

ODA3 INSTITUTE

CROSSWALK

GAISSF™–NIS2 Mapping

Regulatory Crosswalk — Directive (EU) 2022/2555

GAISSF-CRO-029 | Informative crosswalk | Draft for Publication

Version 1.0 | Updated 6 October 2026

© 2026 ODA3 Pvt Ltd

Document ID	GAISSF-CRO-029
Classification	Crosswalk — informative
GAISSF baseline	GAISSF v1.0 — 59 controls
External baseline	Directive (EU) 2022/2555
Distribution	Website / GitHub
Status	Draft for Publication

The strongest operational alignment is with Article 20 governance, Article 21 cybersecurity risk-management measures, Article 22 supply-chain risk assessment and Article 23 reporting obligations. GAISSF supplies control and evidence structures; it does not determine legal scope, entity classification, jurisdiction, reporting deadlines or national supervisory requirements.

2. Purpose and Intended Use

- Support NIS2 readiness and gap analysis.
- Reuse GAISSF control evidence in national NIS2 programmes.
- Identify legal, procedural and country-specific work beyond GAISSF.
- Support internal assurance without asserting regulatory compliance.

3. Legal and Source Baseline

Primary legal source: Directive (EU) 2022/2555, adopted 14 December 2022 and published in OJ L 333 on 27 December 2022; EUR-Lex identifies the Directive as in force. The transposition deadline was 17 October 2024. Entity-level obligations must be checked against applicable Member State law and competent-authority rules. The European Commission's current transposition page remains a country-by-country state-of-play resource; on 8 July 2026 the Commission referred Ireland, Spain, France and the Netherlands to the Court of Justice for failure to notify NIS2 transposition measures.

Commission Implementing Regulation (EU) 2024/2690 is in force and remains a separate, directly applicable implementation layer for the specified entity classes, including DNS and TLD providers, cloud/data-centre/CDN providers, managed and managed-security service providers, online marketplaces/search/social-networking platforms, and trust service providers. It specifies technical and methodological Article 21 measures and significant-incident criteria under Article 23; it is not silently merged into this base Directive article mapping.

4. Scope

The crosswalk covers all GAISSF controls and all NIS2 articles. Entity-facing technical and governance provisions receive substantive mappings. Member State cooperation, institutional, enforcement and final provisions are retained in the reverse register and classified as outside GAISSF scope where appropriate.

5. Mapping Methodology

Each mapping compares intended outcome, actor, lifecycle scope, evidence expectation and normative character. Similar terminology is insufficient. Relationship strength and confidence are assigned independently. Composite support is recorded where several GAISSF controls jointly support one article.

6. Key Findings

Governance

D6 and selected D8 controls support management oversight, approval, auditability and accountability under Article 20.

Risk management

D1–D7 and D9 controls provide extensive technical and operational support for Article 21, particularly incident handling, continuity, supply-chain security, access control, integrity and monitoring.

Reporting

GAISSF incident controls support detection and evidence, but Article 23 notification thresholds, 24-hour early warning, 72-hour incident notification, final reporting and national channels require separate procedures.

Supervision

GAISSF evidence may support supervisory review, audits or inspections where relevant, but competent-authority powers, national procedures, fines, liability, remediation orders and enforcement consequences are legal matters outside GAISSF conformance.

7. NIS2 Article Coverage Register

Article	Title	Chapter	Mapped controls	Coverage	Residual gap
1	Subject matter	Chapter I — General provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
2	Scope	Chapter I — General provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
3	Essential and important entities	Chapter I — General provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
4	Sector-specific Union legal acts	Chapter I — General provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
5	Minimum harmonisation	Chapter I — General provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
6	Definitions	Chapter I — General provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
7	National cybersecurity strategy	Chapter II — Coordinated cybersecurity frameworks	2	Partially Addressed	GAISSF provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
8	Competent authorities and single points of contact	Chapter II — Coordinated cybersecurity frameworks	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
9	National cyber crisis management frameworks	Chapter II — Coordinated cybersecurity frameworks	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
10	Computer security incident response teams (CSIRTs)	Chapter II — Coordinated cybersecurity frameworks	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
11	Requirements, technical capabilities and tasks of CSIRTs	Chapter II — Coordinated cybersecurity frameworks	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
12	Cooperation at national level	Chapter II — Coordinated	0	Outside Scope	This provision primarily concerns Member

