

GOVERNANCE DOCS

EU NIS2 Directive

Gap Assessment Report

EU NIS2 Directive (Directive (EU) 2022/2555) cybersecurity risk-management measures

Alpenwerk Energy (sample)

The electricity distribution business, its control centre and the supporting IT and OT networks.

ASSESSED	25 September 2026
EDITION	Directive (EU) 2022/2555
IN SCOPE	60 requirements, 60 applicable
PROFILE	Energy and utilities · 250 to 999 people
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Alpenwerk Energy (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Alpenwerk Energy (sample) stands against NIS2

OVERALL READINESS

64.2%

Level 2 · Developing

The programme is under way, with material gaps an auditor would find.

Initial

Developing

Established

Audit-ready

APPLICABLE

60

EVIDENCED

19

OPEN GAPS

41

HIGH PRIORITY

12

STATUS OF EVERY REQUIREMENT

4

8

17

12

19

Not started

Planned

Partially implemented

Implemented, not evidenced

Implemented and evidenced

GAPS WITH AN OWNER

14 of 41

WITH A TARGET DATE

10 of 41

NOT ANSWERED

0

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 64.2% against NIS2 across 60 applicable controls. 19 of them are implemented and evidenced.
- Most open gaps: Governance and management liability, with 5 at 35%. Strongest area: 21(2)(i) HR security, access control and asset management at 95%.
- 12 controls are operating but not evidenced. Collecting their records alone lifts the score to 69.2% (+5.0 points), the cheapest gain available.
- 12 gaps are high priority (not started or only planned); 3 of them are in Governance and management liability.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 3 high-priority gaps in Governance and management liability	HR Manager	Cybersecurity Governance Management Accountability Policy
2	MEDIUM	Adopt and tailor the Cybersecurity Governance Management Accountability Policy, which closes 4 open gaps	To assign	Cybersecurity Governance Management Accountability Policy
3	LOW	Evidence the 12 controls that already operate (+5.0 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

With an overall score of 64.2%, you should focus immediately on formalizing governance and executive management approval.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our self-assessment shows a developing readiness level with an overall score of 64.2% across 60 requirements. Our primary exposure centers on governance oversight, supervisory readiness, and crisis testing, where 12 high priority gaps remain open. To ensure proper operational resilience and meet regulatory expectations, management requires board approval for key governance policies and authorization to assign formal remediation owners across departments.

WHERE YOU STAND

Your readiness level is 2 of 4, rated as Developing, with an overall score of 64.2%. Out of 60 applicable requirements, there are 41 open gaps, including 12 high priority gaps. Currently, 4 gaps are not started, 8 are planned, 17 are partially implemented, and 12 are implemented but not evidenced. Only 14 gaps have an assigned owner, and only 10 have target dates, indicating that remediation lacks structured execution.

WHAT IT MEANS FOR THE ORGANIZATION

Governance and management liability scored 35%, Cryptography scored 25%, and Supervision and enforcement scored 31.3%. Meanwhile, HR security, access control and asset management scored 95%. This pattern indicates that operational teams maintain good baseline hygiene, but senior leadership oversight and formal governance remain disconnected. Without formal management approval and clear accountability, technical measures lack strategic backing, leaving the organization exposed during formal regulatory reviews and operational disruptions.

WHERE TO FOCUS FIRST

Evidencing what already runs raises the score to 69.2%, while completing partially implemented controls achieves 83.3%. Initial efforts must target governance policies, incident reporting workflows, and business continuity validation. Establishing formal management body approval and supervisory readiness addresses key exposures immediately. Operating defined incident reporting procedures ensures your team can submit notifications within 24 hours during critical events. Assigning owners and dates to all 12 high priority gaps will ensure steady remediation.

