Ansvar

CONFIDENTIAL

GAP ANALYSIS

Gap Analysis Report

nis2 — EU, EE

PREPARED FOR	Baltika Freight Systems OÜ — a fictional 90-person Estonian SaaS company providing freight-forwarding and customs-clear…
REFERENCE	63f045b3-1299-4057-9a5a-431b0e0fe43c
GENERATED	2026-07-11T18:30:01.857645+00:00
SOURCE	workflow:63f045b3-1299-4057-9a5a-431b0e0fe43c

CONTENTS

OVERVIEW

Executive Summary

10	0	2	6
CONTROLS	FULLY COMPLIANT	LARGELY COMPLIANT	PARTIAL

2	2
NOT IMPLEMENTED	CRITICAL GAPS

METHODOLOGY

Scope & Methodology

FRAMEWORK	nis2
JURISDICTIONS	EU, EE
ENTITY	Baltika Freight Systems OÜ — a fictional 90-person Estonian SaaS company providing freight-forwarding and customs-clearance software (Baltika TMS) to logistics operators in the Baltic region. Presumed "important entity" under NIS2 (digital-infrastructure-adjacent transport logistics software). Assessment subject: the company's Information Security Policy POL-BLTK-2026-02 v2.1 (uploaded, DOC-6DCN), assessed against NIS2 Article 21(2) minimum measures and Article 23 reporting obligations.

ASSESSMENT_START	2026-07-11 18:12:20.165260+00:00
ASSESSMENT_END	2026-07-11 18:13:16.277548+00:00
DOCUMENTS_REVIEWED	1
CONTROLS_ASSESSED	10
FRAMEWORK	nis2
JURISDICTIONS	EU, EE
FRAMEWORK_DISPLAY_NAME	NIS2 Directive (EU) 2022/2555 — Art. 21 cybersecurity risk-management measures
PER_FRAMEWORK_NOTICE	## NIS2 sector scope NIS2 Art. 21(2) measures apply to essential and important entities under Annex I/II. Sector caveats (energy, transport, banking, health, digital infrastructure, public administration) may add supervisory obligations — the sector-routing pass (Pass 3) surfaces the competent authority.
JURISDICTION_SPECIFIC_OBLIGATIONS	Member-state NIS2 transpositions vary in incident-notification deadlines and registration. The per-control assessment cites the transposing national act where the jurisdiction's corpus provides it.
REPORT_FOOTER	Generated by Ansvar Workflow MCP — workflow `gap_analysis_nis2`. Not legal advice; a structured basis for the organisation's own compliance assessment.

GAP ANALYSIS

Findings

Art.21.2.a **Risk analysis and information system security policies** MEDIUM

Compliance: partial **Evidence tier:** documentary **Provision resolution:** n/a

Risk analysis is informal: no documented methodology or criteria (ISO 27001 6.1.2), backlog-based risk register, annual-only cadence with no change-triggered reassessment (ISO 27001 8.2). NIS2 IR (EU) 2024/2690 Annex I additionally expects topic-specific policies and management-body information flows beyond the single policy document. Sector search returned only tangential EU rows; EE scope FAILED THIS RUN — gateway reported 'EE temporarily unavailable' (22 servers unavailable). Estonian transposition (küberturvalisuse seadus / E-ITS baseline) NOT verified; held open as unresolved rather than assumed. NIS2 Art. 21(2)(a) 'policies on risk analysis and information system security' anchored via get_provision NIS2:art_21 (exact). resolution_method=exact (sub-point folded to parent article). Blue: NIS2:art_21 (eur-lex), IR 2024/2690 Annex I (eur-lex), SS-EN ISO/IEC 27001:2023 6.1.2/8.2/6.2 (SIS). Amber: ENISA guidance (CC-BY-4). Gray: none load-bearing. No case-law rows returned for this control (broadened search surfaced Implementing Regulation (EU) 2024/2690 Annex I instead, cited as Blue anchor). case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance + ENISA 'Cybersecurity roles and skills for NIS2 entities' — both fetched, license ENISA-CC-BY-4. Adopt a documented risk-assessment methodology with acceptance criteria (ISO 27001 6.1.2), move the risk register out of the engineering backlog, add change-triggered reassessment (8.2), and derive topic-specific policies per IR 2024/2690 Annex I §1. SS-EN ISO/IEC 27001:2023 (SIS-licensed, fetched this run): 6.1.2 Information security risk assessment (defined process with criteria — MISSING), 8.2 risk assessment at planned intervals or on significant change (PARTIAL: annual only), 6.2 objectives from risk-assessment results (PARTIAL). Attribution: SIS-Reproduction-Licence. GDPR: applies (Art. 32 security of processing overlaps; customer TMS data is personal data in part). EU AI Act: not applicable (no AI system in the TMS per entity description). CSRD: not applicable at 90 employees (below thresholds). EN 301 549: not applicable to this control. NIS2: primary regime. True Policy POL-BLTK-2026-02 §2 (governance: CEO accountable, security officer role, quarterly management reporting, annual re-approval) and §3 (annual risk assessment covering TMS platform and corporate IT; risks recorded in engineering backlog; CEO sign-off for accepting high risks). An information-system security policy exists and is approved; a risk-analysis practice exists but has no defined methodology, no risk-acceptance criteria per ISO/IEC 27001 6.1.2, and no re-assessment trigger on material change (annual-only, contra SS-EN ISO/IEC 27001:2023 8.2 'planned intervals or when significant changes occur').

Strengthen and complete controls for “Art.21.2.a”. Address the identified gap: Risk analysis is informal: no documented methodology or criteria (ISO 27001 6.1.2), backlog-based risk register, annual-only cadence with no change-triggered reassessment (ISO 27001 8.2). NIS2 IR (EU) 2024/2690 Annex I additionally expects topic-specific policies and management-body information flows beyond the single policy document. Sector search returned only tangential EU rows; EE scope FAILED THIS RUN — gateway reported 'EE temporarily unavailable' (22 servers unavailable). Estonian transposition (küberturvalisuse seadus / E-ITS baseline) NOT verified; held open as unresolved rather than assumed. NIS2 Art. 21(2)(a) 'policies on risk analysis and information system security' anchored via get_provision NIS2:art_21 (exact). resolution_method=exact (sub-point folded to parent article). Blue: NIS2:art_21 (eur-lex), IR 2024/2690 Annex I (eur-lex), SS-EN ISO/IEC 27001:2023 6.1.2/8.2/6.2 (SIS). Amber: ENISA guidance (CC-BY-4). Gray: none load-bearing. No case-law rows returned for this control (broadened search surfaced Implementing Regulation (EU) 2024/2690 Annex I instead, cited as Blue anchor). case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance + ENISA 'Cybersecurity

roles and skills for NIS2 entities' — both fetched, license ENISA-CC-BY-4. Adopt a documented risk-assessment methodology with acceptance criteria (ISO 27001 6.1.2), move the risk register out of the engineering backlog, add change-triggered reassessment (8.2), and derive topic-specific policies per IR 2024/2690 Annex I §1. SS-EN ISO/IEC 27001:2023 (SIS-licensed, fetched this run): 6.1.2 Information security risk assessment (defined process with criteria — MISSING), 8.2 risk assessment at planned intervals or on significant change (PARTIAL: annual only), 6.2 objectives from risk-assessment results (PARTIAL). Attribution: SIS-Reproduction-Licence. GDPR: applies (Art. 32 security of processing overlaps; customer TMS data is personal data in part). EU AI Act: not applicable (no AI system in the TMS per entity description). CSRD: not applicable at 90 employees (below thresholds). EN 301 549: not applicable to this control. NIS2: primary regime. True Policy POL-BLTK-2026-02 §2 (governance: CEO accountable, security officer role, quarterly management reporting, annual re-approval) and §3 (annual risk assessment covering TMS platform and corporate IT; risks recorded in engineering backlog; CEO sign-off for accepting high risks). An information-system security policy exists and is approved; a risk-analysis practice exists but has no defined methodology, no risk-acceptance criteria per ISO/IEC 27001 6.1.2, and no re-assessment trigger on material change (annual-only, contra SS-EN ISO/IEC 27001:2023 8.2 'planned intervals or when significant changes occur').