Article	Title	Chapter	Mapped controls	Coverage	Residual gap
		cybersecurity frameworks			States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSE controls.
13	Cooperation Group	Chapter III — Cooperation	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSE controls.
14	CSIRTs network	Chapter III — Cooperation	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSE controls.
15	European cyber crisis liaison organisation network (EU-CyCLONe)	Chapter III — Cooperation	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSE controls.
16	Report on the state of cybersecurity in the Union	Chapter III — Cooperation	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSE controls.
17	Peer reviews	Chapter III — Cooperation	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSE controls.
18	Mutual assistance	Chapter III — Cooperation	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSE controls.
19	Union-level coordinated security risk assessments of critical supply chains	Chapter III — Cooperation	3	Partially Addressed	GAISSE provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
20	Governance	Chapter IV — Risk management and reporting	10	Substantially Addressed	GAISSE provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
21	Cybersecurity risk-management measures	Chapter IV — Risk management and reporting	47	Substantially Addressed	GAISSE provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
22	Coordinated security risk assessments of critical supply chains	Chapter IV — Risk management and reporting	7	Partially Addressed	GAISSE provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
23	Reporting obligations	Chapter IV — Risk management and reporting	5	Partially Addressed	GAISSE provides implementation controls, but legal

Article	Title	Chapter	Mapped controls	Coverage	Residual gap
					applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
24	Use of European cybersecurity certification schemes	Chapter IV — Risk management and reporting	6	Partially Addressed	GAISSF provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
25	Standardisation	Chapter IV — Risk management and reporting	6	Partially Addressed	GAISSF provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
26	Jurisdiction and territoriality	Chapter IV — Risk management and reporting	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
27	Registry of entities	Chapter IV — Risk management and reporting	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
28	Domain name registration data	Chapter IV — Risk management and reporting	0	Not Addressed	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
29	Cybersecurity information-sharing arrangements	Chapter IV — Risk management and reporting	5	Partially Addressed	GAISSF provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
30	Voluntary notification of relevant information	Chapter IV — Risk management and reporting	4	Partially Addressed	GAISSF provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
31	General aspects concerning supervision and enforcement	Chapter VII — Supervision and enforcement	9	Partially Addressed	GAISSF provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
32	Supervisory and enforcement measures in relation to essential entities	Chapter VII — Supervision and enforcement	7	Partially Addressed	GAISSF provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.
33	Supervisory and enforcement measures in relation to important entities	Chapter VII — Supervision and enforcement	4	Partially Addressed	GAISSF provides implementation controls, but legal applicability, national transposition details and regulator-facing procedures remain outside framework conformance.

Article	Title	Chapter	Mapped controls	Coverage	Residual gap
34	General conditions for imposing administrative fines	Chapter VII — Supervision and enforcement	0	Not Addressed	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
35	Infringements entailing a personal data breach	Chapter VII — Supervision and enforcement	0	Not Addressed	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
36	Penalties	Chapter VII — Supervision and enforcement	0	Not Addressed	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
37	Delegation of power	Chapter VII — Supervision and enforcement	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
38	Exercise of the delegation	Chapter VIII — Delegated, implementing and final provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
39	Committee procedure	Chapter VIII — Delegated, implementing and final provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
40	Review	Chapter VIII — Delegated, implementing and final provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
41	Transposition	Chapter VIII — Delegated, implementing and final provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
42	Amendment of Regulation (EU) No 910/2014	Chapter VIII — Delegated, implementing and final provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
43	Amendment of Directive (EU) 2018/1972	Chapter VIII — Delegated, implementing and final provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
44	Repeal	Chapter VIII — Delegated, implementing and final provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.
45	Entry into force	Chapter VIII — Delegated, implementing and final provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal

Article	Title	Chapter	Mapped controls	Coverage	Residual gap
					procedure and is not established by GAISSF controls.
46	Addressees	Chapter VIII — Delegated, implementing and final provisions	0	Outside Scope	This provision primarily concerns Member States, EU cooperation, jurisdiction, supervision, enforcement or legal procedure and is not established by GAISSF controls.