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Formalize management body approval and governance oversight 20.1a Management body approval · 20.1b Oversight of implementation · 20.1c Awareness of personal liability	Unapproved governance frameworks leave executive leadership without clear accountability structures during regulatory reviews. Establishing formal oversight ensures cybersecurity measures receive operational backing and strategic direction.	Submit the governance accountability policy to senior leadership for formal adoption.	Cybersecurity Governance Management Accountability Policy NIS2 Toolkit - 75+ Comprehensive Templates	30 DAYS
2 Establish supervisory readiness and implementation tracking 32-33 Supervisory readiness · PROG Implementation programme	Operating without an active implementation programme creates significant exposure to supervisory scrutiny. A structured programme ensures audit activities and remedial actions proceed systematically across departments.	Consolidate open gaps and assign milestones using the readiness checklist.	NIS2 Checklist NIS2 Toolkit - 75+ Comprehensive Templates	30 DAYS
3 Implement mandatory incident reporting procedures 23.4a Early warning within 24 hours · 23.4d Final report within one month	Missing statutory reporting windows during operational disruptions damages regulatory standing. Establishing clear notification workflows ensures timely internal escalation and external reporting.	Integrate the early warning notification template into current operational response procedures.	NIS2 Early Warning Notification Template NIS2 Toolkit - 75+ Comprehensive Templates	60 DAYS
4 Validate disaster recovery and operational continuity plans 21.2c-3 Disaster recovery and testing · 21.2c-1 Business continuity plans	Untested continuity plans risk extended operational downtime during major infrastructure disruptions. Rigorous testing validates technical recovery steps and operational resilience under pressure.	Schedule a business continuity exercise following the testing plan framework.	Business Continuity Exercising and Testing Plan NIS2 Toolkit - 75+ Comprehensive Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS - Formally approve the Cybersecurity Governance Management Accountability Policy at executive level. - Deploy the NIS2 Checklist to map open remediation tasks across operational teams. - Assign designated owners and completion dates to each of the 12 high priority gaps.	DAYS 31 TO 60 - Operationalize incident notification workflows using the NIS2 Early Warning Notification Template. - Implement the Cryptographic Policy to establish baseline controls for encryption and key management. - Compile formal evidence for the 12 requirements currently implemented without documentation.	DAYS 61 TO 90 - Conduct operational continuity testing using the Business Continuity Exercising and Testing Plan. - Review key third-party relationships using the Directory of Suppliers and Service Providers. - Initiate internal oversight checks under the Internal Audit and Compliance Review Procedure.
---	---	--

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

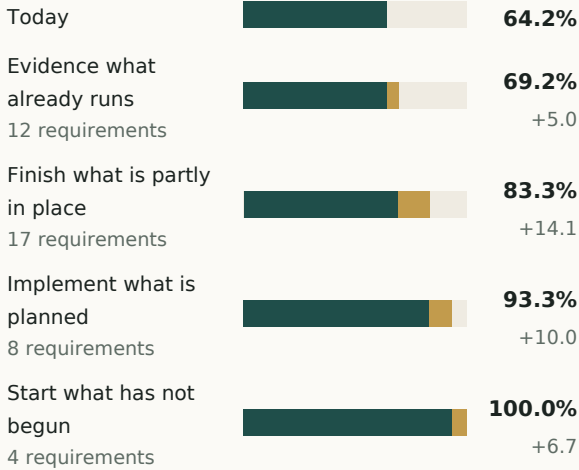
AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope and registration	1 2 3	83%	0 1 2
Governance and management liability	1 2 1 1	35%	3 1 1
21(2)(a) Risk analysis and security policies	1 1 2	81%	0 1 1
21(2)(b) Incident handling	1 1 2	81%	0 1 1
21(2)(c) Business continuity and crisis management	1 2 1	50%	1 2 1
21(2)(d) Supply chain security	2 1 1	69%	0 2 1
21(2)(e) Secure acquisition, development and maintenance	1 3	88%	0 1 0
21(2)(f) Effectiveness of measures	1 1 1	67%	1 0 1
21(2)(g) Cyber hygiene and training	2 1	33%	2 1 0
21(2)(h) Cryptography	1 1 1	25%	2 1 0
21(2)(i) HR security, access control and asset management	1 4	95%	0 0 1
21(2)(j) Authentication and secured communications	3 1	63%	0 3 0
Incident reporting	1 2 2 2	68%	1 2 2
Supervision and enforcement	2 1 1	31%	2 1 1

Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced

Where the next points come from

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.



DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.



All of these are in the NIS2 Toolkit (78 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 4

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
20.1a	Management body approval	Governance and management liability	To assign	Cybersecurity Governance Management Accountability Policy
21.2h-2	Encryption applied	21(2)(h) Cryptography	Operations Manager 7 Jan 2027	Cryptographic Policy · Data Masking Pseudonymisation Policy
32-33	Supervisory readiness	Supervision and enforcement	Risk Manager 4 Feb 2027	NIS2 Checklist · Internal Audit and Compliance Review Procedure
PROG	Implementation programme	Supervision and enforcement	Compliance Lead 26 Nov 2026	NIS2 Project Plan · NIS2 Checklist

HIGH Planned · 8

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
20.1b	Oversight of implementation	Governance and management liability	To assign	Cybersecurity Governance Management Accountability Policy · Internal Audit and Compliance Review Procedure
20.1c	Awareness of personal liability	Governance and management liability	HR Manager 12 Nov 2026	Technical Briefing on Security Roles and Responsibilities Matrix · Cybersecurity Governance Management Accountability Policy
21.2c-3	Disaster recovery and testing	21(2)(c) Business continuity and crisis management	To assign	Business Continuity Exercising and Testing Plan · Business Continuity Exercising and Testing Report
21.2f-3	Improvement actions	21(2)(f) Effectiveness of measures	To assign	Internal Audit and Compliance Review Procedure · Cybersecurity Control Effectiveness and Improvement Procedure
21.2g-1	Basic cyber hygiene	21(2)(g) Cyber hygiene and training	To assign	NIS2 Cybersecurity Operations Policy · Malware & Cyber Threat Protection Policy