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p7`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p9`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p7`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p9`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

Art.21.2.b **Incident handling** LOW

Compliance: largely_compliant **Evidence tier:** documentary **Provision resolution:** n/a

The section governs internal handling and CUSTOMER notification only. It contains no CSIRT/competent-authority notification chain (NIS2 Art. 23 early warning 24h / incident notification 72h / final report) — assessed separately, but its absence also weakens the handling procedure's escalation completeness. No incident-response exercise/test cadence (ENISA NIS2 Technical Implementation Guidance expects tested procedures). ISO 27001 A.5.24 expects communicated processes, roles and responsibilities — roles beyond the security officer are not defined. EE corpus responded this pass (unlike control (a)) but broadened-query rows were tangential (agricultural-vehicle type-approval; REACH). No sector-regulator modifier surfaced for incident handling; Estonian transposition detail still unverified overall. NIS2 Art. 21(2)(b) 'incident handling' via get_provision NIS2:art_21, resolution_method=exact (sub-point folds to parent). Blue: NIS2:art_21 (eur-lex), SS-EN ISO/IEC 27001:2023 A.5.24 (SIS). Amber: ENISA guidance (CC-BY-4). Gray: none load-bearing. No on-point ruling; broadened fan-out returned an unrelated CJEU appeal-admissibility opinion (ECLI:EU:C:2024:522) — not cited as authority. case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance, 'INCIDENT HANDLING POLICY' section: define clear objectives; ensure policy complies with laws/regulations/standards. Fetched, ENISA-CC-BY-4. Add the Art. 23 authority-notification chain to §6 (see reporting assessment), define incident roles beyond the security officer (A.5.24), reference GDPR Art. 33/34 breach duties, and adopt an annual incident-response exercise. SS-EN ISO/IEC 27001:2023 A.5.24 Information security incident management planning and preparation (PARTIAL: process exists; roles beyond security officer undefined, no exercise cadence). Attribution: SIS-Reproduction-Licence. GDPR: applies — personal-data breaches in the TMS would trigger Art. 33/34 duties not referenced by §6. EU AI Act: not applicable. CSRD: not applicable (size). EN 301 549: not applicable. NIS2: primary. True Policy §6 Incident management (0.p15): immediate reporting duty to security officer, 4-hour classification on a three-level severity ladder, security-officer-led response, 72-hour customer notification for incidents affecting customer data or availability, post-incident review within two weeks for major/critical with recorded lessons learned. This covers detection, triage, response and learning — the core of Art. 21(2)(b).

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p15`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p15`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance`

Art.21.2.c **Business continuity and crisis management** MEDIUM

Compliance: partial **Evidence tier:** documentary **Provision resolution:** n/a

No crisis-management function or escalation organisation (who declares a crisis, who communicates — IR (EU) 2024/2690 Annex I §4 expects crisis management distinct from backups; DORA Art. 11 illustrates the expected shape). No defined RTO/RPO. Restore testing annual-only; SS-EN ISO/IEC 27001:2023 A.5.30 requires ICT readiness 'planned, implemented, maintained and tested' based on business requirements — a single untested-in-anger runbook does not satisfy it. Verdict: partial. EE scope FAILED AGAIN this pass ('EE temporarily unavailable', 22 servers) — EE reachability is intermittent this run (down for controls a and c, up for b). Estonian transposition detail remains unverified; held unresolved. NIS2 Art. 21(2)(c) 'business continuity, such as backup management and disaster recovery, and crisis management' via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21, IR 2024/2690 Annex I §4 (eur-lex), SS-EN ISO/IEC 27001:2023 A.5.30 (SIS). Amber: ENISA + Commission guidance. Gray: none load-bearing. No on-point ruling; broadened fan-out surfaced IR 2024/2690 Annex I §4 (used as Blue anchor) and an off-topic bank-resolution opinion (ECLI:EU:C:2024:511, not cited as authority). case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance 'BUSINESS CONTINUITY AND CRISIS MANAGEMENT' section + Commission NIS2 Art. 4 Guidelines enumerating 21(2) measures. Both fetched. Define RTO/RPO per service, add a crisis-management procedure with declared roles and communication plan (IR 2024/2690 Annex I §4), and raise restore/failover testing beyond annual per A.5.30. SS-EN ISO/IEC 27001:2023 A.5.30 ICT readiness for business continuity (PARTIAL: backups exist, readiness not tested against business requirements; no RTO/RPO). Attribution: SIS-Reproduction-Licence. GDPR: applies (Art. 32(1)(c) restore availability after incident). DORA: NOT directly applicable (Baltika is not a financial entity) but fetched Art. 11 shows the crisis-function shape; noted as comparative only. EU AI Act / CSRD / EN 301 549: not applicable. NIS2: primary. True Policy §7 (0.p17): daily database backups to a separate availability zone, 35-day retention, one restore test per year, written recovery runbook, restore-from-backup strategy for regional outage. Backup management and basic disaster recovery exist.

Strengthen and complete controls for “Art.21.2.c”. Address the identified gap: No crisis-management function or escalation organisation (who declares a crisis, who communicates — IR (EU) 2024/2690 Annex I §4 expects crisis management distinct from backups; DORA Art. 11 illustrates the expected shape). No defined RTO/RPO. Restore testing annual-only; SS-EN ISO/IEC 27001:2023 A.5.30 requires ICT readiness 'planned, implemented, maintained and tested' based on business requirements — a single untested-in-anger runbook does not satisfy it. Verdict: partial. EE scope FAILED AGAIN this pass ('EE temporarily unavailable', 22 servers) — EE reachability is intermittent this run (down for controls a and c, up for b). Estonian transposition detail remains unverified; held unresolved. NIS2 Art. 21(2)(c) 'business continuity, such as backup management and disaster recovery, and crisis management' via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21, IR 2024/2690 Annex I §4 (eur-lex), SS-EN ISO/IEC 27001:2023 A.5.30 (SIS). Amber: ENISA + Commission guidance. Gray: none load-bearing. No on-point ruling; broadened fan-out surfaced IR 2024/2690 Annex I §4 (used as Blue anchor) and an off-topic bank-resolution opinion (ECLI:EU:C:2024:511, not cited as authority). case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance 'BUSINESS CONTINUITY AND CRISIS MANAGEMENT' section + Commission NIS2 Art. 4 Guidelines enumerating 21(2) measures. Both fetched. Define RTO/RPO per service, add a crisis-management procedure with declared roles and communication plan (IR 2024/2690 Annex I §4), and raise restore/failover testing beyond annual per

A.5.30. SS-EN ISO/IEC 27001:2023 A.5.30 ICT readiness for business continuity (PARTIAL: backups exist, readiness not tested against business requirements; no RTO/RPO). Attribution: SIS-Reproduction-Licence. GDPR: applies (Art. 32(1)(c) restore availability after incident). DORA: NOT directly applicable (Baltika is not a financial entity) but fetched Art. 11 shows the crisis-function shape; noted as comparative only. EU AI Act / CSRD / EN 301 549: not applicable. NIS2: primary. True Policy §7 (0.p17): daily database backups to a separate availability zone, 35-day retention, one restore test per year, written recovery runbook, restore-from-backup strategy for regional outage. Backup management and basic disaster recovery exist.