8. Control-to-Article Mapping Register

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
GAISSF-CRO-029-MAP-0001	D1-CTL-01 — Dataset Provenance & Poisoning Prevention	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0002	D1-CTL-01 — Dataset Provenance & Poisoning Prevention	Art. 24 — Use of European cybersecurity certification schemes	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0003	D1-CTL-01 — Dataset Provenance & Poisoning Prevention	Art. 25 — Standardisation	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0004	D1-CTL-02 — Model Extraction Resistance	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0005	D1-CTL-03 — Behavioral Drift Detection	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0006	D1-CTL-04 — Federated Learning Poisoning Prevention	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0007	D1-CTL-04 — Federated Learning Poisoning Prevention	Art. 24 — Use of European cybersecurity certification schemes	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
						effectiveness require separate verification.
GAISSF-CRO-029-MAP-0008	D1-CTL-04 — Federated Learning Poisoning Prevention	Art. 25 — Standardisation	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0009	D1-CTL-05 — Embedding Space Robustness	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0010	D1-CTL-06 — Post-Quantum Model Signing & Crypto Hardening	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0011	D1-CTL-06 — Post-Quantum Model Signing & Crypto Hardening	Art. 24 — Use of European cybersecurity certification schemes	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0012	D1-CTL-06 — Post-Quantum Model Signing & Crypto Hardening	Art. 25 — Standardisation	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0013	D1-CTL-07 — Lora/Adapter Integrity Verification	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0014	D1-CTL-08 — Model Merge Attack Detection	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0015	D1-CTL-08 — Model Merge Attack Detection	Art. 29 — Cybersecurity information-sharing arrangements	S	Medium	Supports structured sharing or voluntary notification of cyber-threat and incident information.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0016	D1-CTL-08 — Model Merge Attack Detection	Art. 30 — Voluntary notification of relevant information	S	Medium	Supports structured sharing or voluntary notification of cyber-	NIS2 applicability, essential/important entity classification,

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
					threat and incident information.	national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0017	D1-CTL-09 — Quantization Backdoor Screening	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0018	D2-CTL-01 — Direct Prompt Injection Prevention	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0019	D2-CTL-02 — Indirect Prompt Injection Prevention	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0020	D2-CTL-03 — Jailbreak Resistance Testing	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0021	D2-CTL-04 — Multi-Modal Injection Defense	Art. 21 — Cybersecurity risk-management measures	P	Medium	The control contributes to an all-hazards cybersecurity risk-management capability, subject to entity and system scope.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0022	D2-CTL-05 — Function Call/Tool Call Injection Prevention	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0023	D2-CTL-06 — Cross-Context Hijacking Mitigation	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0024	D3-CTL-01 — Least Agency Enforcement	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
						procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0025	D3-CTL-02 — Inter-Agent Communication Security	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0026	D3-CTL-03 — Agentic Prompt Chaining Detection	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0027	D3-CTL-04 — Embodied Ai Safety Controls	Art. 21 — Cybersecurity risk-management measures	P	Medium	The control contributes to an all-hazards cybersecurity risk-management capability, subject to entity and system scope.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0028	D3-CTL-05 — Multi-Agent Trust Chain Attestation	Art. 21 — Cybersecurity risk-management measures	P	Medium	The control contributes to an all-hazards cybersecurity risk-management capability, subject to entity and system scope.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0029	D3-CTL-06 — Persistent Memory Exfiltration Prevention	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0030	D3-CTL-07 — Secure Memory Lifecycle Management	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0031	D3-CTL-07 — Secure Memory Lifecycle Management	Art. 22 — Coordinated security risk assessments of critical supply chains	SP	High	Supports supply-chain security, supplier due diligence and risk treatment for ICT products and services.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0032	D3-CTL-07 — Secure Memory Lifecycle Management	Art. 19 — Union-level coordinated security risk assessments of critical supply chains	S	Medium	Provides entity-level evidence relevant to critical supply-chain risk analysis.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-	D4-CTL-01 — Ai Bill	Art. 21 —	SP	High	Supports supply-	NIS2 applicability,

