TOMORIS
MORE THAN IT

FREE DOWNLOAD

TEMPLATE · TOMORIS TOOLBOX

Security Awareness: Annual Plan for Training and Awareness

Topics per quarter, audiences, formats, training for management bodies and evidence, based on NIST SP 800-50 Rev. 1, BSI ORP.3 and the NISG 2026

UPDATED
Oct 25, 2026

LENGTH
PDF, 8 pages

ONLINE
tomoris.com/en/downloads/security-awareness-jahresplan

AT A GLANCE

§ 31
NISG 2026: training for management and employees

3
Audiences according to NIST, from everyone to security roles

4
Quarters in the annual plan to fill in

Oct.
European Cybersecurity Month

WHO IT IS FOR

- Management that approves training and takes part in training itself
- Information security officers who plan and evaluate the program
- HR departments that look after new employees and records
- Managers who model and enforce security rules

Adaptation for your own use permitted; redistribute unchanged

WHAT THIS COVERS

A single mandatory talk once a year changes little. Effective awareness runs throughout the year, reaches every audience with suitable content and is measured. This template helps you set up an annual plan: define audiences, spread topics across four quarters, choose formats, schedule training for management bodies and document participation and effectiveness. It is based on NIST SP 800-50 Rev. 1, module ORP.3 of the BSI IT-Grundschutz-Kompendium and, for entities subject to NIS2, § 31 NISG 2026 (Austrian Network and Information Systems Security Act 2026) and Annex no. 8 of Implementing Regulation (EU) 2024/2690.

Adapt this template to your company, your risks and your tools; the topics, formats and rhythm are TOMORIS recommendations. It does not replace legal advice. For entities under the NISG 2026, the text of the law, the NISV 2026 and Implementing Regulation (EU) 2024/2690 in their current versions are decisive. Clear phishing exercises and evaluations with the works council and data protection in advance.

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

CONTENTS

01 What is required 2
02 Define audiences 3
03 Formats: raise awareness, practice, train 4
04 Annual plan to fill in 5
05 Training for management bodies 6
06 Evidence and effectiveness 6
07 Common mistakes 7
08 Sources 8

01

What is required

Obligations under the NISG 2026 and the Implementing Regulation, recommendations from the BSI and NIST

For essential and important entities, training is mandatory: management bodies must attend cybersecurity training designed specifically for them, and entities must offer similar training to their employees on a regular basis (§ 31 para. 2 NISG 2026, implementing Art. 20(2) of the NIS 2 Directive). Failing to provide for this is an administrative offense (§ 45 para. 1 nos. 1 and 2 NISG 2026); for public administration bodies, § 46 applies instead. For all other companies, the BSI and NIST describe what a good program looks like.

§ 31 para. 2 NISG 2026	Management bodies attend specifically designed cybersecurity training. The entity regularly offers similar training to its employees so that they can identify and assess risks and know cybersecurity management practices and their impact on the entity's services.
Implementing Regulation (EU) 2024/2690, Annex point 8.1	Awareness program for employees, members of management bodies and, where appropriate, direct suppliers: scheduled so that activities are repeated and reach new employees; covering cyber threats, existing measures, points of contact and cyber hygiene practices. Test effectiveness where appropriate, update the program at planned intervals.
Implementing Regulation (EU) 2024/2690, Annex point 8.2	Identify employees whose roles require security-relevant skills and train them regularly: secure configuration and operation including mobile devices, known cyber threats, behavior in security-relevant events; evaluate effectiveness, and also provide training when someone moves into such a role.
§ 2 NISV 2026 (Austrian NIS Regulation 2026)	Declares the Annex to the Implementing Regulation applicable also to the types of entities in Annexes 1 and 2 of the NISG 2026 that the Implementing Regulation itself does not cover; number 8 therefore applies to all essential and important entities.
BSI IT-Grundschutz, ORP.3	Module on information security awareness and training (Edition 2023): raise awareness among top management and obtain its support (A1), instruct staff in the secure use of IT (A3), audience-oriented program (A4), training according to tasks (A6), measure learning success (A8).
Art. 4 AI Act	Since the amendment by Regulation (EU) 2026/1744, providers and deployers of AI systems take measures to support the development of AI literacy of their staff; they do not have to guarantee a specific level of literacy.

> The topics, formats and annual rhythm in this template are TOMORIS recommendations. For entities subject to NIS2, the legal requirements are the content of § 31 NISG 2026 and Annex no. 8 of the Implementing Regulation cited above; they do not prescribe a specific frequency in months.