21.2g-3	Acceptable use	21(2)(g) Cyber hygiene and training	To assign	Acceptable Use and Communications Policy
21.2h-3	Key management	21(2)(h) Cryptography	IT Manager 21 Jan 2027	Cryptographic Policy
23.4a	Early warning within 24 hours	Incident reporting	IT Manager 24 Dec 2026	NIS2 Early Warning Notification Template

MEDIUM

Partially implemented · 17

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
SC.3	Size threshold assessment	Scope and registration	To assign	NIS2 Scope and Registration Document · NIS2 Checklist
20.2a	Management body training	Governance and management liability	Operations Manager 24 Dec 2026	Cybersecurity Training Records Log
21.2a-3	Risk treatment	21(2)(a) Risk analysis and security policies	HR Manager	Risk Treatment Plan · Acceptance of Residual Risks
21.2b-4	Incident records	21(2)(b) Incident handling	To assign	Significant Incident Reporting Form · Minor Incident Response Procedure
21.2c-1	Business continuity plans	21(2)(c) Business continuity and crisis management	To assign	BCM Crisis and Operational Resilience Plan
21.2c-2	Backup management	21(2)(c) Business continuity and crisis management	IT Manager 21 Jan 2027	Backup and Recovery Policy · Data Restoration Form
21.2d-1	Supplier register	21(2)(d) Supply chain security	To assign	Directory of Suppliers and Service Providers
21.2d-3	Contractual security requirements	21(2)(d) Supply chain security	IT Manager 4 Feb 2027	Supply Chain and Third Party Security – Policy Procedure and Agreement
21.2e-2	Secure development	21(2)(e) Secure acquisition, development and maintenance	To assign	Secure Development and Software Supply Chain Policy · Secure Coding Policy
21.2g-2	Security awareness training	21(2)(g) Cyber hygiene and training	To assign	Cybersecurity Training Records Log
21.2h-1	Cryptography policy	21(2)(h) Cryptography	Risk Manager	Cryptographic Policy
21.2j-1	Multi-factor authentication	21(2)(j) Authentication and secured communications	To assign	Access Control Identity Management Policy

21.2j-2	Secured voice, video and text	21(2)(j) Authentication and secured communications	IT Manager	Information Transfer and Secure Communications Procedure
21.2j-4	Remote access security	21(2)(j) Authentication and secured communications	Risk Manager	Mobile Computing and Remote Access Policy · Remote Working Policy
23.1	Notifying service recipients	Incident reporting	To assign	Stakeholder Email Templates · Communication Plan
23.4d	Final report within one month	Incident reporting	To assign	Significant Incident Reporting Form · Minor Incident Response Procedure
34	Awareness of penalty exposure	Supervision and enforcement	HR Manager 21 Jan 2027	Cybersecurity Governance Management Accountability Policy

LOW Implemented, not evidenced · 12

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
SC.4	Member state and jurisdiction	Scope and registration	To assign	Legal Regulatory and Compliance Obligations Policy
SC.5	National registration	Scope and registration	To assign	NIS2 Scope and Registration Document · Key Contacts Register
20.2b	Employee training offered	Governance and management liability	To assign	Cybersecurity Training Records Log
21.2a-4	Risk register maintained	21(2)(a) Risk analysis and security policies	To assign	NIS2 Information Risk Register
21.2b-1	Incident handling process	21(2)(b) Incident handling	To assign	Significant Incident Handling Procedure · Minor Incident Response Procedure
21.2c-4	Crisis management	21(2)(c) Business continuity and crisis management	To assign	BCM Crisis and Operational Resilience Plan · Communication Plan
21.2d-2	Supplier risk assessment	21(2)(d) Supply chain security	To assign	Supply Chain Third Party Risk Assessment Form
21.2f-2	Internal audit	21(2)(f) Effectiveness of measures	To assign	NIS2 Audit Plan · NIS2 Audit Schedule +1 more
21.2i-5	Information classification and handling	21(2)(i) HR security, access control and asset management	To assign	Information Classification and Handling Policy · Information Classification Matrix +1 more
23.3	Awareness trigger	Incident reporting	To assign	Significant Incident Handling Procedure · NIS2 Cybersecurity Roles and Responsibilities
23.4c	Intermediate reports	Incident reporting	To assign	Significant Incident Handling Procedure

32.4	Ability to act on binding instructions	Supervision and enforcement	To assign	Cybersecurity Control Effectiveness and Improvement Procedure
------	--	-----------------------------	-----------	---

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com