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
MAP-0033	Of Materials (Ai Bom) Maintenance	Cybersecurity risk-management measures			chain security, supplier due diligence and risk treatment for ICT products and services.	essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0034	D4-CTL-01 — Ai Bill Of Materials (Ai Bom) Maintenance	Art. 22 — Coordinated security risk assessments of critical supply chains	SP	High	Supports supply-chain security, supplier due diligence and risk treatment for ICT products and services.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0035	D4-CTL-01 — Ai Bill Of Materials (Ai Bom) Maintenance	Art. 19 — Union-level coordinated security risk assessments of critical supply chains	S	Medium	Provides entity-level evidence relevant to critical supply-chain risk analysis.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0036	D4-CTL-02 — Model File & Artifact Scanning	Art. 21 — Cybersecurity risk-management measures	P	Medium	The control contributes to an all-hazards cybersecurity risk-management capability, subject to entity and system scope.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0037	D4-CTL-03 — Model Hub & Registry Vetting	Art. 21 — Cybersecurity risk-management measures	SP	High	Supports supply-chain security, supplier due diligence and risk treatment for ICT products and services.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0038	D4-CTL-03 — Model Hub & Registry Vetting	Art. 22 — Coordinated security risk assessments of critical supply chains	SP	High	Supports supply-chain security, supplier due diligence and risk treatment for ICT products and services.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0039	D4-CTL-03 — Model Hub & Registry Vetting	Art. 19 — Union-level coordinated security risk assessments of critical supply chains	S	Medium	Provides entity-level evidence relevant to critical supply-chain risk analysis.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0040	D4-CTL-04 — Mcp Server Behavioral Monitoring	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0041	D4-CTL-04 — Mcp Server Behavioral Monitoring	Art. 22 — Coordinated security risk assessments of critical supply chains	SP	High	Supports supply-chain security, supplier due diligence and risk treatment for ICT products and	NIS2 applicability, essential/important entity classification, national transposition, proportionality,

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
					services.	reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0042	D4-CTL-05 — Third-Party Ai Api Security Assessment	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0043	D4-CTL-05 — Third-Party Ai Api Security Assessment	Art. 22 — Coordinated security risk assessments of critical supply chains	SP	High	Supports supply-chain security, supplier due diligence and risk treatment for ICT products and services.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0044	D4-CTL-05 — Third-Party Ai Api Security Assessment	Art. 31 — General aspects concerning supervision and enforcement	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0045	D4-CTL-05 — Third-Party Ai Api Security Assessment	Art. 32 — Supervisory and enforcement measures in relation to essential entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0046	D4-CTL-06 — Shadow Ai Discovery & Governance	Art. 20 — Governance	SP	High	Supports management oversight, accountability and documented approval of cybersecurity measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0047	D4-CTL-06 — Shadow Ai Discovery & Governance	Art. 31 — General aspects concerning supervision and enforcement	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0048	D4-CTL-06 — Shadow Ai Discovery & Governance	Art. 32 — Supervisory and enforcement measures in relation to essential entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0049	D4-CTL-06 — Shadow Ai Discovery & Governance	Art. 33 — Supervisory and enforcement measures in relation to important entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
GAISSF-CRO-029-MAP-0050	D4-CTL-07 — Ai Software Composition Analysis (Sca)	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	separate verification. NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0051	D4-CTL-07 — Ai Software Composition Analysis (Sca)	Art. 22 — Coordinated security risk assessments of critical supply chains	SP	High	Supports supply-chain security, supplier due diligence and risk treatment for ICT products and services.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0052	D5-CTL-01 — Harmful Content Blocking	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0053	D5-CTL-02 — Pii Leakage Prevention	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0054	D5-CTL-03 — Copyright Detection	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0055	D5-CTL-04 — Ai Watermarking Robustness	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0056	D5-CTL-05 — Privacy-By-Design Verification	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0057	D5-CTL-06 — Privacy-Preserving MI Validation	Art. 20 — Governance	SP	High	Supports management oversight, accountability and documented approval of cybersecurity measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0058	D5-CTL-06 — Privacy-Preserving MI Validation	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to	NIS2 applicability, essential/important entity classification, national