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p17`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p17`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

Art.21.2.d **Supply chain security** HIGH

Compliance: not_implemented **Evidence tier:** documentary **Provision resolution:** n/a

Entire measure missing. NIS2 Art. 21(2)(d) requires supply-chain security including 'security-related aspects concerning the relationships between each entity and its direct suppliers or service providers', and Art. 21(3) requires weighing supplier-specific vulnerabilities and overall supplier practices. NIS Cooperation Group guidance: the policy 'should identify the entity's role in the supply chain and state network and information security requirements accordingly to direct suppliers'. ISO 27001 A.5.19 (supplier relationships), A.5.22 (monitoring/review of supplier services), A.5.23 (cloud services security requirements) all unaddressed — A.5.23 is acute since the entire platform runs on one cloud provider. Verdict: not_implemented. Highest-priority gap of the register. EE corpus responded this pass; broadened rows tangential (vehicle type-approval, REACH). No sector modifier surfaced. Estonian transposition detail still unverified overall this run. NIS2 Art. 21(2)(d) + Art. 21(3) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21 incl. 21(3) (eur-lex), SS-EN ISO/IEC 27001:2023 A.5.19/A.5.22/A.5.23 (SIS). Amber: NIS Cooperation Group + ENISA/JRC guidance. Gray: none load-bearing. No on-point security ruling — the only case-law row (ECLI:EU:C:2022:923 Tilman v Unilever Supply Chain) is a jurisdiction-clause dispute matching on the words 'supply chain', not authority here; not cited. case_law_unconfirmed: true. NIS Cooperation Group security-measures guidance ('Supply chain security policy' — identify role, state requirements to direct suppliers) + ENISA/JRC CRA standards mapping. Both fetched. Author a supplier-security policy: supplier/dependency inventory (start: hosting provider, CI/CD, key third-party components), minimum security requirements + contractual clauses per A.5.19/A.5.23 and GDPR Art. 28, annual supplier review per A.5.22, and reclaim or contractually bind encryption-key management currently delegated in §5. SS-EN ISO/IEC 27001:2023 A.5.19 Information security in supplier relationships (MISSING), A.5.22 Monitoring, review and change management of supplier services (MISSING), A.5.23 Information security for use of cloud services (MISSING — acute). Attribution: SIS-Reproduction-Licence. GDPR: applies — the hosting provider is a processor; Art. 28 contract obligations intersect (fetched EDPB/EDPS row references Art. 28 security measures). EU AI Act / CSRD / EN 301 549: not applicable. CRA: relevant only as supplier-side context (fetched ENISA CRA standards mapping references supply-chain security standards). True None. The policy contains no supply-chain security section. The only supplier reference is §11 (0.p25): production is 'hosted with a cloud provider certified to recognised security standards' — an unnamed certification claim, not a supplier-security measure. There is no supplier inventory, no security requirements flowed to direct suppliers (hosting provider, CI/CD tooling, third-party dependencies), no supplier monitoring or exit criteria, and §5 even delegates encryption-key management to the hosting provider without any contractual security requirement.

Establish and document controls for “Art.21.2.d”. Address the identified gap: Entire measure missing. NIS2 Art. 21(2)(d) requires supply-chain security including 'security-related aspects concerning the relationships between each entity and its direct suppliers or service providers', and Art. 21(3) requires weighing supplier-specific vulnerabilities and overall supplier practices. NIS Cooperation Group guidance: the policy 'should identify the entity's role in the supply chain and state network and information security requirements accordingly to direct suppliers'. ISO 27001 A.5.19 (supplier relationships), A.5.22 (monitoring/review of supplier services), A.5.23 (cloud services security requirements) all unaddressed — A.5.23 is acute since the entire platform runs on one cloud provider. Verdict: not_implemented. Highest-priority gap of the register. EE corpus responded this pass;

broadened rows tangential (vehicle type-approval, REACH). No sector modifier surfaced. Estonian transposition detail still unverified overall this run. NIS2 Art. 21(2)(d) + Art. 21(3) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21 incl. 21(3) (eur-lex), SS-EN ISO/IEC 27001:2023 A.5.19/A.5.22/A.5.23 (SIS). Amber: NIS Cooperation Group + ENISA/JRC guidance. Gray: none load-bearing. No on-point security ruling — the only case-law row (ECLI:EU:C:2022:923 Tilman v Unilever Supply Chain) is a jurisdiction-clause dispute matching on the words 'supply chain', not authority here; not cited. case_law_unconfirmed: true. NIS Cooperation Group security-measures guidance ('Supply chain security policy' — identify role, state requirements to direct suppliers) + ENISA/JRC CRA standards mapping. Both fetched. Author a supplier-security policy: supplier/dependency inventory (start: hosting provider, CI/CD, key third-party components), minimum security requirements + contractual clauses per A.5.19/A.5.23 and GDPR Art. 28, annual supplier review per A.5.22, and reclaim or contractually bind encryption-key management currently delegated in §5. SS-EN ISO/IEC 27001:2023 A.5.19 Information security in supplier relationships (MISSING), A.5.22 Monitoring, review and change management of supplier services (MISSING), A.5.23 Information security for use of cloud services (MISSING — acute). Attribution: SIS-Reproduction-Licence. GDPR: applies — the hosting provider is a processor; Art. 28 contract obligations intersect (fetched EDPB/EDPS row references Art. 28 security measures). EU AI Act / CSRD / EN 301 549: not applicable. CRA: relevant only as supplier-side context (fetched ENISA CRA standards mapping references supply-chain security standards). True None. The policy contains no supply-chain security section. The only supplier reference is §11 (0.p25): production is 'hosted with a cloud provider certified to recognised security standards' — an unnamed certification claim, not a supplier-security measure. There is no supplier inventory, no security requirements flowed to direct suppliers (hosting provider, CI/CD tooling, third-party dependencies), no supplier monitoring or exit criteria, and §5 even delegates encryption-key management to the hosting provider without any contractual security requirement.

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p25`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p13`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p25`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p13`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

Art.21.2.e **Security in network and information systems acquisition, development and maintenance** MEDIUM

Compliance: partial **Evidence tier:** documentary **Provision resolution:** n/a

The measure's other half is missing: no coordinated vulnerability DISCLOSURE channel (Art. 21(2)(e) explicitly includes 'vulnerability handling and disclosure' — no security.txt, no reporting contact, no CVD procedure for external reporters). No secure-development rules for Baltika's own TMS code (ISO 27001 A.8.25 secure development life cycle, A.8.28 secure coding — the policy covers third-party dependencies but not first-party code standards), and no acquisition-security requirements for procured systems. Verdict: partial. EE scope FAILED this pass again ('EE temporarily unavailable', 22 servers). Third EE failure of the run (a, c, e); transposition detail stays unresolved. NIS2 Art. 21(2)(e) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21, IR 2024/2690 Annex I §6 (eur-lex), SS-EN ISO/IEC 27001:2023 A.8.8/A.8.25/A.8.28 (SIS). Amber: ENISA guidance. Gray: none load-bearing. No case-law rows; broadened results returned IR (EU) 2024/2690 Annex I §6 (Security in acquisition/development/maintenance) — used as Blue anchor. case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance, 'SECURITY IN NETWORK AND INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE' section. Fetched. Publish a coordinated vulnerability disclosure channel (security.txt + CVD procedure), adopt secure-development rules for first-party TMS code per A.8.25/A.8.28, and add security requirements to system acquisition. SS-EN ISO/IEC 27001:2023 A.8.8 Management of technical vulnerabilities (LARGELY MET by §8), A.8.25 Secure development life cycle (MISSING for first-party code), A.8.28 Secure coding (MISSING). Attribution: SIS-Reproduction-Licence. GDPR: applies indirectly (Art. 32 state-of-the-art maintenance). EU AI Act / CSRD / EN 301 549: not applicable. CRA: would apply to Baltika as software manufacturer once placed on the market with digital elements post-transition — flagged as forward-looking only, not assessed. NIS2: primary. True Policy §8 (0.p19): monthly OS/dependency patch cycle, 72-hour patching of vendor-critical vulnerabilities, CI dependency scanning that blocks builds on known-critical findings. Maintenance-side vulnerability HANDLING is real and operational.