02

Define audiences

Who needs which content, from all employees to management

NIST divides participants into three overlapping groups: all users, holders of privileged accounts and persons with significant cybersecurity or privacy responsibilities (SP 800-50 Rev. 1, Section 2.5). The BSI recommends an audience analysis and a program tailored to it (standard requirement ORP.3.A4).

Audiences and focus areas

AUDIENCE	FOCUS	BASIS
All employees	Usage rules, recognizing attacks, reporting channel, cyber hygiene; refreshed continuously	§ 31 para. 2 NISG 2026; Implementing Regulation point 8.1; ORP.3.A3; NIST 2.5.1
Management bodies	Training designed for management on obligations, risks and decisions	§ 31 para. 2 NISG 2026; ORP.3.A1
Privileged accounts	Additional training on the rights and risks of administrative accounts	NIST 2.5.2
Security roles	Role-based training: secure configuration, threats, behavior in events	Implementing Regulation point 8.2; NIST 2.5.3
New employees and role changes	Rules for the systems they will access; training for a new role	Implementing Regulation points 8.1.2(a) and 8.2.4; NIST 3.1.2.2
External parties and suppliers	Instruction of external users and, where appropriate, direct suppliers	ORP.3.A3; Implementing Regulation point 8.1.2
Particularly exposed persons	In-depth training on targeted attacks and precautions (elevated protection needs)	ORP.3.A9

03

Formats: raise awareness, practice, train

The three building blocks of a program and how to mix them

Awareness	Ongoing throughout the year, as a campaign or event-driven, e.g. notices on the login screen, newsletter articles, posters, action days in October, short emails with tips or after an incident (NIST 2.7.1).
Exercise	Practical scenarios that simulate events: phishing, smishing or vishing simulations, quizzes, tabletop exercises, emergency and recovery exercises (NIST 2.7.2).
Training	Conveys knowledge and skills, as an in-person or online course, demonstration or scenario-based exercise; role-based for people with security tasks (NIST 2.5.3, 2.7.3).

> Phishing exercises are learning opportunities: NIST recommends first determining the baseline click rate per group and stresses that such exercises should not be punitive and that no one should be singled out for their response (Section 2.7.2). Clear simulations with the works council and data protection in advance.

04

Annual plan to fill in

Topics spread across four quarters, with audience, format and date

The topics are a TOMORIS proposal and cover the content listed in Annex point 8.1.2(c) of the Implementing Regulation: cyber threats, existing measures, points of contact and cyber hygiene practices. Adapt the order and topics to your risks, incidents and tools, and enter dates and responsible persons.

Annual plan [Year] for [Company] (TOMORIS proposal)

PERIOD	TOPIC	AUDIENCE	FORMAT	DATE, RESPONSIBLE
Q1	Kickoff: goals, rules, incident reporting channel	everyone	Short training	_____
Q1	Training for management bodies	Management	Workshop	_____
Q1	Passwords, password managers, MFA	everyone	Online course	_____
Q2	Phishing and social engineering	everyone	Training	_____
Q2	Phishing exercise with evaluation	everyone	Simulation	_____
Q2	Handling data and data protection	everyone	Online course	_____
Q3	Mobile work, devices, updates	everyone	Short training	_____
Q3	Emergency: who does what?	Management, IT	Tabletop exercise	_____
Q3	Using administrative accounts securely	Admins	Training	_____
Q4	October: activities during Cybersecurity Month	everyone	Campaign	_____
Q4	Using AI tools securely	everyone	Training	_____
Q4	Evaluation and plan for the following year	Information security officer, management	Meeting	_____
ongoing	Onboarding of new employees	New hires	Onboarding	_____
ongoing	Alerts about current attacks	everyone	Email	_____

October is European Cybersecurity Month, an annual EU campaign supported by ENISA together with the European Commission. Your own activities during this month combine well with public materials.

05

Training for management bodies

What training designed for management should cover

The management bodies of essential and important entities must ensure and oversee compliance with the risk management measures (§ 31 para. 1 NISG 2026). Training under § 31 para. 2 should enable them to do so. The BSI also requires that top management be sufficiently sensitized and that its support be obtained before a program starts (ORP.3.A1). Content, TOMORIS recommendation:

- [ ] Management obligations: ensure and oversee (§ 31 para. 1), attend training personally (§ 31 para. 2).
- [ ] An overview of the minimum content of the risk management measures under § 32 para. 4 lit. a to j NISG 2026, from risk analysis to multi-factor authentication.
- [ ] Reporting obligations for significant incidents: early warning within 24 hours, notification within 72 hours, final report no later than one month afterward (§ 34 para. 2 NISG 2026).
- [ ] Self-declaration and evidence of measures to the cybersecurity authority (§ 33 NISG 2026).
- [ ] Penalty ranges: for essential entities up to €10 million or 2% of worldwide annual turnover, for important entities up to €7 million or 1.4%, whichever is higher (§ 45 paras. 2 and 3 NISG 2026); for public administration bodies, a declaratory administrative decision instead of a fine (§ 46).
- [ ] The current threat landscape and the risks of your own company (Implementing Regulation point 8.1.3).
- [ ] Your own role in an emergency: decisions, availability, communication.
- [ ] Leading by example: managers implement security requirements and remind their employees to comply (ORP.3.A1).

06

Evidence and effectiveness

Document participation, measure learning success, improve the program

Participation figures alone are not enough: NIST requires measuring, beyond mere compliance, the impact on skills, attitudes and behavior (Section 2.4.1). The BSI recommends measuring learning success quantitatively and qualitatively for each audience and incorporating the results into the offering (ORP.3.A8).

- [ ] Participation documented per person: date, topic, format, duration, confirmation.
- [ ] Materials of each training archived with version date, so it is traceable what was taught.

- [ ] New employees instructed before first access, and this documented (TOMORIS recommendation, cf. NIST 3.1.2.2; the program must reach new employees, Implementing Regulation point 8.1.2(a)).
- [ ] Effectiveness measured, e.g. quiz with pass mark, practical test, click rate in phishing exercises (NIST 2.7.2 and 3.2, ORP.3.A8).
- [ ] Results discussed with HR and data protection (ORP.3.A8).
- [ ] Program updated at planned intervals (Implementing Regulation points 8.1.3, 8.2.5; ORP.3.A4), and additionally after incidents (NIST 2.5.1).
- [ ] For entities subject to NIS2: evidence of management body training readily available.

Attendance record (sample)

DATE	TOPIC	NAME	FORMAT, DURATION	CONFIRMATION
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

07

Common mistakes

Why awareness programs fail in practice

- Only one mandatory session per year. NIST describes awareness as an ongoing activity throughout the year (Section 2.7.1).
- Management is missing. According to the BSI, a program should not even start without its support (ORP.3.A1); management bodies subject to NIS2 must attend themselves.
- Everyone gets the same thing. Administrators and security roles need additional, role-based training (NIST 2.5.2, 2.5.3; Implementing Regulation point 8.2).
- Phishing exercises turn into public shaming. NIST expressly advises a non-punitive approach that does not single anyone out (Section 2.7.2).
- Only the participation rate is measured, not the impact on behavior (NIST 2.4.1, ORP.3.A8).
- New employees and external parties are forgotten (Implementing Regulation point 8.1.2, ORP.3.A3).

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

Link checker (German)
tomoris.com/tools/link-check

Email header analysis (German)
tomoris.com/tools/mail-header-analyse

DISCUSS IMPLEMENTATION

Get in Touch
tomoris.com/en/contact

contact@tomoris.com

08

Sources

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

1 **NIST SP 800-50 Rev. 1: Building a Cybersecurity and Privacy Learning Program (September 2024)**
Sections 2.4.1, 2.5, 2.7, 3.1 and 3.2, accessed October 25, 2026
doi.org/10.6028/NIST.SP.800-50r1

2 **BSI IT-Grundschutz-Kompendium, module ORP.3 Information Security Awareness and Training (Edition 2023)**
Requirements A1, A3, A4, A6, A8, A9, accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...

3 **NISG 2026, BGBl. I No. 94/2025, current version in the RIS**
§§ 31 to 34, 45 and 46, accessed October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...

4 **NISV 2026, BGBl. II No. 290/2026**
§ 2 applicability of the Implementing Regulation, accessed October 25, 2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290

5 **Implementing Regulation (EU) 2024/2690, German version on EUR-Lex**
Annex points 8.1 and 8.2, accessed October 25, 2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu

6 **Directive (EU) 2022/2555 (NIS 2 Directive), German version on EUR-Lex**
Art. 20(2), accessed October 25, 2026
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu

7 **Regulation (EU) 2026/1744 (Digital Omnibus Regulation on AI), OJ L of July 24, 2026**
Art. 1(5), new version of Art. 4 AI Act, accessed October 25, 2026
eur-lex.europa.eu/eli/reg/2026/1744/oj/deu

8 **ENISA: European Cybersecurity Month**
Description of the campaign, accessed October 25, 2026
www.enisa.europa.eu/topics/cyber-hygiene/european-cybersecurity...