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
					NIS2 risk-management measures.	transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0059	D5-CTL-06 — Privacy-Preserving MI Validation	Art. 31 — General aspects concerning supervision and enforcement	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0060	D5-CTL-06 — Privacy-Preserving MI Validation	Art. 32 — Supervisory and enforcement measures in relation to essential entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0061	D6-CTL-01 — Human-In-The-Loop For High-Risk Actions	Art. 20 — Governance	SP	High	Supports management oversight, accountability and documented approval of cybersecurity measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0062	D6-CTL-02 — Audit Trail Completeness	Art. 20 — Governance	SP	High	Supports management oversight, accountability and documented approval of cybersecurity measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0063	D6-CTL-02 — Audit Trail Completeness	Art. 23 — Reporting obligations	P	High	Supports incident detection, evidence capture, escalation and reporting workflows, but does not by itself satisfy statutory notification timing and content.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0064	D6-CTL-02 — Audit Trail Completeness	Art. 31 — General aspects concerning supervision and enforcement	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0065	D6-CTL-02 — Audit Trail Completeness	Art. 32 — Supervisory and enforcement measures in relation to essential entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0066	D6-CTL-03 — Ai Model Card Completeness	Art. 20 — Governance	SP	High	Supports management oversight, accountability and documented approval of cybersecurity measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
						evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0067	D6-CTL-03 — Ai Model Card Completeness	Art. 31 — General aspects concerning supervision and enforcement	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0068	D6-CTL-03 — Ai Model Card Completeness	Art. 32 — Supervisory and enforcement measures in relation to essential entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0069	D6-CTL-03 — Ai Model Card Completeness	Art. 33 — Supervisory and enforcement measures in relation to important entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0070	D6-CTL-04 — Ai Incident Response Readiness	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0071	D6-CTL-04 — Ai Incident Response Readiness	Art. 23 — Reporting obligations	P	High	Supports incident detection, evidence capture, escalation and reporting workflows, but does not by itself satisfy statutory notification timing and content.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0072	D6-CTL-04 — Ai Incident Response Readiness	Art. 29 — Cybersecurity information-sharing arrangements	S	Medium	Supports structured sharing or voluntary notification of cyber-threat and incident information.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0073	D6-CTL-04 — Ai Incident Response Readiness	Art. 30 — Voluntary notification of relevant information	S	Medium	Supports structured sharing or voluntary notification of cyber-threat and incident information.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0074	D6-CTL-05 — Model Deprecation & Decommissioning	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0075	D6-CTL-06 — Third-Party Ai Vendor	Art. 20 — Governance	SP	High	Supports management	NIS2 applicability, essential/important

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
	Governance				oversight, accountability and documented approval of cybersecurity measures.	entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0076	D6-CTL-06 — Third-Party Ai Vendor Governance	Art. 21 — Cybersecurity risk-management measures	SP	High	Supports supply-chain security, supplier due diligence and risk treatment for ICT products and services.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0077	D6-CTL-06 — Third-Party Ai Vendor Governance	Art. 22 — Coordinated security risk assessments of critical supply chains	SP	High	Supports supply-chain security, supplier due diligence and risk treatment for ICT products and services.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0078	D6-CTL-06 — Third-Party Ai Vendor Governance	Art. 31 — General aspects concerning supervision and enforcement	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0079	D6-CTL-07 — Ai Resilience & Business Continuity	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0080	D7-CTL-H01 — Ai-Generated Phishing Simulation	Art. 29 — Cybersecurity information-sharing arrangements	S	Medium	Supports structured sharing or voluntary notification of cyber-threat and incident information.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0081	D7-CTL-H01 — Ai-Generated Phishing Simulation	Art. 30 — Voluntary notification of relevant information	S	Medium	Supports structured sharing or voluntary notification of cyber-threat and incident information.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0082	D7-CTL-H02 — Deepfake Detection Training	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0083	D7-CTL-H03 — Out-Of-Band Authentication	Art. 21 — Cybersecurity risk-management measures	P	Medium	The control contributes to an all-hazards cybersecurity risk-management capability, subject to entity and system	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines,