Strengthen and complete controls for “Art.21.2.e”. Address the identified gap: The measure's other half is missing: no coordinated vulnerability DISCLOSURE channel (Art. 21(2)(e) explicitly includes 'vulnerability handling and disclosure' — no security.txt, no reporting contact, no CVD procedure for external reporters). No secure-development rules for Baltika's own TMS code (ISO 27001 A.8.25 secure development life cycle, A.8.28 secure coding — the policy covers third-party dependencies but not first-party code standards), and no acquisition-security requirements for procured systems. Verdict: partial. EE scope FAILED this pass again ('EE temporarily unavailable', 22 servers). Third EE failure of the run (a, c, e); transposition detail stays unresolved. NIS2 Art. 21(2)(e) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21, IR 2024/2690 Annex I §6 (eur-lex), SS-EN ISO/IEC 27001:2023 A.8.8/A.8.25/A.8.28 (SIS). Amber: ENISA guidance. Gray: none load-bearing. No case-law rows; broadened results returned IR (EU) 2024/2690 Annex I §6 (Security in acquisition/development/maintenance) — used as Blue anchor. case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance, 'SECURITY IN NETWORK AND INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE' section. Fetched. Publish a coordinated vulnerability disclosure channel (security.txt + CVD procedure), adopt secure-development rules for first-party TMS code per A.8.25/A.8.28, and add security requirements to system acquisition. SS-EN

ISO/IEC 27001:2023 A.8.8 Management of technical vulnerabilities (LARGELY MET by §8), A.8.25 Secure development life cycle (MISSING for first-party code), A.8.28 Secure coding (MISSING). Attribution: SIS-Reproduction-Licence. GDPR: applies indirectly (Art. 32 state-of-the-art maintenance). EU AI Act / CSRD / EN 301 549: not applicable. CRA: would apply to Baltika as software manufacturer once placed on the market with digital elements post-transition — flagged as forward-looking only, not assessed. NIS2: primary. True Policy §8 (0.p19): monthly OS/dependency patch cycle, 72-hour patching of vendor-critical vulnerabilities, CI dependency scanning that blocks builds on known-critical findings. Maintenance-side vulnerability HANDLING is real and operational.

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p19`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p19`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

Art.21.2.f **Policies and procedures to assess the effectiveness of cybersecurity risk-management measures** MEDIUM

Compliance: partial **Evidence tier:** documentary **Provision resolution:** n/a

No defined policy or procedure to assess whether the risk-management measures WORK: no security metrics/KPIs (ISO 27001 9.1 monitoring, measurement, analysis and evaluation), no internal audit programme, no management review with defined inputs (9.3.2 expects nonconformities, monitoring results, audit results), no penetration testing or control-testing cadence. ENISA guidance for Art. 21(2)(f) expects an established, implemented and applied policy assessing measure effectiveness. Reviewing the policy DOCUMENT annually is not assessing the MEASURES. Verdict: partial (weak). EE scope FAILED this pass ('EE temporarily unavailable', 22 servers). Fourth EE failure of the run; transposition detail stays unresolved. NIS2 Art. 21(2)(f) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21, IR 2024/2690 Annex I §7 (eur-lex), SS-EN ISO/IEC 27001:2023 9.1/9.3.2 (SIS). Amber: ENISA guidance. Gray: none load-bearing. No case-law rows; broadened results = IR 2024/2690 Annex I §7 (Blue anchor) + an off-topic REACH provision (not cited). case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance ('establish, implement and apply a policy and procedures to assess whether the cybersecurity risk-management measures...') + ENISA ECSF/NIS2 roles mapping (risk assessment reports and remediation plans to assess and improve effectiveness). Both fetched. Define an effectiveness-assessment procedure: a small KPI set (patch latency, restore-test results, incident MTTR, training completion), an annual internal audit or control self-assessment, and a management review with the 9.3.2 input list. SS-EN ISO/IEC 27001:2023 9.1 Monitoring, measurement, analysis and evaluation (MISSING), 9.3.2 Management review inputs (PARTIAL: review exists, inputs undefined), internal audit 9.2 (MISSING — surfaced as 9.2.1 in the control-a fetch). Attribution: SIS-Reproduction-Licence. GDPR: applies — Art. 32(1)(d) requires 'a process for regularly testing, assessing and evaluating the effectiveness' of security measures; same gap. EU AI Act / CSRD / EN 301 549: not applicable. NIS2: primary (IR 2024/2690 Annex I §7 details the requirement). True Policy §2 (0.p7): management reviews and re-approves the policy annually or after any material incident; quarterly security reporting to management. §12 (0.p27): exception register with approvals. These are governance touchpoints, not an effectiveness-assessment procedure.

Strengthen and complete controls for “Art.21.2.f”. Address the identified gap: No defined policy or procedure to assess whether the risk-management measures WORK: no security metrics/KPIs (ISO 27001 9.1 monitoring, measurement, analysis and evaluation), no internal audit programme, no management review with defined inputs (9.3.2 expects nonconformities, monitoring results, audit results), no penetration testing or control-testing cadence. ENISA guidance for Art. 21(2)(f) expects an established, implemented and applied policy assessing measure effectiveness. Reviewing the policy DOCUMENT annually is not assessing the MEASURES. Verdict: partial (weak). EE scope FAILED this pass ('EE temporarily unavailable', 22 servers). Fourth EE failure of the run; transposition detail stays unresolved. NIS2 Art. 21(2)(f) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21, IR 2024/2690 Annex I §7 (eur-lex), SS-EN ISO/IEC 27001:2023 9.1/9.3.2 (SIS). Amber: ENISA guidance. Gray: none load-bearing. No case-law rows; broadened results = IR 2024/2690 Annex I §7 (Blue anchor) + an off-topic REACH provision (not cited). case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance ('establish, implement and apply a policy and procedures to assess whether the cybersecurity risk-management measures...') + ENISA ECSF/NIS2 roles mapping (risk assessment

reports and remediation plans to assess and improve effectiveness). Both fetched. Define an effectiveness-assessment procedure: a small KPI set (patch latency, restore-test results, incident MTTR, training completion), an annual internal audit or control self-assessment, and a management review with the 9.3.2 input list. SS-EN ISO/IEC 27001:2023 9.1 Monitoring, measurement, analysis and evaluation (MISSING), 9.3.2 Management review inputs (PARTIAL: review exists, inputs undefined), internal audit 9.2 (MISSING — surfaced as 9.2.1 in the control-a fetch). Attribution: SIS-Reproduction-Licence. GDPR: applies — Art. 32(1)(d) requires 'a process for regularly testing, assessing and evaluating the effectiveness' of security measures; same gap. EU AI Act / CSRD / EN 301 549: not applicable. NIS2: primary (IR 2024/2690 Annex I §7 details the requirement). True Policy §2 (0.p7): management reviews and re-approves the policy annually or after any material incident; quarterly security reporting to management. §12 (0.p27): exception register with approvals. These are governance touchpoints, not an effectiveness-assessment procedure.

