ways to deviate from a requirement

Compensating measure `§ 4 NISV 2026`	If you cannot meet a requirement temporarily or because of your size, you implement compensating measures that fulfill its purpose as far as possible based on a risk assessment, document them with reasons and review their effectiveness at least annually. According to the explanatory notes, temporarily means, for example, an ongoing procurement procedure; for this, the BCS expects a specific schedule for the actual implementation. Size is not a blanket argument.
Justified non-application `Art. 2(2), second subparagraph, IR`	Where the Annex says "where appropriate", "applicable" or "feasible", a clearly documented justification of why the requirement does not fit you is sufficient; you then do not have to compensate (§ 4 para. 4 NISV 2026). Examples: points 1.2.5, 3.2.2 and 11.7.1.

08

Self-declaration, audits and deadlines (§ 33 NISG 2026)

Self-declaration by September 30, 2027, request for an audit no earlier than October 1, 2028, penalty ranges.

Deadlines from the entry into force of the NISG 2026

Oct 1, 2026
Obligations apply

§§ 31 to 33 NISG 2026 in force (§ 51 para. 2); NISV 2026 since the end of that day (§ 9 NISV).

Jan 1, 2027
Registration

Within three months of entry into force (§ 29 para. 3) via NIS2 Services in the USP (Austrian business service portal); according to the BCS by January 1, 2027, and because of § 33 para. 2 AVG (Austrian General Administrative Procedure Act) by January 4, 2027, at the latest. The BCS FAQ states December 31, 2026.

Sep 30, 2027
Self-declaration

Within twelve months after the registration obligation arises (§ 33 para. 1), according to the BCS by September 30, 2027.

from Oct 1, 2028
Audit possible

First request for evidence from an independent body no earlier than two years after entry into force (§ 33 para. 2).

The self-declaration provides information on the measures implemented, in particular on the network and information systems used, supply chain security and the results of the risk analysis (§ 33 para. 1). According to the BCS, it will be a form with short, specific questions in the business service portal (USP) and will not replace an audit. Entities that become essential or important later count the twelve months from the date the conditions are met (explanatory notes on § 33). Preparation, recommended by TOMORIS:

- [ ] Inventory of services and systems (Annex point 12.4) and register of direct suppliers (point 5.2) up to date.
- [ ] Risk analysis with the four categories of § 3 NISV 2026 (technological, human, ICT supply chain, location-related), treatment plan and accepted residual risks.
- [ ] Status recorded for each row of checklists 1 to 3, with responsible people and dates; deviations documented with reasons.
- [ ] Access to the USP clarified; defined who fills in and who approves; information checked against the evidence.

Evidence from an independent body (§ 33 paras. 2 to 5 NISG 2026)

ITEM	RULE
Request	According to the BCS, no earlier than Oct 1, 2028; for important entities only if the authority learns from evidence such as the self-declaration or from other substantiated indications that the entity presumably does not meet its obligations (§ 33 para. 2, § 38 para. 2).
Deadlines	Two years from the request; essential entities provide evidence of the operational and organizational implementation within two months (§ 33 para. 2).
Certificates	Valid relevant certificates can demonstrate operational and organizational implementation (§ 33 para. 2), but according to the BCS not technical implementation. The scope must cover the entire entity; partial recognition is possible, and you prove the rest through an audit. The scope, deviations and any audit reports are sent to the authority together with the certificate.
Audit report	Signed by the management bodies and the auditors, with deficiencies and an action plan (§ 33 para. 3); audit plan sent to the authority one month in advance (para. 5).

Penalty ranges (§§ 45 and 46 NISG 2026)

VIOLATION	REFERENCE	PENALTY RANGE
Measures under § 32 not implemented, unless the authority knows this only from the self-declaration; training under § 31 para. 2 not provided	§ 45 para. 1 nos. 1 to 3	essential entity up to €10 million or 2%, important entity up to €7 million or 1.4% of the previous year's worldwide turnover of the undertaking to which it belongs, whichever is higher
Registration, self-declaration or audit report not on time; self-declaration knowingly false; audit not announced	§ 45 para. 4 nos. 1, 7 to 10	up to €50,000, for repeat offenses up to €100,000
Authorities and other public administration bodies, including municipalities	§ 46 para. 2, § 39 para. 6	no fine under § 45: determination by official decision with a deadline, publication in case of non-compliance; no prohibition of management functions

09

Common mistakes

What makes implementing § 32 NISG 2026 and providing evidence to the cybersecurity authority harder in practice.

- Management only informed: approving the policy and the individual training of each member are tasks of the management bodies; residual risks are accepted by management or an authorized person who reports to it (IR Annex points 1.1.1(k), 2.1.1; § 31 para. 2 NISG 2026).
- Outsourcing as relief: according to the BCS, the entity itself remains responsible even if a service provider runs the IT; requirements belong in the contract where appropriate (point 5.1.4).
- Plans never tested: incident response, contingency plan, recovery and crisis management must be tested at planned intervals (points 3.5.5, 4.1.4, 4.2.6, 4.3.4).

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 **NISG 2026, BGBl. I No. 94/2025, version in force in the RIS**
Version of October 25, 2026 (original version); §§ 3 no. 11, 27, 29, 31 to 33, 38, 39, 44 to 46, 51; accessed October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...

2 **NISV 2026, BGBl. II No. 290/2026, authentic promulgation in the RIS**
§§ 2 to 4 risk management measures, § 7, § 9 entry into force; accessed October 25, 2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290

3 **Federal Office for Cybersecurity: Explanatory notes to the NISV 2026 (PDF)**
General part, on §§ 2, 4 and 8: framework, DORA, § 7 by analogy, compensating measures, references; accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut...

4 **Explanatory notes to the government bill NISG 2026 (308 d. B. XXVIII. GP), at the Federal Office for Cybersecurity (PDF)**
On §§ 31, 44 and 45 (approval, penalty addressee, § 9 VStG) and on § 33 (self-declaration); accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/501/files/nis-2026-gesetzer...

5 **Verwaltungsstrafgesetz 1991 (VStG, Austrian Administrative Penal Act), § 9, in the RIS**
§ 9 para. 1 liability of those authorized to represent externally; accessed October 25, 2026
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...

6 **Directive (EU) 2022/2555 (NIS2 Directive), Art. 20 and 21**
Art. 20(1) and Art. 21(2); OJ L 333 of December 27, 2022; accessed October 25, 2026
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu

7 **Implementing Regulation (EU) 2024/2690, Art. 2 and Annex**
Art. 1, 2 and Annex points 1 to 13; OJ L of October 18, 2024; accessed October 25, 2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu

8 **ENISA: NIS2 Technical Implementation Guidance, June 2025, Version 1.0**
Examples of evidence for points 1 to 13, guidance on 4.3.2; not binding according to ENISA; accessed October 25, 2026
www.enisa.europa.eu/publications/nis2-technical-implementation-...

9 **Federal Office for Cybersecurity: Registration**
Initial registration by January 1, 2027, at the latest January 4, 2027 (§ 33 para. 2 AVG), NIS2 Services; page of October 2, 2026, accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/303/registrierung.html

10 **Federal Office for Cybersecurity: Frequently asked questions, registration**
Registration by December 31, 2026, via the USP; page of September 25, 2026, accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/faq/registrierung.html

11 **Federal Office for Cybersecurity: Frequently asked questions, executive management**
Management body, training per member, no administrative penalties; page of September 25, 2026, accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/faq/geschaeftsleitung.html

12 **Federal Office for Cybersecurity: Frequently asked questions, measures**
Responsibility for outsourced IT; page of October 15, 2026, accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/faq/massnahmen.html

13 **Federal Office for Cybersecurity: Frequently asked questions, § 2 requirements for risk management measures**
Proportionality with spreadsheet example; page of October 20, 2026, accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/faq/anforderungen-an-risiko...

14 **Federal Office for Cybersecurity: Frequently asked questions, § 4 compensating measures**
Schedule for temporary deviations; page of October 20, 2026, accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/faq/kompensierende-massnahm...

15 **Federal Office for Cybersecurity: Frequently asked questions, evidence**
Self-declaration by September 30, 2027, via the USP, ISO 27001, scope, partial recognition; page of September 25, 2026, accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/faq/nachweise.html

16 **Federal Office for Cybersecurity: Audits by independent bodies**
Request no earlier than October 1, 2028, deadlines, certificates with scope; page of September 21, 2026, accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/303/ueberpruefung-durch-una...