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
					scope.	competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0084	D7-CTL-H04 — Ai Social Engineering Ir	Art. 23 — Reporting obligations	P	High	Supports incident detection, evidence capture, escalation and reporting workflows, but does not by itself satisfy statutory notification timing and content.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0085	D7-CTL-H05 — Ai-Enhanced External Attack Defense	Art. 20 — Governance	SP	High	Supports management oversight, accountability and documented approval of cybersecurity measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0086	D7-CTL-H05 — Ai-Enhanced External Attack Defense	Art. 24 — Use of European cybersecurity certification schemes	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0087	D7-CTL-H05 — Ai-Enhanced External Attack Defense	Art. 25 — Standardisation	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0088	D7-CTL-H05 — Ai-Enhanced External Attack Defense	Art. 29 — Cybersecurity information-sharing arrangements	S	Medium	Supports structured sharing or voluntary notification of cyber-threat and incident information.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0089	D8-CTL-01 — Eu Ai Act Risk Tier Mapping	Art. 20 — Governance	SP	High	Supports management oversight, accountability and documented approval of cybersecurity measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0090	D8-CTL-01 — Eu Ai Act Risk Tier Mapping	Art. 7 — National cybersecurity strategy	C	Low	Can inform organisational alignment with national cybersecurity strategies but does not implement Member State duties.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0091	D8-CTL-02 — Iso 42001 Gap Analysis	Art. 20 — Governance	SP	High	Supports management oversight, accountability and documented approval of cybersecurity measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
GAISSF-CRO-029-MAP-0092	D8-CTL-02 — Iso 42001 Gap Analysis	Art. 24 — Use of European cybersecurity certification schemes	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0093	D8-CTL-02 — Iso 42001 Gap Analysis	Art. 25 — Standardisation	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0094	D8-CTL-02 — Iso 42001 Gap Analysis	Art. 7 — National cybersecurity strategy	C	Low	Can inform organisational alignment with national cybersecurity strategies but does not implement Member State duties.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0095	D8-CTL-03 — Gpai Technical Documentation Verification	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0096	D8-CTL-03 — Gpai Technical Documentation Verification	Art. 31 — General aspects concerning supervision and enforcement	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0097	D8-CTL-03 — Gpai Technical Documentation Verification	Art. 32 — Supervisory and enforcement measures in relation to essential entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0098	D8-CTL-03 — Gpai Technical Documentation Verification	Art. 33 — Supervisory and enforcement measures in relation to important entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0099	D8-CTL-04 — Dora Ict Incident Reporting (Financial Sector)	Art. 23 — Reporting obligations	P	High	Supports incident detection, evidence capture, escalation and reporting workflows, but does not by itself satisfy statutory notification timing and content.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0100	D8-CTL-05 — Nist Sp 800-218A Compliance Check	Art. 20 — Governance	SP	High	Supports management oversight, accountability and documented	NIS2 applicability, essential/important entity classification, national transposition,

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
					approval of cybersecurity measures.	proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0101	D8-CTL-05 — Nist Sp 800-218A Compliance Check	Art. 24 — Use of European cybersecurity certification schemes	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0102	D8-CTL-05 — Nist Sp 800-218A Compliance Check	Art. 25 — Standardisation	S	Medium	May support use of certification, standards and technical specifications contemplated by NIS2.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0103	D8-CTL-05 — Nist Sp 800-218A Compliance Check	Art. 31 — General aspects concerning supervision and enforcement	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0104	D9-CTL-01 — Physical Harm Boundary Enforcement	Art. 21 — Cybersecurity risk-management measures	P	Medium	The control contributes to an all-hazards cybersecurity risk-management capability, subject to entity and system scope.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0105	D9-CTL-02 — Safe State And Graceful Degradation	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0106	D9-CTL-03 — Human Override And Emergency Stop	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0107	D9-CTL-04 — Cyber-Physical Attack Detection	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0108	D9-CTL-04 — Cyber-Physical Attack Detection	Art. 29 — Cybersecurity information-sharing arrangements	S	Medium	Supports structured sharing or voluntary notification of cyber-threat and incident information.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating