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p7`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p27`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p7`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p27`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

Art.21.2.g **Basic cyber hygiene practices and cybersecurity training** LOW

Compliance: largely_compliant **Evidence tier:** documentary **Provision resolution:** n/a

Two-year cadence for engineering secure-development training is thin against an annual baseline; no management-body training (NIS2 Art. 20(2) expects management to follow training — ENISA roles guidance targets 'training programmes aimed at members of management bodies'); no phishing-simulation or effectiveness check on the training (ISO 27001 7.3 awareness + A.6.3 'regular updates'). Verdict: largely_compliant. EE scope FAILED this pass ('EE temporarily unavailable', 22 servers). Fifth EE failure of the run; transposition detail stays unresolved. NIS2 Art. 21(2)(g) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21, IR 2024/2690 Annex I §8 (eur-lex), SS-EN ISO/IEC 27001:2023 A.6.3/7.3 (SIS). Amber: ENISA guidance. Gray: none load-bearing. No case-law rows; broadened results = IR 2024/2690 Annex I §8 (Blue anchor) + an EIOPA supervisory statement (insurance-sector, tangential, not cited as authority). case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance 'AWARENESS RAISING AND BASIC CYBER HYGIENE PRACTICES' + ENISA roles/skills (management-body training programmes). Both fetched. Add management-body cybersecurity training (NIS2 Art. 20(2)), raise engineering secure-development training to annual, and add a simple training-effectiveness check (completion tracking + periodic phishing simulation). SS-EN ISO/IEC 27001:2023 A.6.3 Information security awareness, education and training (LARGELY MET; 'regular updates' partially — annual only, no effectiveness check), 7.3 Awareness (MET in substance). Attribution: SIS-Reproduction-Licence. GDPR: applies lightly (Art. 39(1)(b) awareness-raising is DPO-side; §9's data-handling module covers staff). EU AI Act / CSRD / EN 301 549: not applicable. NIS2: primary (IR 2024/2690 Annex I §8 'Basic cyber hygiene practices and security training'). True Policy §9 (0.p21): security awareness training at onboarding and annually (phishing, password hygiene, data handling, incident reporting), plus secure-development training for engineering every two years. §4 (0.p11): password rules (12+ chars, unique, password manager, no shared production accounts) — core hygiene practices. This is the policy's second-strongest area.

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p11`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p11`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

Art.21.2.h

Policies and procedures regarding the use of cryptography and encryption

MEDIUM

Compliance: partial **Evidence tier:** documentary **Provision resolution:** n/a

The at-rest commitment is conditional — 'where technically feasible' is a weasel clause that makes the control unverifiable (IR 2024/2690 Annex I §9 expects a policy 'ensuring adequate and effective use of cryptography'; ISO 27001 A.8.24 requires RULES for effective use of cryptography INCLUDING cryptographic key management). Key management is wholly delegated to the hosting provider with no requirements, no inventory of what is/isn't encrypted at rest, no algorithm/protocol baseline (TLS 1.2 floor is dated; no 1.3 preference stated). Verdict: partial. EE scope FAILED this pass ('EE temporarily unavailable', 22 servers). Sixth EE failure of the run; transposition detail stays unresolved. NIS2 Art. 21(2)(h) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21, IR 2024/2690 Annex I §9 (eur-lex), SS-EN ISO/IEC 27001:2023 A.8.24 (SIS). Amber: Commission guidelines, ENISA IoT crypto practices. Gray: none load-bearing. No case-law rows; broadened results = IR 2024/2690 Annex I §9 cryptography policy text (Blue anchor). case_law_unconfirmed: true. Commission NIS2 Art. 4 Guidelines (enumerating the cryptography measure) + MDCG 2019-16 mapping row (tangential, not load-bearing). Fetched. Replace 'where technically feasible' with a definitive at-rest encryption statement plus a documented exception list; add key-management rules (ownership, rotation, escrow) per A.8.24 — or contractual requirements on the provider; state an algorithm/protocol baseline with TLS 1.3 preferred. SS-EN ISO/IEC 27001:2023 A.8.24 Use of cryptography (PARTIAL: transit rules exist; key-management rules absent, at-rest conditional), A.5.23 cloud-services security (intersects — key management delegated without requirements, same finding as control d). Attribution: SIS-Reproduction-Licence. GDPR: applies directly — Art. 32(1)(a) names encryption of personal data; the conditional at-rest clause weakens the Art. 32 posture too. EU AI Act / CSRD / EN 301 549: not applicable. NIS2: primary. True Policy §5 (0.p13): TLS 1.2+ for all customer data in transit; data at rest encrypted 'where the underlying hosting platform makes this technically feasible'; encryption keys for customer-facing services 'managed by the hosting provider'.

Strengthen and complete controls for “Art.21.2.h”. Address the identified gap: The at-rest commitment is conditional — 'where technically feasible' is a weasel clause that makes the control unverifiable (IR 2024/2690 Annex I §9 expects a policy 'ensuring adequate and effective use of cryptography'; ISO 27001 A.8.24 requires RULES for effective use of cryptography INCLUDING cryptographic key management). Key management is wholly delegated to the hosting provider with no requirements, no inventory of what is/isn't encrypted at rest, no algorithm/protocol baseline (TLS 1.2 floor is dated; no 1.3 preference stated). Verdict: partial. EE scope FAILED this pass ('EE temporarily unavailable', 22 servers). Sixth EE failure of the run; transposition detail stays unresolved. NIS2 Art. 21(2)(h) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21, IR 2024/2690 Annex I §9 (eur-lex), SS-EN ISO/IEC 27001:2023 A.8.24 (SIS). Amber: Commission guidelines, ENISA IoT crypto practices. Gray: none load-bearing. No case-law rows; broadened results = IR 2024/2690 Annex I §9 cryptography policy text (Blue anchor). case_law_unconfirmed: true. Commission NIS2 Art. 4 Guidelines (enumerating the cryptography measure) + MDCG 2019-16 mapping row (tangential, not load-bearing). Fetched. Replace 'where technically feasible' with a definitive at-rest encryption statement plus a documented exception list; add key-management rules (ownership, rotation, escrow) per A.8.24 — or contractual requirements on the provider; state an algorithm/protocol baseline with TLS 1.3 preferred. SS-EN

ISO/IEC 27001:2023 A.8.24 Use of cryptography (PARTIAL: transit rules exist; key-management rules absent, at-rest conditional), A.5.23 cloud-services security (intersects — key management delegated without requirements, same finding as control d). Attribution: SIS-Reproduction-Licence. GDPR: applies directly — Art. 32(1)(a) names encryption of personal data; the conditional at-rest clause weakens the Art. 32 posture too. EU AI Act / CSRD / EN 301 549: not applicable. NIS2: primary. True Policy §5 (0.p13): TLS 1.2+ for all customer data in transit; data at rest encrypted 'where the underlying hosting platform makes this technically feasible'; encryption keys for customer-facing services 'managed by the hosting provider'.

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p13`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p13`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

Art.21.2.i **Human resources security, access control policies and asset management** MEDIUM

Compliance: partial **Evidence tier:** documentary **Provision resolution:** n/a

The third component — ASSET MANAGEMENT — is absent: no inventory of information and associated assets with owners (ISO 27001 A.5.9), no asset classification, no acceptable-use rules. Also no privileged-access-specific rules beyond the general least-privilege statement (A.8.2 expects restricted allocation of privileged rights). Verdict: partial (access control and HR strong, asset management missing). EE scope FAILED this pass ('EE temporarily unavailable', 22 servers). Seventh EE failure of the run; transposition detail stays unresolved. NIS2 Art. 21(2)(i) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21 (eur-lex), SS-EN ISO/IEC 27001:2023 A.5.9/A.5.18/A.8.2 (SIS). Amber: NIS CG + ENISA guidance. Gray: none load-bearing. No on-point ruling (broadened rows: ENISA guidance + an unrelated batteries-regulation recital, not cited). case_law_unconfirmed: true. NIS Cooperation Group security measures ('should also address human resources security and have in place appropriate access control policies') + ENISA NIS2 Technical Implementation Guidance (access control in line with HR security procedures §10.1). Both fetched. Create an asset inventory with named owners and classification (A.5.9) — for a 90-person SaaS this is a spreadsheet-day, not a programme; add privileged-access rules (A.8.2: separate admin accounts, JIT elevation where possible). SS-EN ISO/IEC 27001:2023 A.5.9 Inventory of information and other associated assets (MISSING), A.5.18 Access rights (MET by §4), A.8.2 Privileged access rights (PARTIAL). Attribution: SIS-Reproduction-Licence. GDPR: applies (Art. 32 access control; Art. 30 records intersect asset inventory). EU AI Act / CSRD / EN 301 549: not applicable. DORA RTS 2024/1774 Art. 18 fetched as comparative shape only (financial-sector, not applicable to Baltika). NIS2: primary. True Access control — policy §4 (0.p11): least privilege, role-based, quarterly reviews, next-business-day revocation on exit, password rules, no shared production accounts. HR security — §10 (0.p23): confidentiality clauses, reference checks for production-access hires, offboarding with equipment return. Two of the measure's three components are genuinely covered.

Strengthen and complete controls for “Art.21.2.i”. Address the identified gap: The third component — ASSET MANAGEMENT — is absent: no inventory of information and associated assets with owners (ISO 27001 A.5.9), no asset classification, no acceptable-use rules. Also no privileged-access-specific rules beyond the general least-privilege statement (A.8.2 expects restricted allocation of privileged rights). Verdict: partial (access control and HR strong, asset management missing). EE scope FAILED this pass ('EE temporarily unavailable', 22 servers). Seventh EE failure of the run; transposition detail stays unresolved. NIS2 Art. 21(2)(i) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21 (eur-lex), SS-EN ISO/IEC 27001:2023 A.5.9/A.5.18/A.8.2 (SIS). Amber: NIS CG + ENISA guidance. Gray: none load-bearing. No on-point ruling (broadened rows: ENISA guidance + an unrelated batteries-regulation recital, not cited). case_law_unconfirmed: true. NIS Cooperation Group security measures ('should also address human resources security and have in place appropriate access control policies') + ENISA NIS2 Technical Implementation Guidance (access control in line with HR security procedures §10.1). Both fetched. Create an asset inventory with named owners and classification (A.5.9) — for a 90-person SaaS this is a spreadsheet-day, not a programme; add privileged-access rules (A.8.2: separate admin accounts, JIT elevation where possible). SS-EN ISO/IEC 27001:2023 A.5.9 Inventory of information and other associated assets (MISSING), A.5.18 Access rights (MET by §4), A.8.2 Privileged

access rights (PARTIAL). Attribution: SIS-Reproduction-Licence. GDPR: applies (Art. 32 access control; Art. 30 records intersect asset inventory). EU AI Act / CSRD / EN 301 549: not applicable. DORA RTS 2024/1774 Art. 18 fetched as comparative shape only (financial-sector, not applicable to Baltika). NIS2: primary. True Access control — policy §4 (0.p11): least privilege, role-based, quarterly reviews, next-business-day revocation on exit, password rules, no shared production accounts. HR security — §10 (0.p23): confidentiality clauses, reference checks for production-access hires, offboarding with equipment return. Two of the measure's three components are genuinely covered.

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p11`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p23`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p11`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p23`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

Art.21.2.j

Multi-factor authentication, secured communication and emergency communication systems

HIGH

Compliance: not_implemented **Evidence tier:** documentary **Provision resolution:** n/a

NIS2 Art. 21(2)(j) expects MFA or continuous authentication 'where appropriate' — for a SaaS operator whose staff hold production access to customer freight data, MFA on production and admin access is squarely 'appropriate' (ENISA NIS2 guidance: access 'governed through strong logical access controls, such as multi-factor authentication'; ENISA Threat Landscape 2025 lists MFA (M1032) as the counter to credential misuse, the dominant intrusion vector). ISO 27001 A.8.5 requires secure authentication technologies based on access restrictions. Password-only production access in 2026 is a headline gap. Verdict: not_implemented. EE scope FAILED this pass ('EE temporarily unavailable', 22 servers). Eighth EE failure of the run; transposition detail stays unresolved. NIS2 Art. 21(2)(j) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21 (eur-lex), SS-EN ISO/IEC 27001:2023 A.8.5 (SIS). Amber: ENISA guidance ×2, ENISA ETL 2025. Gray: none load-bearing. No on-point ruling (broadened rows: UN-R10 EMC definition, off-topic; ENISA ETL access-privilege section used as guidance instead). case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance ('access to corporate resources is governed through strong logical access controls, such as multi-factor authentication') + ENISA roles/skills ('security features like multi-factor authentication (MFA), and secure communications for voice, video, text, and emergencies'). Both fetched. Mandate MFA for all production, admin, and remote access immediately (highest-impact, lowest-cost fix in this register), extend to all corporate accounts, and add an out-of-band emergency communication channel to §6. SS-EN ISO/IEC 27001:2023 A.8.5 Secure authentication (MISSING — 'secure authentication technologies and procedures shall be implemented based on information access restrictions'). Attribution: SIS-Reproduction-Licence. GDPR: applies (Art. 32 state-of-the-art — password-only access to personal data is below it). EU AI Act / CSRD / EN 301 549: not applicable. NIS2: primary. True None for multi-factor authentication: policy §4 (0.p11) relies on passwords alone (12+ chars, unique, password manager) — MFA appears NOWHERE in the document, for production access, corporate IT, or the TMS platform. No continuous-authentication alternative, no secured-communications provision for incident/emergency coordination (if email/chat are down during an incident, §6 has no out-of-band channel).

Establish and document controls for “Art.21.2.j”. Address the identified gap: NIS2 Art. 21(2)(j) expects MFA or continuous authentication 'where appropriate' — for a SaaS operator whose staff hold production access to customer freight data, MFA on production and admin access is squarely 'appropriate' (ENISA NIS2 guidance: access 'governed through strong logical access controls, such as multi-factor authentication'; ENISA Threat Landscape 2025 lists MFA (M1032) as the counter to credential misuse, the dominant intrusion vector). ISO 27001 A.8.5 requires secure authentication technologies based on access restrictions. Password-only production access in 2026 is a headline gap. Verdict: not_implemented. EE scope FAILED this pass ('EE temporarily unavailable', 22 servers). Eighth EE failure of the run; transposition detail stays unresolved. NIS2 Art. 21(2)(j) via get_provision NIS2:art_21, resolution_method=exact. Blue: NIS2:art_21 (eur-lex), SS-EN ISO/IEC 27001:2023 A.8.5 (SIS). Amber: ENISA guidance ×2, ENISA ETL 2025. Gray: none load-bearing. No on-point ruling (broadened rows: UN-R10 EMC definition, off-topic; ENISA ETL access-privilege section used as guidance instead). case_law_unconfirmed: true. ENISA NIS2 Technical Implementation Guidance

('access to corporate resources is governed through strong logical access controls, such as multi-factor authentication') + ENISA roles/skills ('security features like multi-factor authentication (MFA), and secure communications for voice, video, text, and emergencies'). Both fetched. Mandate MFA for all production, admin, and remote access immediately (highest-impact, lowest-cost fix in this register), extend to all corporate accounts, and add an out-of-band emergency communication channel to §6. SS-EN ISO/IEC 27001:2023 A.8.5 Secure authentication (MISSING — 'secure authentication technologies and procedures shall be implemented based on information access restrictions'). Attribution: SIS-Reproduction-Licence. GDPR: applies (Art. 32 state-of-the-art — password-only access to personal data is below it). EU AI Act / CSRD / EN 301 549: not applicable. NIS2: primary. True None for multi-factor authentication: policy §4 (0.p11) relies on passwords alone (12+ chars, unique, password manager) — MFA appears NOWHERE in the document, for production access, corporate IT, or the TMS platform. No continuous-authentication alternative, no secured-communications provision for incident/emergency coordination (if email/chat are down during an incident, §6 has no out-of-band channel).

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p11`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p15`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p11`

`doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p15`

`https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21`

REMEDIATION

Remediation Roadmap

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
Art.21.2.d			Supply chain security	not_implemented	Establish and docum “Art.21.2.d”. Address gap: Entire measure 21(2)(d) requires sup including 'security-re concerning the relati each entity and its di service providers', ar requires weighing su vulnerabilities and ov practices. NIS Coope guidance: the policy the entity's role in the and state network ar security requirement direct suppliers'. ISO (supplier relationship (monitoring/review of services), A.5.23 (clo security requirement — A.5.23 is acute sin platform runs on one Verdict: not_impleme priority gap of the re responded this pass; tangential (vehicle ty REACH). No sector m Estonian transpositio unverified overall this 21(2)(d) + Art. 21(3) NIS2:art_21, resolutio Blue: NIS2:art_21 incl SS-EN ISO/IEC 2700 A.5.19/A.5.22/A.5.23 NIS Cooperation Gro guidance. Gray: none

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					on-point security rulir case-law row (ECLI:E Tilman v Unilever Sup jurisdiction-clause dis on the words 'supply authority here; not cit case_law_unconfirme Cooperation Group s guidance ('Supply ch policy' — identify role requirements to direc ENISA/JRC CRA stan Both fetched. Author security policy: supp inventory (start: host CI/CD, key third-part minimum security rec contractual clauses p and GDPR Art. 28, ar review per A.5.22, ar contractually bind en management current §5. SS-EN ISO/IEC 27 Information security i relationships (MISSIN Monitoring, review ar management of supp (MISSING), A.5.23 In security for use of clo (MISSING — acute). Reproduction-Licenc — the hosting provid Art. 28 contract oblig (fetched EDPB/EDPS Art. 28 security meas CSRD / EN 301 549: CRA: relevant only as context (fetched ENI standards mapping r chain security standa The policy contains n security section. The reference is §11 (0.p2

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					'hosted with a cloud to recognised securit an unnamed certifica supplier-security mea supplier inventory, nc requirements flowed suppliers (hosting pr tooling, third-party d supplier monitoring o §5 even delegates er management to the h without any contract requirement.
Art.21.2.j			Multi-factor authentication, secured communication and emergency communication systems	not_implemented	Establish and docum "Art.21.2.j". Address gap: NIS2 Art. 21(2)(continuous authentic appropriate' — for a whose staff hold proc customer freight data production and admi squarely 'appropriate guidance: access 'gc strong logical access multi-factor authentic Threat Landscape 2((M1032) as the coun misuse, the dominant ISO 27001 A.8.5 requ authentication techn access restrictions. P production access in headline gap. Verdict not_implemented. EE this pass ('EE tempor 22 servers). Eighth E run; transposition det unresolved. NIS2 Art get_provision NIS2:a resolution_method=e NIS2:art_21 (eur-lex), 27001:2023 A.8.5 (S

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					ENISA guidance ×2, Gray: none load-bear ruling (broadened rov definition, off-topic; E access-privilege sect guidance instead). case_law_unconfirme NIS2 Technical Imple Guidance ('access to resources is governe logical access contro factor authentication roles/skills ('security multi-factor authentic secure communicatio video, text, and emer fetched. Mandate MI production, admin, a immediately (highest cost fix in this registe corporate accounts, of-band emergency channel to §6. SS-EN 27001:2023 A.8.5 Se authentication (MISS authentication techn procedures shall be i based on information restrictions'). Attribut Reproduction-Licenc (Art. 32 state-of-the- only access to perso it). EU AI Act / CSRD applicable. NIS2: prir for multi-factor authe §4 (0.p11) relies on p (12+ chars, unique, p manager) — MFA ap in the document, for access, corporate IT, platform. No continuo authentication alterna communications prov

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					incident/emergency email/chat are down incident, §6 has no o channel).
Art.21.2.a			Risk analysis and information system security policies	partial	Strengthen and comp "Art.21.2.a". Address gap: Risk analysis is documented method (ISO 27001 6.1.2), ba register, annual-only change-triggered rea 27001 8.2). NIS2 IR Annex I additionally e specific policies and body information flov single policy docume returned only tangen scope FAILED THIS R reported 'EE tempora (22 servers unavailab transposition (kübert / E-ITS baseline) NO open as unresolved r assumed. NIS2 Art. 2 on risk analysis and i system security' ancl get_provision NIS2:a resolution_method=e folded to parent artic NIS2:art_21 (eur-lex), Annex I (eur-lex), SS 27001:2023 6.1.2/8.2 Amber: ENISA guida Gray: none load-bear rows returned for this (broadened search s Implementing Regula 2024/2690 Annex I i Blue anchor). case_la true. ENISA NIS2 Tec Implementation Guid 'Cybersecurity roles a

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					entities' — both fetch ENISA-CC-BY-4. Ado risk-assessment meth acceptance criteria (move the risk registe engineering backlog, triggered reassessme derive topic-specific 2024/2690 Annex I 27001:2023 (SIS-lice this run): 6.1.2 Inform assessment (defined criteria — MISSING), assessment at planne significant change (P only), 6.2 objectives assessment results (P Attribution: SIS-Repr GDPR: applies (Art. 3 processing overlaps; data is personal data Act: not applicable (r the TMS per entity d not applicable at 90 thresholds). EN 301 5 applicable to this cor primary regime. True 2026-02 §2 (govern accountable, security quarterly manageme annual re-approval) a risk assessment cove platform and corpora recorded in engineer sign-off for acceptin information-system s exists and is approve practice exists but ha methodology, no risk- criteria per ISO/IEC 2 no re-assessment trig change (annual-only, ISO/IEC 27001:2023

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					intervals or when sig occur').
Art.21.2.c			Business continuity and crisis management	partial	Strengthen and comp "Art.21.2.c". Address gap: No crisis-manag or escalation organis declares a crisis, wh — IR (EU) 2024/269 expects crisis manag from backups; DORA the expected shape) RTO/RPO. Restore te SS-EN ISO/IEC 2700 requires ICT readines implemented, mainta based on business re single untested-in-an not satisfy it. Verdict: FAILED AGAIN this p temporarily unavailab — EE reachability is i run (down for control b). Estonian transpos remains unverified; h NIS2 Art. 21(2)(c) 'bu such as backup man disaster recovery, an management' via get NIS2:art_21, resolutio Blue: NIS2:art_21, IR Annex I §4 (eur-lex), 27001:2023 A.5.30 (ENISA + Commission none load-bearing. N broadened fan-out s 2024/2690 Annex I anchor) and an off-to resolution opinion (ECLI:EU:C:2024:511, authority). case_law_ true. ENISA NIS2 Tec Implementation Guid

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					CONTINUITY AND C MANAGEMENT' sect NIS2 Art. 4 Guideline 21(2) measures. Both RTO/RPO per service management proced roles and communica 2024/2690 Annex I § restore/failover testin per A.5.30. SS-EN IS 27001:2023 A.5.30 I business continuity (I backups exist, readin against business requ RTO/RPO). Attributio Reproduction-Licenc (Art. 32(1)(c) restore incident). DORA: NO applicable (Baltika is entity) but fetched A crisis-function shape comparative only. EU EN 301 549: not app primary. True Policy § database backups to availability zone, 35- restore test per year, runbook, restore-fron strategy for regional management and ba recovery exist.
Art.21.2.e			Security in network and information systems acquisition, development and maintenance	partial	Strengthen and comp "Art.21.2.e". Address gap: The measure's c missing: no coordinat DISCLOSURE channe explicitly includes 'vu handling and disclosu security.txt, no repor CVD procedure for e No secure-developm Baltika's own TMS co

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					A.8.25 secure develo A.8.28 secure coding covers third-party de not first-party code s no acquisition-securit for procured systems EE scope FAILED this temporarily unavailab Third EE failure of the transposition detail st NIS2 Art. 21(2)(e) via NIS2:art_21, resolutio Blue: NIS2:art_21, IR Annex I §6 (eur-lex), 27001:2023 A.8.8/A (SIS). Amber: ENISA none load-bearing. N broadened results re 2024/2690 Annex I acquisition/developm — used as Blue anch case_law_unconfirme NIS2 Technical Imple Guidance, 'SECURITY AND INFORMATION ACQUISITION, DEVE MAINTENANCE' sec Publish a coordinated disclosure channel (s procedure), adopt se development rules fo code per A.8.25/A.8. security requirements acquisition. SS-EN IS 27001:2023 A.8.8 M technical vulnerabiliti MET by §8), A.8.25 S development life cyc first-party code), A.8 coding (MISSING). A Reproduction-Licenc indirectly (Art. 32 sta maintenance). EU AI

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					301 549: not applica apply to Baltika as sc manufacturer once p market with digital el transition — flagged looking only, not asse primary. True Policy § monthly OS/depende 72-hour patching of vulnerabilities, CI dep scanning that blocks critical findings. Main vulnerability HANDLI operational.
Art.21.2.f			Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	partial	Strengthen and comp "Art.21.2.f". Address gap: No defined poli to assess whether th management measur security metrics/KPIs monitoring, measurer evaluation), no intern programme, no mana with defined inputs (9 nonconformities, mor audit results), no pen control-testing cader guidance for Art. 21(2 established, impleme policy assessing mea effectiveness. Review DOCUMENT annually the MEASURES. Verd (weak). EE scope FAI temporarily unavailab Fourth EE failure of th transposition detail st NIS2 Art. 21(2)(f) via NIS2:art_21, resolutio Blue: NIS2:art_21, IR Annex I §7 (eur-lex), 27001:2023 9.1/9.3.2

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					ENISA guidance. Gra bearing. No case-law results = IR 2024/26 (Blue anchor) + an of provision (not cited). case_law_unconfirme NIS2 Technical Imple Guidance ('establish, apply a policy and pr assess whether the c management measur ECSF/NIS2 roles map assessment reports a plans to assess and i effectiveness). Both f effectiveness-assess a small KPI set (patch test results, incident completion), an annu control self-assessme management review input list. SS-EN ISO/ 9.1 Monitoring, measu and evaluation (MISS Management review review exists, inputs internal audit 9.2 (MI surfaced as 9.2.1 in t fetch). Attribution: SI Licence. GDPR: appli requires 'a process fo testing, assessing an effectiveness' of secu same gap. EU AI Act 549: not applicable. I 2024/2690 Annex I s requirement). True Po management reviews the policy annually or material incident; qua reporting to manager exception register wi These are governanc

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					not an effectiveness-procedure.
Art.21.2.h			Policies and procedures regarding the use of cryptography and encryption	partial	Strengthen and comp “Art.21.2.h”. Address gap: The at-rest com conditional — 'where feasible' is a weasel the control unverifiab Annex I §9 expects a adequate and effecti cryptography'; ISO 2 requires RULES for e cryptography INCLU cryptographic key m management is wholl the hosting provider requirements, no inve is/isn't encrypted at algorithm/protocol ba floor is dated; no 1.3 stated). Verdict: part FAILED this pass ('EE unavailable', 22 serv failure of the run; tran stays unresolved. NI via get_provision NIS resolution_method=e NIS2:art_21, IR 2024 (eur-lex), SS-EN ISO/ A.8.24 (SIS). Amber: guidelines, ENISA IoT practices. Gray: none case-law rows; broad 2024/2690 Annex I policy text (Blue anch case_law_unconfirme Commission NIS2 Art (enumerating the cry measure) + MDCG 2(row (tangential, not l Fetched. Replace 'wh feasible' with a defini

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					encryption statement documented excepti management rules (c rotation, escrow) per contractual requirem provider; state an alg baseline with TLS 1.3 ISO/IEC 27001:2023 cryptography (PARTI exist; key-manageme at-rest conditional), A services security (int management delegat requirements, same f d). Attribution: SIS-R Licence. GDPR: appli 32(1)(a) names encry data; the conditional weakens the Art. 32 AI Act / CSRD / EN 3 applicable. NIS2: pri §5 (0.p13): TLS 1.2+ data in transit; data a 'where the underlying makes this technicall encryption keys for c services 'managed b provider'.
Art.21.2.i			Human resources security, access control policies and asset management	partial	Strengthen and comp “Art.21.2.i”. Address gap: The third compo MANAGEMENT — is inventory of informat associated assets wit 27001 A.5.9), no ass no acceptable-use ru privileged-access-sp beyond the general l statement (A.8.2 exp allocation of privilege partial (access contr asset management m

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					FAILED this pass ('EE unavailable', 22 serv failure of the run; trar stays unresolved. NI get_provision NIS2:a resolution_method=e NIS2:art_21 (eur-lex), 27001:2023 A.5.9/A. Amber: NIS CG + EN Gray: none load-bear ruling (broadened ro guidance + an unrela regulation recital, not case_law_unconfirme Cooperation Group s ('should also address security and have in access control policie Technical Implementa (access control in line procedures §10.1). Bo Create an asset inver owners and classifica a 90-person SaaS th spreadsheet-day, no add privileged-acces separate admin acco elevation where poss ISO/IEC 27001:2023 of information and ot assets (MISSING), A. rights (MET by §4), A access rights (PARTI SIS-Reproduction-Lic applies (Art. 32 acce records intersect ass AI Act / CSRD / EN 3 applicable. DORA RT 18 fetched as compa (financial-sector, not Baltika). NIS2: prima control — policy §4 (privilege, role-based,

CONTROL	ACTION	PRIORITY	CONTROL_TITLE	COMPLIANCE_LEVEL	REMEDIATION
					reviews, next-busine on exit, password rul production accounts. §10 (0.p23): confide reference checks for access hires, offboar equipment return. Tw measure's three com genuinely covered.

PROVENANCE

Evidence & Citations

DOCUMENT	SEGMENT	SHA-256	NOTE
Untitled	—	—	
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p7	—	—	
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p9	—	—	
https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21	—	—	
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p15	—	—	
https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance	—	—	
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p17	—	—	
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p25	—	—	
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p13	—	—	
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p19	—	—	
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p27	—	—	
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p21	—	—	
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p11	—	—	

DOCUMENT	SEGMENT	SHA-256	NOTE
doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p23	—	—	

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p7

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p9

https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p15

https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p17

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p25

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p13

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p19

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p27

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p21

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p11

doc://fe2dc6df-3a15-4d8e-bc98-df8f95f128a7/segment/paragraph/0.p23

baltika-information-security-policy.md

PROVENANCE

Citation Integrity

VALIDATION PERFORMED

CITATIONS	14
DRIFTED	0
ATTRIBUTION MISSING	10