Record	GAISSF control	NIS2 article	Relationship	Confidence	Rationale	Residual gap
						effectiveness require separate verification.
GAISSF-CRO-029-MAP-0109	D9-CTL-04 — Cyber-Physical Attack Detection	Art. 30 — Voluntary notification of relevant information	S	Medium	Supports structured sharing or voluntary notification of cyber-threat and incident information.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0110	D9-CTL-05 — Physical Environment Integrity Monitoring	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0111	D9-CTL-06 — Actuator Command Verification	Art. 21 — Cybersecurity risk-management measures	SP	High	Provides a technical, operational or organisational safeguard relevant to NIS2 risk-management measures.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0112	D9-CTL-07 — Physical Incident Evidence Preservation	Art. 23 — Reporting obligations	P	High	Supports incident detection, evidence capture, escalation and reporting workflows, but does not by itself satisfy statutory notification timing and content.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0113	D9-CTL-07 — Physical Incident Evidence Preservation	Art. 31 — General aspects concerning supervision and enforcement	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0114	D9-CTL-07 — Physical Incident Evidence Preservation	Art. 32 — Supervisory and enforcement measures in relation to essential entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.
GAISSF-CRO-029-MAP-0115	D9-CTL-07 — Physical Incident Evidence Preservation	Art. 33 — Supervisory and enforcement measures in relation to important entities	P	Medium	Produces evidence that may support supervisory review, inspection or remediation, subject to national law.	NIS2 applicability, essential/important entity classification, national transposition, proportionality, reporting deadlines, competent-authority procedures and evidence of operating effectiveness require separate verification.

D9 mappings are additional/conditional. Where Physical AI or cyber-physical actuation is in scope, PAI-SF™ v1.0 may be used alongside GAISSF; CSX-PAISF-004 is mapping only and does not establish equivalence, evidence sufficiency, operating effectiveness, legal compliance, or automatic conformance.

9. Limitations

- This crosswalk is informative and is not legal advice or a legal-compliance determination.
- NIS2 is a directive transposed through Member State law; applicable national legislation and competent-authority requirements control entity-level obligations.

- Scope depends on sector, size, entity type and Member State rules.
- Mapping does not establish legal equivalence, control implementation, evidence sufficiency, operating effectiveness, regulatory acceptance, or automatic NIS2 compliance.
- National authorities may impose additional procedures, evidence and deadlines.
- Commission Implementing Regulation (EU) 2024/2690, national implementing measures, later guidance and future legal changes require separate applicability analysis and controlled revalidation.

10. Notably Absent

- No automatic NIS2 or national-law compliance claim
- No determination that an organisation is an essential or important entity
- No country-specific transposition analysis
- No European Commission, ENISA, Member State authority or regulator endorsement
- No proof of operating effectiveness
- No automatic satisfaction of incident notification deadlines

11. Sources

Directive (EU) 2022/2555 — <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>

Commission Implementing Regulation (EU) 2024/2690 is in force and remains a separate, directly applicable implementation layer for the specified entity classes, including DNS and TLD providers, cloud/data-centre/CDN providers, managed and managed-security service providers, online marketplaces/search/social-networking platforms, and trust service providers. It specifies technical and methodological Article 21 measures and significant-incident criteria under Article 23; it is not silently merged into this base Directive article mapping.

European Commission NIS2 transposition status — <https://digital-strategy.ec.europa.eu/en/policies/nis-transposition>

GAISSF-NOR-001 and GAISSF-NOR-004 v1.0.

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute.