

ODA3 INSTITUTE

CROSSWALK — INFORMATIVE

GAISSF–EU AI Act Mapping

Article-Level Regulatory Alignment Crosswalk — EU AI Act consolidated 27 July 2026

GAISSF-CRO-027 | Public | Draft for Publication

Issued 29 June 2026 | Updated 06 October 2026

© 2026 ODA3 Pvt Ltd

Document ID	GAISSF-CRO-027
Version	1.0
Status	Draft for Publication
Classification	Crosswalk — informative
Publication date	29 June 2026
Publisher	ODA3 Institute

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute. EU legislation and institutional names remain the property of their respective institutions. No endorsement or affiliation is implied.

Executive Summary

GAISSF-CRO-027 maps all 59 GAISSF™ v1.0 controls to 51 selected material provisions of Regulation (EU) 2024/1689, using the consolidated text of 27 July 2026 incorporating Regulation (EU) 2026/1744. The register contains 236 control-to-article records and a reverse article-coverage view. The crosswalk supports readiness planning, evidence reuse and gap identification; it is informative only and does not establish legal compliance, equivalence, conformity, certification credit, evidence sufficiency or operating effectiveness.

1. Purpose and Intended Use

Use this document to identify where GAISSF™ security, safety, governance and assurance controls may be relevant to implementation of EU AI Act obligations. Legal counsel and qualified conformity-assessment professionals must determine scope, classification, actor role, applicable dates and sector-specific obligations. GAISSF certification is not currently offered.

2. Source Baseline

Source	Identifier	Status	Use
GAISSF Framework Standard	GAISSF-NOR-001 v1.0	Normative	Framework and conformance baseline
GAISSF Control Catalogue	GAISSF-NOR-004 v1.0	Normative	Authoritative 59-control catalogue
EU Artificial Intelligence Act	Regulation (EU) 2024/1689; consolidated 27 July 2026	Binding EU regulation	Primary current legal mapping baseline
Digital Omnibus on AI	Regulation (EU) 2026/1744; OJ 24 July 2026; in force 27 July 2026	Binding amending regulation	Amendments and revised application dates
European Commission AI Act pages	Regulatory framework and enforcement framework	Official implementation support	Current implementation and enforcement context

3. Legal and Temporal Interpretation

The Act applies in phases. This edition uses Regulation (EU) 2024/1689 as consolidated on 27 July 2026, incorporating Regulation (EU) 2026/1744. Chapters I-II generally apply from 2 February 2025; Chapter V, Chapter VII, Chapter XII (except Article 101), Chapter III Section 4 and Article 78 apply from 2 August 2025; the general application date is 2 August 2026; Articles 102-110 apply from 27 July 2026. Chapter III Sections 1-3 apply from 2 December 2027 for Article 6(2)/Annex III high-risk systems and 2 August 2028 for Article 6(1)/Annex I high-risk systems. Specified new Article 5 prohibitions apply from 2 December 2026. Application date is distinct from entry into force. Users must verify the Official Journal, later amendments, delegated and implementing acts, harmonised standards, codes of practice and competent-authority guidance at the date of reliance.

Legal review checkpoints: the 27 July 2026 consolidated text was reviewed article-by-article for the selected scope. Article 2 sectoral-law rules and future Article 2(13) delegated acts can limit obligations for some Article 6(1) product systems. Regulation (EU) 2026/1744 materially changed Articles 1, 3, 4, 5, 6, 10, 11, 17, 25, 27, 43, 50, 57, 72, 75, 95, 99, 111 and 113 and inserted Article 4a, Article 60a and Articles 75a-75d. Article 42(3) may create a Cyber Resilience Act-based presumption of conformity for Article 15 cybersecurity requirements in qualifying cases. Articles 4a, 60a, 75a-75d, Article 42(3) and Article 101 are legal dependencies but do not receive standalone mapping records in this v1.0 crosswalk.

4. Mapping Methodology

Mappings compare operative outcomes, technical and organisational measures, evidence expectations, lifecycle coverage and accountable actors. Similar terminology alone is insufficient. Relationship and confidence are recorded separately. Mapping density is not a legal-sufficiency score: one GAISF control may be relevant to several articles, and one article may require several GAISF controls plus legal and procedural measures outside GAISF.

Code	Meaning
SP	Strong partial
P	Partial
S	Supporting
C	Contextual
N	No material mapping
O	Outside scope
U	Unable to determine

5. Article Coverage Summary

Provision	Title	Group	Controls	Coverage	Application status
Article 1	Subject matter	General	0	No mapped GAISF control	Applicable since 2 February 2025 under Article 113(a) (Chapter I).
Article 2	Scope	General	0	No mapped GAISF control	Applicable since 2 February 2025 under Article 113(a) (Chapter I); scope was amended from 27 July 2026 by Regulation (EU) 2026/1744.
Article 3	Definitions	General	0	No mapped GAISF control	Applicable since 2 February 2025 under Article 113(a) (Chapter I); definitions were amended from 27 July 2026 by Regulation (EU) 2026/1744.
Article 4	AI literacy	General	4	Partial mapping	Applicable since 2 February 2025 under Article 113(a); Article 4 was replaced from 27 July 2026 by Regulation (EU) 2026/1744.
Article 5	Prohibited AI practices	Prohibited practices	6	Partial mapping	Generally applicable since 2 February 2025; Article 5(1)(ba), 5(1)(bb), 5(1a) and 5(1b) apply from 2 December 2026 under amended Article 113(a).
Article 6	Classification rules for high-risk AI systems	Classification	0	No mapped GAISF control	Article 6(5) applies from 2 August 2026; the remainder of Chapter III Section 1 applies from 2 December

Provision	Title	Group	Controls	Coverage	Application status
					2027 for Article 6(2)/Annex III systems and from 2 August 2028 for Article 6(1)/Annex I systems.
Article 8	Compliance with the requirements	High-risk requirements	0	No mapped GAISSE control	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 9	Risk management system	High-risk requirements	49	High mapping density	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 10	Data and data governance	High-risk requirements	0	No mapped GAISSE control	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 11	Technical documentation	High-risk requirements	7	Partial mapping	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 12	Record-keeping	High-risk requirements	2	Indirect mapping	Applies from 2 December 2027 for Article 6(2)/Annex III

Provision	Title	Group	Controls	Coverage	Application status
					high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 13	Transparency and provision of information to deployers	High-risk requirements	10	High mapping density	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 14	Human oversight	High-risk requirements	27	High mapping density	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 15	Accuracy, robustness and cybersecurity	High-risk requirements	44	High mapping density	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 16	Obligations of providers of high-risk AI systems	Provider obligations	0	No mapped GAISSE control	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.

Provision	Title	Group	Controls	Coverage	Application status
Article 17	Quality management system	Provider obligations	12	High mapping density	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 18	Documentation keeping	Provider obligations	0	No mapped GAISSE control	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 19	Automatically generated logs	Provider obligations	1	Indirect mapping	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 20	Corrective actions and duty of information	Provider obligations	2	Indirect mapping	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 21	Cooperation with competent authorities	Provider obligations	1	Indirect mapping	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2

Provision	Title	Group	Controls	Coverage	Application status
					sectoral-law rules and Article 111 transitional provisions.
Article 22	Authorised representatives of providers of high-risk AI systems	Supply chain roles	1	Indirect mapping	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 23	Obligations of importers	Supply chain roles	0	No mapped GAISSE control	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 24	Obligations of distributors	Supply chain roles	0	No mapped GAISSE control	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 25	Responsibilities along the AI value chain	Supply chain roles	6	Partial mapping	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems; paragraphs 2 and 4 were amended from 27 July 2026.
Article 26	Obligations of deployers of high-risk AI systems	Deployer obligations	15	High mapping density	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-

Provision	Title	Group	Controls	Coverage	Application status
					risk systems, subject to Article 2 sectoral-law rules and Article 111 transitional provisions.
Article 27	Fundamental rights impact assessment for high-risk AI systems	Deployer obligations	13	High mapping density	Applies from 2 December 2027 for Article 6(2)/Annex III high-risk systems and from 2 August 2028 for Article 6(1)/Annex I high-risk systems; paragraph 4 was amended from 27 July 2026 to permit DPIA cross-referencing/reuse where obligations are already met.
Article 43	Conformity assessment	Conformity	13	High mapping density	Generally applicable from 2 August 2026. Its operative high-risk conformity-assessment duties depend on the applicable Article 6 pathway, the delayed Chapter III Sections 1-3 dates, Article 2 sectoral-law rules, and Article 111 transitions.
Article 47	EU declaration of conformity	Conformity	0	No mapped GAISF control	Generally applicable from 2 August 2026. Its operative declaration-of-conformity duties depend on the applicable high-risk pathway and delayed Chapter III Sections 1-3 dates.
Article 48	CE marking	Conformity	0	No mapped GAISF control	Generally applicable from 2 August 2026. Its operative CE-marking duties depend on the applicable high-risk pathway and delayed Chapter III Sections 1-3 dates.
Article 49	Registration	Conformity	0	No mapped GAISF control	Generally applicable from 2 August 2026. Registration

Provision	Title	Group	Controls	Coverage	Application status
					duties must be read with the applicable high-risk pathway, Article 6(5), and delayed Chapter III Sections 1-3 dates.
Article 50	Transparency obligations for providers and deployers of certain AI systems	Transparency	0	No mapped GAISSF control	Applicable from 2 August 2026; Article 111(4) gives pre-2 August 2026 synthetic-content systems until 2 December 2026 to comply with Article 50(2).
Article 51	Classification of general-purpose AI models as general-purpose AI models with systemic risk	GPAI	1	Indirect mapping	Chapter V applicable since 2 August 2025. Article 101 fine powers apply from 2 August 2026; pre-2 August 2025 GPAI models have the Article 111(3) transition until 2 August 2027.
Article 52	Procedure	GPAI	0	No mapped GAISSF control	Chapter V applicable since 2 August 2025. Article 101 fine powers apply from 2 August 2026; pre-2 August 2025 GPAI models have the Article 111(3) transition until 2 August 2027.
Article 53	Obligations for providers of general-purpose AI models	GPAI	2	Indirect mapping	Chapter V applicable since 2 August 2025. Article 101 fine powers apply from 2 August 2026; pre-2 August 2025 GPAI models have the Article 111(3) transition until 2 August 2027.
Article 54	Authorised representatives of providers of general-purpose AI models	GPAI	1	Indirect mapping	Chapter V applicable since 2 August 2025. Article 101 fine powers apply from 2 August 2026; pre-2 August 2025 GPAI models have the Article 111(3) transition until 2 August 2027.

Provision	Title	Group	Controls	Coverage	Application status
Article 55	Obligations of providers of general-purpose AI models with systemic risk	GPAI systemic risk	7	Partial mapping	Chapter V applicable since 2 August 2025. Article 101 fine powers apply from 2 August 2026; pre-2 August 2025 GPAI models have the Article 111(3) transition until 2 August 2027.
Article 56	Codes of practice	GPAI	0	No mapped GAISF control	Chapter V applicable since 2 August 2025. Article 101 fine powers apply from 2 August 2026; pre-2 August 2025 GPAI models have the Article 111(3) transition until 2 August 2027.
Article 57	AI regulatory sandboxes	Innovation	0	No mapped GAISF control	Generally applicable from 2 August 2026; amended Article 57(1) requires at least one national AI regulatory sandbox to be operational by 2 August 2027.
Article 59	Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox	Innovation	0	No mapped GAISF control	Generally applicable from 2 August 2026; processing remains conditional on the strict Article 59 safeguards and applicable EU data-protection law.
Article 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	Monitoring	10	High mapping density	Generally applicable from 2 August 2026; because Article 72 addresses high-risk AI systems, practical obligations must be read with the applicable Article 6 pathway, delayed Chapter III dates and Article 111 transitions.
Article 73	Reporting of serious incidents	Incident reporting	2	Indirect mapping	Generally applicable from 2 August 2026; because Article 73 addresses high-risk AI systems,

Provision	Title	Group	Controls	Coverage	Application status
					practical obligations must be read with the applicable Article 6 pathway, delayed Chapter III dates and Article 111 transitions. Reporting deadlines are immediate and no later than 15 days ordinarily, 2 days for widespread infringement or Article 3(49)(b) incidents, and 10 days where a death occurs, subject to the statutory triggers.
Article 78	Confidentiality	Governance	0	No mapped GAISSE control	Applicable since 2 August 2025 under Article 113(b).
Article 79	Procedure for dealing with AI systems presenting a risk at national level	Market surveillance	0	No mapped GAISSE control	Generally applicable from 2 August 2026; enforcement against high-risk systems must be read with the provisions that are applicable to the relevant system and actor at the time.
Article 80	Procedure for dealing with AI systems classified by the provider as non-high-risk in application of Annex III	Market surveillance	0	No mapped GAISSE control	Generally applicable from 2 August 2026; Article 80 concerns Annex III systems treated by the provider as non-high-risk and must be read with Article 6 and the applicable timing rules.
Article 86	Right to explanation of individual decision-making	Rights	0	No mapped GAISSE control	Generally applicable from 2 August 2026; the right applies only within Article 86 conditions and does not displace rights otherwise provided under Union law.
Article 95	Codes of conduct for voluntary application of specific requirements	Voluntary	0	No mapped GAISSE control	Generally applicable from 2 August 2026; voluntary codes do not create a presumption of

Provision	Title	Group	Controls	Coverage	Application status
					conformity unless another legal instrument expressly provides one.
Article 99	Penalties	Enforcement	0	No mapped GAISSF control	Applicable since 2 August 2025 under Article 113(b) (Chapter XII); amended from 27 July 2026 by Regulation (EU) 2026/1744. Penalty exposure depends on the underlying infringed provision being applicable.
Article 110	Amendment to Directive (EU) 2020/1828	Amendment	0	No mapped GAISSF control	Applicable from 27 July 2026 under amended Article 113(d).
Article 111	AI systems already placed on the market or put into service and general-purpose AI models already placed on the market	Transition	0	No mapped GAISSF control	Generally applicable from 2 August 2026. Transitional rules include 31 December 2030 for certain Annex X large-scale IT systems, significant-change treatment for pre-application high-risk systems, 2 August 2030 for high-risk systems intended for public-authority use, 2 August 2027 for pre-2 August 2025 GPAI models, and 2 December 2026 for pre-2 August 2026 systems subject to Article 50(2).
Article 112	Evaluation and review	Review	0	No mapped GAISSF control	Generally applicable from 2 August 2026; evaluation and review duties contain their own milestones, including 2 August 2028, 2 August 2029 and 2 August 2031.
Article 113	Entry into force and application	Application	0	No mapped GAISSF control	In force since 1 August 2024; Article 113 sets the phased application schedule, including 2

Provision	Title	Group	Controls	Coverage	Application status
					February 2025, 2 August 2025, 27 July 2026, 2 August 2026, 2 December 2026, 2 December 2027 and 2 August 2028 milestones.

6. GAISSF-to-EU AI Act Mapping Register

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-027-MAP-0001	D1-CTL-01	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D1-CTL-01 operationalises part of Article 15 through Hash verification + source allowlist + poisoning detection. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0002	D1-CTL-01	Art. 9	Risk management system	SP	High	GAISSF D1-CTL-01 operationalises part of Article 9 through Hash verification + source allowlist + poisoning detection. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0003	D1-CTL-01	Art. 17	Quality management system	SP	High	GAISSF D1-CTL-01 operationalises part of Article 17 through Hash verification + source allowlist + poisoning detection. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0004	D1-CTL-01	Art. 55	Obligations of providers of general-purpose AI models with systemic risk	P	Medium-High	GAISSF D1-CTL-01 operationalises part of Article 55 through Hash verification + source allowlist + poisoning detection. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 55 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0005	D1-CTL-02	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D1-CTL-02 operationalises part of Article 15 through Rate limiting + diversity detection + extraction monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0006	D1-CTL-02	Art. 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	P	Medium-High	GAISSF D1-CTL-02 operationalises part of Article 72 through Rate limiting + diversity	Article 72 also depends on legal role, system classification, territorial scope, procedural duties,

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap and evidence requirements not established by this control alone.
						detection + extraction monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	
GAISSF-CRO-027-MAP-0007	D1-CTL-02	Art. 55	Obligations of providers of general-purpose AI models with systemic risk	P	Medium-High	GAISSF D1-CTL-02 operationalises part of Article 55 through Rate limiting + diversity detection + extraction monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 55 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0008	D1-CTL-02	Art. 9	Risk management system	SP	High	GAISSF D1-CTL-02 operationalises part of Article 9 through Rate limiting + diversity detection + extraction monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0009	D1-CTL-03	Art. 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	P	Medium-High	GAISSF D1-CTL-03 operationalises part of Article 72 through Baseline profiling + KL divergence monitoring + accuracy tracking. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 72 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0010	D1-CTL-03	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D1-CTL-03 operationalises part of Article 15 through Baseline profiling + KL divergence monitoring + accuracy tracking. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0011	D1-CTL-03	Art. 20	Corrective actions and duty of information	P	Medium-High	GAISSF D1-CTL-03 operationalises part of Article 20 through Baseline profiling + KL divergence monitoring + accuracy tracking. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 20 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0012	D1-CTL-03	Art. 73	Reporting of serious incidents	P	Medium-High	GAISSF D1-CTL-03 operationalises part of Article 73 through Baseline profiling + KL divergence monitoring + accuracy tracking. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 73 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-	D1-CTL-04	Art. 9	Risk management	SP	High	GAISSF D1-	Article 9 also

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
MAP-0013			system			CTL-04 operationalises part of Article 9 through Gradient anomaly detection + robust aggregation. The relationship is limited to the control's stated scope and does not establish legal compliance.	depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0014	D1-CTL-04	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D1-CTL-04 operationalises part of Article 15 through Gradient anomaly detection + robust aggregation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0015	D1-CTL-04	Art. 55	Obligations of providers of general-purpose AI models with systemic risk	P	Medium-High	GAISSF D1-CTL-04 operationalises part of Article 55 through Gradient anomaly detection + robust aggregation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 55 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0016	D1-CTL-04	Art. 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	P	Medium-High	GAISSF D1-CTL-04 operationalises part of Article 72 through Gradient anomaly detection + robust aggregation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 72 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0017	D1-CTL-05	Art. 9	Risk management system	SP	High	GAISSF D1-CTL-05 operationalises part of Article 9 through Adversarial training + independently evaluated robustness measurement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0018	D1-CTL-05	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D1-CTL-05 operationalises part of Article 15 through Adversarial training + independently evaluated robustness measurement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0019	D1-CTL-05	Art. 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	P	Medium-High	GAISSF D1-CTL-05 operationalises part of Article 72 through Adversarial training + independently evaluated robustness measurement. The relationship is limited to the control's stated scope and does not	Article 72 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-027-MAP-0020	D1-CTL-05	Art. 43	Conformity assessment	S	Medium	GAISSF D1-CTL-05 operationalises part of Article 43 through Adversarial training + independently evaluated robustness measurement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0021	D1-CTL-06	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D1-CTL-06 operationalises part of Article 15 through PQC signing (ML-DSA/SLH-DSA) + PQC key exchange (ML-KEM). The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0022	D1-CTL-06	Art. 9	Risk management system	S	Medium	GAISSF D1-CTL-06 operationalises part of Article 9 through PQC signing (ML-DSA/SLH-DSA) + PQC key exchange (ML-KEM). The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0023	D1-CTL-06	Art. 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	P	Medium-High	GAISSF D1-CTL-06 operationalises part of Article 72 through PQC signing (ML-DSA/SLH-DSA) + PQC key exchange (ML-KEM). The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 72 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0024	D1-CTL-06	Art. 43	Conformity assessment	S	Medium	GAISSF D1-CTL-06 operationalises part of Article 43 through PQC signing (ML-DSA/SLH-DSA) + PQC key exchange (ML-KEM). The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0025	D1-CTL-07	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D1-CTL-07 operationalises part of Article 15 through Adapter scanning + provenance verification + registry allowlist. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0026	D1-CTL-07	Art. 9	Risk management system	S	Medium	GAISSF D1-CTL-07 operationalises part of Article 9 through	Article 9 also depends on legal role, system classification,

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						Adapter scanning + provenance verification + registry allowlist. The relationship is limited to the control's stated scope and does not establish legal compliance.	territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0027	D1-CTL-07	Art. 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	P	Medium-High	GAISSF D1-CTL-07 operationalises part of Article 72 through Adapter scanning + provenance verification + registry allowlist. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 72 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0028	D1-CTL-07	Art. 43	Conformity assessment	S	Medium	GAISSF D1-CTL-07 operationalises part of Article 43 through Adapter scanning + provenance verification + registry allowlist. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0029	D1-CTL-08	Art. 9	Risk management system	S	Medium	GAISSF D1-CTL-08 operationalises part of Article 9 through Pre-registration behavioural evaluation + regression testing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0030	D1-CTL-08	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D1-CTL-08 operationalises part of Article 15 through Pre-registration behavioural evaluation + regression testing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0031	D1-CTL-08	Art. 43	Conformity assessment	S	Medium	GAISSF D1-CTL-08 operationalises part of Article 43 through Pre-registration behavioural evaluation + regression testing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0032	D1-CTL-08	Art. 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	P	Medium-High	GAISSF D1-CTL-08 operationalises part of Article 72 through Pre-registration behavioural evaluation + regression testing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 72 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-027-MAP-0033	D1-CTL-09	Art. 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	P	Medium-High	GAISSF D1-CTL-09 operationalises part of Article 72 through Cross-precision behavioural comparison + delta threshold monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 72 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0034	D1-CTL-09	Art. 9	Risk management system	SP	High	GAISSF D1-CTL-09 operationalises part of Article 9 through Cross-precision behavioural comparison + delta threshold monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0035	D1-CTL-09	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D1-CTL-09 operationalises part of Article 15 through Cross-precision behavioural comparison + delta threshold monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0036	D1-CTL-09	Art. 43	Conformity assessment	S	Medium	GAISSF D1-CTL-09 operationalises part of Article 43 through Cross-precision behavioural comparison + delta threshold monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0037	D2-CTL-01	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D2-CTL-01 operationalises part of Article 15 through Input validation + adversarial pattern matching + system prompt isolation + guardrail sidecar. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0038	D2-CTL-01	Art. 9	Risk management system	SP	High	GAISSF D2-CTL-01 operationalises part of Article 9 through Input validation + adversarial pattern matching + system prompt isolation + guardrail sidecar. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0039	D2-CTL-01	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D2-CTL-01 operationalises part of Article 26 through Input	Article 26 also depends on legal role, system classification, territorial scope,

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						validation + adversarial pattern matching + system prompt isolation + guardrail sidecar. The relationship is limited to the control's stated scope and does not establish legal compliance.	procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0040	D2-CTL-01	Art. 13	Transparency and provision of information to deployers	P	Medium-High	GAISSF D2-CTL-01 operationalises part of Article 13 through Input validation + adversarial pattern matching + system prompt isolation + guardrail sidecar. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 13 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0041	D2-CTL-02	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D2-CTL-02 operationalises part of Article 15 through Contextual separation + source allowlisting + output validation + RAG sanitization pipeline. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0042	D2-CTL-02	Art. 9	Risk management system	S	Medium	GAISSF D2-CTL-02 operationalises part of Article 9 through Contextual separation + source allowlisting + output validation + RAG sanitization pipeline. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0043	D2-CTL-02	Art. 14	Human oversight	P	Medium-High	GAISSF D2-CTL-02 operationalises part of Article 14 through Contextual separation + source allowlisting + output validation + RAG sanitization pipeline. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0044	D2-CTL-02	Art. 13	Transparency and provision of information to deployers	P	Medium-High	GAISSF D2-CTL-02 operationalises part of Article 13 through Contextual separation + source allowlisting + output validation + RAG sanitization pipeline. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 13 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0045	D2-CTL-03	Art. 9	Risk management system	SP	High	GAISSF D2-CTL-03 operationalises part of Article 9 through Quarterly red-team prompt library + adversarial training + automated	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						refusal monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	established by this control alone.
GAISSF-CRO-027-MAP-0046	D2-CTL-03	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D2-CTL-03 operationalises part of Article 15 through Quarterly red-team prompt library + adversarial training + automated refusal monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0047	D2-CTL-03	Art. 14	Human oversight	P	Medium-High	GAISSF D2-CTL-03 operationalises part of Article 14 through Quarterly red-team prompt library + adversarial training + automated refusal monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0048	D2-CTL-03	Art. 13	Transparency and provision of information to deployers	P	Medium-High	GAISSF D2-CTL-03 operationalises part of Article 13 through Quarterly red-team prompt library + adversarial training + automated refusal monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 13 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0049	D2-CTL-04	Art. 9	Risk management system	S	Medium	GAISSF D2-CTL-04 operationalises part of Article 9 through Multi-modal content scanning + steganography detection + modality-specific guardrails. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0050	D2-CTL-04	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D2-CTL-04 operationalises part of Article 15 through Multi-modal content scanning + steganography detection + modality-specific guardrails. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0051	D2-CTL-04	Art. 13	Transparency and provision of information to deployers	P	Medium-High	GAISSF D2-CTL-04 operationalises part of Article 13 through Multi-modal content scanning + steganography detection + modality-specific guardrails. The relationship is limited to the	Article 13 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						control's stated scope and does not establish legal compliance.	
GAISSF-CRO-027-MAP-0052	D2-CTL-04	Art. 14	Human oversight	P	Medium-High	GAISSF D2-CTL-04 operationalises part of Article 14 through Multi-modal content scanning + steganography detection + modality-specific guardrails. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0053	D2-CTL-05	Art. 9	Risk management system	S	Medium	GAISSF D2-CTL-05 operationalises part of Article 9 through Parameter schema validation + allowlist enforcement + sandboxed execution. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0054	D2-CTL-05	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D2-CTL-05 operationalises part of Article 15 through Parameter schema validation + allowlist enforcement + sandboxed execution. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0055	D2-CTL-05	Art. 14	Human oversight	P	Medium-High	GAISSF D2-CTL-05 operationalises part of Article 14 through Parameter schema validation + allowlist enforcement + sandboxed execution. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0056	D2-CTL-05	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D2-CTL-05 operationalises part of Article 26 through Parameter schema validation + allowlist enforcement + sandboxed execution. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0057	D2-CTL-06	Art. 9	Risk management system	S	Medium	GAISSF D2-CTL-06 operationalises part of Article 9 through Context window segmentation + prompt anchoring + attention boundary enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-027-MAP-0058	D2-CTL-06	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D2-CTL-06 operationalises part of Article 15 through Context window segmentation + prompt anchoring + attention boundary enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0059	D2-CTL-06	Art. 43	Conformity assessment	S	Medium	GAISSF D2-CTL-06 operationalises part of Article 43 through Context window segmentation + prompt anchoring + attention boundary enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0060	D2-CTL-06	Art. 55	Obligations of providers of general-purpose AI models with systemic risk	P	Medium-High	GAISSF D2-CTL-06 operationalises part of Article 55 through Context window segmentation + prompt anchoring + attention boundary enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 55 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0061	D3-CTL-01	Art. 9	Risk management system	S	Medium	GAISSF D3-CTL-01 operationalises part of Article 9 through Role-based tool scoping + policy-as-code + dynamic permission revocation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0062	D3-CTL-01	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D3-CTL-01 operationalises part of Article 26 through Role-based tool scoping + policy-as-code + dynamic permission revocation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0063	D3-CTL-01	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D3-CTL-01 operationalises part of Article 27 through Role-based tool scoping + policy-as-code + dynamic permission revocation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0064	D3-CTL-01	Art. 14	Human oversight	P	Medium-High	GAISSF D3-CTL-01 operationalises part of Article 14 through Role-based tool scoping +	Article 14 also depends on legal role, system classification, territorial scope, procedural duties,

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						policy-as-code + dynamic permission revocation. The relationship is limited to the control's stated scope and does not establish legal compliance.	and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0065	D3-CTL-02	Art. 9	Risk management system	SP	High	GAISSF D3-CTL-02 operationalises part of Article 9 through mTLS for agent mesh + message signing + payload validation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0066	D3-CTL-02	Art. 14	Human oversight	P	Medium-High	GAISSF D3-CTL-02 operationalises part of Article 14 through mTLS for agent mesh + message signing + payload validation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0067	D3-CTL-02	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D3-CTL-02 operationalises part of Article 15 through mTLS for agent mesh + message signing + payload validation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0068	D3-CTL-02	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D3-CTL-02 operationalises part of Article 26 through mTLS for agent mesh + message signing + payload validation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0069	D3-CTL-03	Art. 9	Risk management system	S	Medium	GAISSF D3-CTL-03 operationalises part of Article 9 through Cross-session behavioural correlation + chain pattern detection + anomaly scoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0070	D3-CTL-03	Art. 14	Human oversight	P	Medium-High	GAISSF D3-CTL-03 operationalises part of Article 14 through Cross-session behavioural correlation + chain pattern detection + anomaly scoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0071	D3-CTL-03	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D3-CTL-03 operationalises part of Article 15	Article 15 also depends on legal role, system classification,

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						through Cross-session behavioural correlation + chain pattern detection + anomaly scoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0072	D3-CTL-03	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D3-CTL-03 operationalises part of Article 26 through Cross-session behavioural correlation + chain pattern detection + anomaly scoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0073	D3-CTL-04	Art. 9	Risk management system	SP	High	GAISSF D3-CTL-04 operationalises part of Article 9 through Sensor integrity verification + safety interlocks + fail-safe state enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0074	D3-CTL-04	Art. 14	Human oversight	P	Medium-High	GAISSF D3-CTL-04 operationalises part of Article 14 through Sensor integrity verification + safety interlocks + fail-safe state enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0075	D3-CTL-04	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D3-CTL-04 operationalises part of Article 15 through Sensor integrity verification + safety interlocks + fail-safe state enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0076	D3-CTL-04	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D3-CTL-04 operationalises part of Article 26 through Sensor integrity verification + safety interlocks + fail-safe state enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0077	D3-CTL-05	Art. 9	Risk management system	S	Medium	GAISSF D3-CTL-05 operationalises part of Article 9 through SPIFFE/SPIRE workload identity + short-lived certificates + continuous attestation. The relationship is limited to the control's stated	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						scope and does not establish legal compliance.	
GAISSF-CRO-027-MAP-0078	D3-CTL-05	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D3-CTL-05 operationalises part of Article 15 through SPIFFE/SPIRE workload identity + short-lived certificates + continuous attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0079	D3-CTL-05	Art. 14	Human oversight	P	Medium-High	GAISSF D3-CTL-05 operationalises part of Article 14 through SPIFFE/SPIRE workload identity + short-lived certificates + continuous attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0080	D3-CTL-05	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D3-CTL-05 operationalises part of Article 26 through SPIFFE/SPIRE workload identity + short-lived certificates + continuous attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0081	D3-CTL-06	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D3-CTL-06 operationalises part of Article 15 through User-scoped memory isolation + encryption at rest + query-level access controls. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0082	D3-CTL-06	Art. 9	Risk management system	SP	High	GAISSF D3-CTL-06 operationalises part of Article 9 through User-scoped memory isolation + encryption at rest + query-level access controls. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0083	D3-CTL-06	Art. 14	Human oversight	P	Medium-High	GAISSF D3-CTL-06 operationalises part of Article 14 through User-scoped memory isolation + encryption at rest + query-level access controls. The relationship is limited to the control's stated scope and does not	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-027-MAP-0084	D3-CTL-06	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D3-CTL-06 operationalises part of Article 26 through User-scoped memory isolation + encryption at rest + query-level access controls. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0085	D3-CTL-07	Art. 9	Risk management system	S	Medium	GAISSF D3-CTL-07 operationalises part of Article 9 through Cryptographic deletion + lifecycle policy enforcement + retention auditing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0086	D3-CTL-07	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D3-CTL-07 operationalises part of Article 15 through Cryptographic deletion + lifecycle policy enforcement + retention auditing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0087	D3-CTL-07	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D3-CTL-07 operationalises part of Article 26 through Cryptographic deletion + lifecycle policy enforcement + retention auditing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0088	D3-CTL-07	Art. 14	Human oversight	P	Medium-High	GAISSF D3-CTL-07 operationalises part of Article 14 through Cryptographic deletion + lifecycle policy enforcement + retention auditing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0089	D4-CTL-01	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D4-CTL-01 operationalises part of Article 15 through Automated BOM generation + version tracking + registry synchronization. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0090	D4-CTL-01	Art. 17	Quality management system	S	Medium	GAISSF D4-CTL-01 operationalises part of Article 17 through Automated BOM generation + version tracking +	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						registry synchronization. The relationship is limited to the control's stated scope and does not establish legal compliance.	requirements not established by this control alone.
GAISSF-CRO-027-MAP-0091	D4-CTL-01	Art. 11	Technical documentation	P	Medium-High	GAISSF D4-CTL-01 operationalises part of Article 11 through Automated BOM generation + version tracking + registry synchronization. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 11 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0092	D4-CTL-01	Art. 25	Responsibilities along the AI value chain	P	Medium-High	GAISSF D4-CTL-01 operationalises part of Article 25 through Automated BOM generation + version tracking + registry synchronization. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 25 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0093	D4-CTL-02	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D4-CTL-02 operationalises part of Article 15 through Static analysis + deserialization sandboxing + signature verification. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0094	D4-CTL-02	Art. 17	Quality management system	S	Medium	GAISSF D4-CTL-02 operationalises part of Article 17 through Static analysis + deserialization sandboxing + signature verification. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0095	D4-CTL-02	Art. 11	Technical documentation	P	Medium-High	GAISSF D4-CTL-02 operationalises part of Article 11 through Static analysis + deserialization sandboxing + signature verification. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 11 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0096	D4-CTL-02	Art. 25	Responsibilities along the AI value chain	P	Medium-High	GAISSF D4-CTL-02 operationalises part of Article 25 through Static analysis + deserialization sandboxing + signature verification. The relationship is limited to the control's stated	Article 25 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						scope and does not establish legal compliance.	
GAISSF-CRO-027-MAP-0097	D4-CTL-03	Art. 11	Technical documentation	P	Medium-High	GAISSF D4-CTL-03 operationalises part of Article 11 through Provenance verification + license compliance + security scorecard. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 11 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0098	D4-CTL-03	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D4-CTL-03 operationalises part of Article 15 through Provenance verification + license compliance + security scorecard. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0099	D4-CTL-03	Art. 17	Quality management system	SP	High	GAISSF D4-CTL-03 operationalises part of Article 17 through Provenance verification + license compliance + security scorecard. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0100	D4-CTL-03	Art. 25	Responsibilities along the AI value chain	P	Medium-High	GAISSF D4-CTL-03 operationalises part of Article 25 through Provenance verification + license compliance + security scorecard. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 25 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0101	D4-CTL-04	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D4-CTL-04 operationalises part of Article 15 through Tool-call logging + anomaly detection + access control enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0102	D4-CTL-04	Art. 25	Responsibilities along the AI value chain	P	Medium-High	GAISSF D4-CTL-04 operationalises part of Article 25 through Tool-call logging + anomaly detection + access control enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 25 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0103	D4-CTL-04	Art. 11	Technical documentation	P	Medium-High	GAISSF D4-CTL-04	Article 11 also depends on legal

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						operationalises part of Article 11 through Tool-call logging + anomaly detection + access control enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0104	D4-CTL-04	Art. 17	Quality management system	SP	High	GAISSF D4-CTL-04 operationalises part of Article 17 through Tool-call logging + anomaly detection + access control enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0105	D4-CTL-05	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D4-CTL-05 operationalises part of Article 15 through Contractual security requirements + penetration testing + data flow mapping. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0106	D4-CTL-05	Art. 11	Technical documentation	P	Medium-High	GAISSF D4-CTL-05 operationalises part of Article 11 through Contractual security requirements + penetration testing + data flow mapping. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 11 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0107	D4-CTL-05	Art. 17	Quality management system	SP	High	GAISSF D4-CTL-05 operationalises part of Article 17 through Contractual security requirements + penetration testing + data flow mapping. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0108	D4-CTL-05	Art. 53	Obligations for providers of general-purpose AI models	P	Medium-High	GAISSF D4-CTL-05 operationalises part of Article 53 through Contractual security requirements + penetration testing + data flow mapping. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 53 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0109	D4-CTL-06	Art. 17	Quality management system	S	Medium	GAISSF D4-CTL-06 operationalises part of Article 17 through Network traffic analysis + SaaS discovery +	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						policy enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	requirements not established by this control alone.
GAISSF-CRO-027-MAP-0110	D4-CTL-06	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D4-CTL-06 operationalises part of Article 15 through Network traffic analysis + SaaS discovery + policy enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0111	D4-CTL-06	Art. 25	Responsibilities along the AI value chain	P	Medium-High	GAISSF D4-CTL-06 operationalises part of Article 25 through Network traffic analysis + SaaS discovery + policy enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 25 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0112	D4-CTL-06	Art. 9	Risk management system	S	Medium	GAISSF D4-CTL-06 operationalises part of Article 9 through Network traffic analysis + SaaS discovery + policy enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0113	D4-CTL-07	Art. 11	Technical documentation	P	Medium-High	GAISSF D4-CTL-07 operationalises part of Article 11 through Dependency scanning + CVE matching + automated patching. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 11 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0114	D4-CTL-07	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D4-CTL-07 operationalises part of Article 15 through Dependency scanning + CVE matching + automated patching. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0115	D4-CTL-07	Art. 17	Quality management system	S	Medium	GAISSF D4-CTL-07 operationalises part of Article 17 through Dependency scanning + CVE matching + automated patching. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0116	D4-CTL-07	Art. 25	Responsibilities along the AI value	P	Medium-High	GAISSF D4-CTL-07	Article 25 also depends on legal

Record	GAISSF	Article	Provision chain	Rel.	Confidence	Rationale	Residual gap
						operationalises part of Article 25 through Dependency scanning + CVE matching + automated patching. The relationship is limited to the control's stated scope and does not establish legal compliance.	role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0117	D5-CTL-01	Art. 9	Risk management system	S	Medium	GAISSF D5-CTL-01 operationalises part of Article 9 through Content safety classifier + refusal engine. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0118	D5-CTL-01	Art. 5	Prohibited AI practices	S	Medium	GAISSF D5-CTL-01 operationalises part of Article 5 through Content safety classifier + refusal engine. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 5 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0119	D5-CTL-01	Art. 13	Transparency and provision of information to deployers	P	Medium-High	GAISSF D5-CTL-01 operationalises part of Article 13 through Content safety classifier + refusal engine. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 13 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0120	D5-CTL-01	Art. 14	Human oversight	P	Medium-High	GAISSF D5-CTL-01 operationalises part of Article 14 through Content safety classifier + refusal engine. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0121	D5-CTL-02	Art. 9	Risk management system	SP	High	GAISSF D5-CTL-02 operationalises part of Article 9 through PII detection + masking + access controls. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0122	D5-CTL-02	Art. 5	Prohibited AI practices	S	Medium	GAISSF D5-CTL-02 operationalises part of Article 5 through PII detection + masking + access controls. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 5 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0123	D5-CTL-02	Art. 13	Transparency and provision of information to deployers	P	Medium-High	GAISSF D5-CTL-02 operationalises part of Article 13 through PII detection + masking + access	Article 13 also depends on legal role, system classification, territorial scope, procedural duties, and evidence

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						controls. The relationship is limited to the control's stated scope and does not establish legal compliance.	requirements not established by this control alone.
GAISSF-CRO-027-MAP-0124	D5-CTL-02	Art. 14	Human oversight	P	Medium-High	GAISSF D5-CTL-02 operationalises part of Article 14 through PII detection + masking + access controls. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0125	D5-CTL-03	Art. 9	Risk management system	S	Medium	GAISSF D5-CTL-03 operationalises part of Article 9 through n-gram overlap detection + refusal. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0126	D5-CTL-03	Art. 5	Prohibited AI practices	S	Medium	GAISSF D5-CTL-03 operationalises part of Article 5 through n-gram overlap detection + refusal. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 5 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0127	D5-CTL-03	Art. 13	Transparency and provision of information to deployers	P	Medium-High	GAISSF D5-CTL-03 operationalises part of Article 13 through n-gram overlap detection + refusal. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 13 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0128	D5-CTL-03	Art. 14	Human oversight	P	Medium-High	GAISSF D5-CTL-03 operationalises part of Article 14 through n-gram overlap detection + refusal. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0129	D5-CTL-04	Art. 9	Risk management system	SP	High	GAISSF D5-CTL-04 operationalises part of Article 9 through C2PA-compliant watermarking + tamper resistance testing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0130	D5-CTL-04	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D5-CTL-04 operationalises part of Article 15 through C2PA-compliant watermarking + tamper resistance testing. The relationship is limited to the control's stated scope and does not establish legal	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale compliance.	Residual gap
GAISSF-CRO-027-MAP-0131	D5-CTL-04	Art. 5	Prohibited AI practices	S	Medium	GAISSF D5-CTL-04 operationalises part of Article 5 through C2PA-compliant watermarking + tamper resistance testing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 5 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0132	D5-CTL-04	Art. 13	Transparency and provision of information to deployers	P	Medium-High	GAISSF D5-CTL-04 operationalises part of Article 13 through C2PA-compliant watermarking + tamper resistance testing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 13 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0133	D5-CTL-05	Art. 9	Risk management system	S	Medium	GAISSF D5-CTL-05 operationalises part of Article 9 through Data minimization + purpose limitation + machine unlearning. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0134	D5-CTL-05	Art. 5	Prohibited AI practices	S	Medium	GAISSF D5-CTL-05 operationalises part of Article 5 through Data minimization + purpose limitation + machine unlearning. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 5 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0135	D5-CTL-05	Art. 13	Transparency and provision of information to deployers	P	Medium-High	GAISSF D5-CTL-05 operationalises part of Article 13 through Data minimization + purpose limitation + machine unlearning. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 13 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0136	D5-CTL-05	Art. 14	Human oversight	P	Medium-High	GAISSF D5-CTL-05 operationalises part of Article 14 through Data minimization + purpose limitation + machine unlearning. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0137	D5-CTL-06	Art. 9	Risk management system	S	Medium	GAISSF D5-CTL-06 operationalises part of Article 9 through Differential privacy + membership inference testing. The relationship is limited to the control's stated scope and does not	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-027-MAP-0138	D5-CTL-06	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D5-CTL-06 operationalises part of Article 15 through Differential privacy + membership inference testing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0139	D5-CTL-06	Art. 13	Transparency and provision of information to deployers	P	Medium-High	GAISSF D5-CTL-06 operationalises part of Article 13 through Differential privacy + membership inference testing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 13 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0140	D5-CTL-06	Art. 14	Human oversight	P	Medium-High	GAISSF D5-CTL-06 operationalises part of Article 14 through Differential privacy + membership inference testing. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0141	D6-CTL-01	Art. 9	Risk management system	SP	High	GAISSF D6-CTL-01 operationalises part of Article 9 through Approval workflow + policy enforcement + audit log. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0142	D6-CTL-01	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D6-CTL-01 operationalises part of Article 27 through Approval workflow + policy enforcement + audit log. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0143	D6-CTL-01	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D6-CTL-01 operationalises part of Article 26 through Approval workflow + policy enforcement + audit log. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0144	D6-CTL-01	Art. 4	AI literacy	S	Medium	GAISSF D6-CTL-01 operationalises part of Article 4 through Approval workflow + policy enforcement + audit log. The relationship is limited to the control's stated scope and does not establish legal	Article 4 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale compliance.	Residual gap
GAISSF-CRO-027-MAP-0145	D6-CTL-02	Art. 9	Risk management system	S	Medium	GAISSF D6-CTL-02 operationalises part of Article 9 through Structured logging + SIEM integration + retention enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0146	D6-CTL-02	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D6-CTL-02 operationalises part of Article 27 through Structured logging + SIEM integration + retention enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0147	D6-CTL-02	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D6-CTL-02 operationalises part of Article 26 through Structured logging + SIEM integration + retention enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0148	D6-CTL-02	Art. 4	AI literacy	S	Medium	GAISSF D6-CTL-02 operationalises part of Article 4 through Structured logging + SIEM integration + retention enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 4 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0149	D6-CTL-03	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D6-CTL-03 operationalises part of Article 27 through Standardized template + version control + public accessibility. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0150	D6-CTL-03	Art. 9	Risk management system	SP	High	GAISSF D6-CTL-03 operationalises part of Article 9 through Standardized template + version control + public accessibility. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0151	D6-CTL-03	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D6-CTL-03 operationalises part of Article 26 through Standardized template + version control + public accessibility. The relationship is limited to the	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						control's stated scope and does not establish legal compliance.	
GAISSF-CRO-027-MAP-0152	D6-CTL-03	Art. 17	Quality management system	SP	High	GAISSF D6-CTL-03 operationalises part of Article 17 through Standardized template + version control + public accessibility. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0153	D6-CTL-04	Art. 9	Risk management system	S	Medium	GAISSF D6-CTL-04 operationalises part of Article 9 through AI-IR runbook + tabletop exercises + containment automation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0154	D6-CTL-04	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D6-CTL-04 operationalises part of Article 27 through AI-IR runbook + tabletop exercises + containment automation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0155	D6-CTL-04	Art. 21	Cooperation with competent authorities	S	Medium	GAISSF D6-CTL-04 operationalises part of Article 21 through AI-IR runbook + tabletop exercises + containment automation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 21 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0156	D6-CTL-04	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D6-CTL-04 operationalises part of Article 15 through AI-IR runbook + tabletop exercises + containment automation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0157	D6-CTL-05	Art. 9	Risk management system	S	Medium	GAISSF D6-CTL-05 operationalises part of Article 9 through Access revocation + decommission audit + scheduled lifecycle. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0158	D6-CTL-05	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D6-CTL-05 operationalises part of Article 27 through Access revocation + decommission audit	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						+ scheduled lifecycle. The relationship is limited to the control's stated scope and does not establish legal compliance.	requirements not established by this control alone.
GAISSF-CRO-027-MAP-0159	D6-CTL-05	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D6-CTL-05 operationalises part of Article 26 through Access revocation + decommission audit + scheduled lifecycle. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0160	D6-CTL-05	Art. 4	AI literacy	S	Medium	GAISSF D6-CTL-05 operationalises part of Article 4 through Access revocation + decommission audit + scheduled lifecycle. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 4 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0161	D6-CTL-06	Art. 17	Quality management system	SP	High	GAISSF D6-CTL-06 operationalises part of Article 17 through Contractual security requirements + annual assessment + audit rights. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0162	D6-CTL-06	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D6-CTL-06 operationalises part of Article 15 through Contractual security requirements + annual assessment + audit rights. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0163	D6-CTL-06	Art. 9	Risk management system	SP	High	GAISSF D6-CTL-06 operationalises part of Article 9 through Contractual security requirements + annual assessment + audit rights. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0164	D6-CTL-06	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D6-CTL-06 operationalises part of Article 27 through Contractual security requirements + annual assessment + audit rights. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0165	D6-CTL-07	Art. 9	Risk management system	S	Medium	GAISSF D6-CTL-07 operationalises part	Article 9 also depends on legal role, system

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						of Article 9 through Failover systems + degraded mode + RTO/RPO definition. The relationship is limited to the control's stated scope and does not establish legal compliance.	classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0166	D6-CTL-07	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D6-CTL-07 operationalises part of Article 27 through Failover systems + degraded mode + RTO/RPO definition. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0167	D6-CTL-07	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D6-CTL-07 operationalises part of Article 26 through Failover systems + degraded mode + RTO/RPO definition. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0168	D6-CTL-07	Art. 4	AI literacy	S	Medium	GAISSF D6-CTL-07 operationalises part of Article 4 through Failover systems + degraded mode + RTO/RPO definition. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 4 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0169	D7-CTL-H01	Art. 9	Risk management system	S	Medium	GAISSF D7-CTL-H01 operationalises part of Article 9 through Simulation campaigns + click tracking + remedial training. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0170	D7-CTL-H01	Art. 14	Human oversight	P	Medium-High	GAISSF D7-CTL-H01 operationalises part of Article 14 through Simulation campaigns + click tracking + remedial training. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0171	D7-CTL-H01	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D7-CTL-H01 operationalises part of Article 27 through Simulation campaigns + click tracking + remedial training. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0172	D7-CTL-H01	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D7-CTL-H01 operationalises part of Article 15 through Simulation campaigns + click	Article 15 also depends on legal role, system classification, territorial scope,

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						tracking + remedial training. The relationship is limited to the control's stated scope and does not establish legal compliance.	procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0173	D7-CTL-H02	Art. 9	Risk management system	S	Medium	GAISSF D7-CTL-H02 operationalises part of Article 9 through Training modules + quiz + simulated attacks. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0174	D7-CTL-H02	Art. 14	Human oversight	P	Medium-High	GAISSF D7-CTL-H02 operationalises part of Article 14 through Training modules + quiz + simulated attacks. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0175	D7-CTL-H02	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D7-CTL-H02 operationalises part of Article 27 through Training modules + quiz + simulated attacks. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0176	D7-CTL-H02	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D7-CTL-H02 operationalises part of Article 15 through Training modules + quiz + simulated attacks. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0177	D7-CTL-H03	Art. 9	Risk management system	S	Medium	GAISSF D7-CTL-H03 operationalises part of Article 9 through Independent channel verification + policy enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0178	D7-CTL-H03	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D7-CTL-H03 operationalises part of Article 27 through Independent channel verification + policy enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0179	D7-CTL-H03	Art. 14	Human oversight	P	Medium-High	GAISSF D7-CTL-H03 operationalises part of Article 14 through Independent channel verification + policy enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-	D7-CTL-H03	Art. 5	Prohibited AI	S	Medium	GAISSF D7-CTL-	Article 5 also

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
MAP-0180			practices			H03 operationalises part of Article 5 through Independent channel verification + policy enforcement. The relationship is limited to the control's stated scope and does not establish legal compliance.	depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0181	D7-CTL-H04	Art. 9	Risk management system	S	Medium	GAISSF D7-CTL-H04 operationalises part of Article 9 through Tabletop exercises + IR plan + verification triggers. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0182	D7-CTL-H04	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D7-CTL-H04 operationalises part of Article 27 through Tabletop exercises + IR plan + verification triggers. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0183	D7-CTL-H04	Art. 14	Human oversight	P	Medium-High	GAISSF D7-CTL-H04 operationalises part of Article 14 through Tabletop exercises + IR plan + verification triggers. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0184	D7-CTL-H04	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D7-CTL-H04 operationalises part of Article 15 through Tabletop exercises + IR plan + verification triggers. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0185	D7-CTL-H05	Art. 9	Risk management system	S	Medium	GAISSF D7-CTL-H05 operationalises part of Article 9 through AI-generated phishing detection + SOC tuning + response automation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0186	D7-CTL-H05	Art. 27	Fundamental rights impact assessment for high-risk AI systems	P	Medium-High	GAISSF D7-CTL-H05 operationalises part of Article 27 through AI-generated phishing detection + SOC tuning + response automation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 27 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0187	D7-CTL-H05	Art. 14	Human oversight	P	Medium-High	GAISSF D7-CTL-H05 operationalises part of Article 14 through AI-generated phishing detection + SOC	Article 14 also depends on legal role, system classification, territorial scope, procedural duties,

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						tuning + response automation. The relationship is limited to the control's stated scope and does not establish legal compliance.	and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0188	D7-CTL-H05	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D7-CTL-H05 operationalises part of Article 15 through AI-generated phishing detection + SOC tuning + response automation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0189	D8-CTL-01	Art. 51	Classification of general-purpose AI models as general-purpose AI models with systemic risk	S	Medium	GAISSF D8-CTL-01 operationalises part of Article 51 through Risk classification framework + conformity assessment. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 51 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0190	D8-CTL-01	Art. 53	Obligations for providers of general-purpose AI models	P	Medium-High	GAISSF D8-CTL-01 operationalises part of Article 53 through Risk classification framework + conformity assessment. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 53 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0191	D8-CTL-01	Art. 54	Authorised representatives of providers of general-purpose AI models	S	Medium	GAISSF D8-CTL-01 operationalises part of Article 54 through Risk classification framework + conformity assessment. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 54 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0192	D8-CTL-01	Art. 55	Obligations of providers of general-purpose AI models with systemic risk	P	Medium-High	GAISSF D8-CTL-01 operationalises part of Article 55 through Risk classification framework + conformity assessment. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 55 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0193	D8-CTL-02	Art. 11	Technical documentation	P	Medium-High	GAISSF D8-CTL-02 operationalises part of Article 11 through Gap analysis methodology + remediation tracking. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 11 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0194	D8-CTL-02	Art. 17	Quality management	S	Medium	GAISSF D8-CTL-02	Article 17 also depends on legal

Record	GAISSF	Article	Provision system	Rel.	Confidence	Rationale	Residual gap
						operationalises part of Article 17 through Gap analysis methodology + remediation tracking. The relationship is limited to the control's stated scope and does not establish legal compliance.	role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0195	D8-CTL-02	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D8-CTL-02 operationalises part of Article 15 through Gap analysis methodology + remediation tracking. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0196	D8-CTL-02	Art. 22	Authorised representatives of providers of high-risk AI systems	S	Medium	GAISSF D8-CTL-02 operationalises part of Article 22 through Gap analysis methodology + remediation tracking. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 22 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0197	D8-CTL-03	Art. 17	Quality management system	S	Medium	GAISSF D8-CTL-03 operationalises part of Article 17 through Technical documentation + training data summary + copyright attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 17 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0198	D8-CTL-03	Art. 55	Obligations of providers of general-purpose AI models with systemic risk	P	Medium-High	GAISSF D8-CTL-03 operationalises part of Article 55 through Technical documentation + training data summary + copyright attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 55 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0199	D8-CTL-03	Art. 43	Conformity assessment	S	Medium	GAISSF D8-CTL-03 operationalises part of Article 43 through Technical documentation + training data summary + copyright attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0200	D8-CTL-03	Art. 9	Risk management system	S	Medium	GAISSF D8-CTL-03 operationalises part of Article 9 through Technical documentation + training data summary +	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap established by this control alone.
						copyright attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	
GAISSF-CRO-027-MAP-0201	D8-CTL-04	Art. 12	Record-keeping	P	Medium-High	GAISSF D8-CTL-04 operationalises part of Article 12 through Incident classification + notification workflow + SLA monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 12 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0202	D8-CTL-04	Art. 20	Corrective actions and duty of information	P	Medium-High	GAISSF D8-CTL-04 operationalises part of Article 20 through Incident classification + notification workflow + SLA monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 20 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0203	D8-CTL-04	Art. 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	P	Medium-High	GAISSF D8-CTL-04 operationalises part of Article 72 through Incident classification + notification workflow + SLA monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 72 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0204	D8-CTL-04	Art. 73	Reporting of serious incidents	P	Medium-High	GAISSF D8-CTL-04 operationalises part of Article 73 through Incident classification + notification workflow + SLA monitoring. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 73 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0205	D8-CTL-05	Art. 43	Conformity assessment	S	Medium	GAISSF D8-CTL-05 operationalises part of Article 43 through Secure development practices + attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0206	D8-CTL-05	Art. 9	Risk management system	S	Medium	GAISSF D8-CTL-05 operationalises part of Article 9 through Secure development practices + attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0207	D8-CTL-05	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D8-CTL-05 operationalises part	Article 15 also depends on legal role, system

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						of Article 15 through Secure development practices + attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0208	D8-CTL-05	Art. 55	Obligations of providers of general-purpose AI models with systemic risk	P	Medium-High	GAISSF D8-CTL-05 operationalises part of Article 55 through Secure development practices + attestation. The relationship is limited to the control's stated scope and does not establish legal compliance.	Article 55 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0209	D9-CTL-01	Art. 9	Risk management system	SP	High	GAISSF D9-CTL-01 (Physical Harm Boundary Enforcement) provides control objectives and evidence expectations that may support part of Article 9 (Risk management system) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0210	D9-CTL-01	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D9-CTL-01 (Physical Harm Boundary Enforcement) provides control objectives and evidence expectations that may support part of Article 15 (Accuracy, robustness and cybersecurity) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0211	D9-CTL-01	Art. 14	Human oversight	P	Medium-High	GAISSF D9-CTL-01 (Physical Harm Boundary Enforcement) provides control objectives and evidence expectations that may support part of Article 14 (Human oversight) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	
GAISSF-CRO-027-MAP-0212	D9-CTL-01	Art. 43	Conformity assessment	S	Medium	GAISSF D9-CTL-01 (Physical Harm Boundary Enforcement) provides control objectives and evidence expectations that may support part of Article 43 (Conformity assessment) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0213	D9-CTL-02	Art. 9	Risk management system	SP	High	GAISSF D9-CTL-02 (Safe State And Graceful Degradation) provides control objectives and evidence expectations that may support part of Article 9 (Risk management system) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0214	D9-CTL-02	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D9-CTL-02 (Safe State And Graceful Degradation) provides control objectives and evidence expectations that may support part of Article 15 (Accuracy, robustness and cybersecurity) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0215	D9-CTL-02	Art. 14	Human oversight	P	Medium-High	GAISSF D9-CTL-02 (Safe State And Graceful Degradation)	Article 14 also depends on legal role, system classification,

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						provides control objectives and evidence expectations that may support part of Article 14 (Human oversight) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0216	D9-CTL-02	Art. 43	Conformity assessment	S	Medium	GAISSF D9-CTL-02 (Safe State And Graceful Degradation) provides control objectives and evidence expectations that may support part of Article 43 (Conformity assessment) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0217	D9-CTL-03	Art. 9	Risk management system	SP	High	GAISSF D9-CTL-03 (Human Override And Emergency Stop) provides control objectives and evidence expectations that may support part of Article 9 (Risk management system) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0218	D9-CTL-03	Art. 14	Human oversight	P	Medium-High	GAISSF D9-CTL-03 (Human Override And Emergency Stop) provides control objectives and evidence expectations that may support part of Article 14 (Human oversight) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						level, architecture, product certification, or implementation method, and does not establish legal compliance.	
GAISSF-CRO-027-MAP-0219	D9-CTL-03	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D9-CTL-03 (Human Override And Emergency Stop) provides control objectives and evidence expectations that may support part of Article 15 (Accuracy, robustness and cybersecurity) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0220	D9-CTL-03	Art. 43	Conformity assessment	S	Medium	GAISSF D9-CTL-03 (Human Override And Emergency Stop) provides control objectives and evidence expectations that may support part of Article 43 (Conformity assessment) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0221	D9-CTL-04	Art. 9	Risk management system	SP	High	GAISSF D9-CTL-04 (Cyber-Physical Attack Detection) provides control objectives and evidence expectations that may support part of Article 9 (Risk management system) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0222	D9-CTL-04	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D9-CTL-04 (Cyber-Physical Attack Detection) provides control objectives and evidence expectations that may support part of	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap established by this control alone.
						Article 15 (Accuracy, robustness and cybersecurity) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	
GAISSF-CRO-027-MAP-0223	D9-CTL-04	Art. 43	Conformity assessment	S	Medium	GAISSF D9-CTL-04 (Cyber-Physical Attack Detection) provides control objectives and evidence expectations that may support part of Article 43 (Conformity assessment) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0224	D9-CTL-04	Art. 14	Human oversight	P	Medium-High	GAISSF D9-CTL-04 (Cyber-Physical Attack Detection) provides control objectives and evidence expectations that may support part of Article 14 (Human oversight) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0225	D9-CTL-05	Art. 9	Risk management system	SP	High	GAISSF D9-CTL-05 (Physical Environment Integrity Monitoring) provides control objectives and evidence expectations that may support part of Article 9 (Risk management system) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-027-MAP-0226	D9-CTL-05	Art. 15	Accuracy, robustness and cybersecurity	SP	High	GAISSF D9-CTL-05 (Physical Environment Integrity Monitoring) provides control objectives and evidence expectations that may support part of Article 15 (Accuracy, robustness and cybersecurity) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0227	D9-CTL-05	Art. 26	Obligations of deployers of high-risk AI systems	P	Medium-High	GAISSF D9-CTL-05 (Physical Environment Integrity Monitoring) provides control objectives and evidence expectations that may support part of Article 26 (Obligations of deployers of high-risk AI systems) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 26 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0228	D9-CTL-05	Art. 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	P	Medium-High	GAISSF D9-CTL-05 (Physical Environment Integrity Monitoring) provides control objectives and evidence expectations that may support part of Article 72 (Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 72 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0229	D9-CTL-06	Art. 9	Risk management system	S	Medium	GAISSF D9-CTL-06 (Actuator Command Verification) provides control objectives and evidence	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						expectations that may support part of Article 9 (Risk management system) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	requirements not established by this control alone.
GAISSF-CRO-027-MAP-0230	D9-CTL-06	Art. 15	Accuracy, robustness and cybersecurity	S	Medium	GAISSF D9-CTL-06 (Actuator Command Verification) provides control objectives and evidence expectations that may support part of Article 15 (Accuracy, robustness and cybersecurity) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 15 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0231	D9-CTL-06	Art. 14	Human oversight	P	Medium-High	GAISSF D9-CTL-06 (Actuator Command Verification) provides control objectives and evidence expectations that may support part of Article 14 (Human oversight) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0232	D9-CTL-06	Art. 43	Conformity assessment	S	Medium	GAISSF D9-CTL-06 (Actuator Command Verification) provides control objectives and evidence expectations that may support part of Article 43 (Conformity assessment) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture,	Article 43 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						product certification, or implementation method, and does not establish legal compliance.	
GAISSF-CRO-027-MAP-0233	D9-CTL-07	Art. 9	Risk management system	SP	High	GAISSF D9-CTL-07 (Physical Incident Evidence Preservation) provides control objectives and evidence expectations that may support part of Article 9 (Risk management system) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 9 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0234	D9-CTL-07	Art. 14	Human oversight	P	Medium-High	GAISSF D9-CTL-07 (Physical Incident Evidence Preservation) provides control objectives and evidence expectations that may support part of Article 14 (Human oversight) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 14 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0235	D9-CTL-07	Art. 12	Record-keeping	P	Medium-High	GAISSF D9-CTL-07 (Physical Incident Evidence Preservation) provides control objectives and evidence expectations that may support part of Article 12 (Record-keeping) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	Article 12 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.
GAISSF-CRO-027-MAP-0236	D9-CTL-07	Art. 19	Automatically generated logs	S	Medium	GAISSF D9-CTL-07 (Physical Incident Evidence Preservation) provides control objectives and evidence expectations that may support part of Article 19 (Automatically	Article 19 also depends on legal role, system classification, territorial scope, procedural duties, and evidence requirements not established by this control alone.

Record	GAISSF	Article	Provision	Rel.	Confidence	Rationale	Residual gap
						generated logs) where Physical AI or cyber-physical actuation is in scope. The mapping does not prescribe a universal safety-integrity level, design-assurance level, architecture, product certification, or implementation method, and does not establish legal compliance.	

7. Reverse Coverage and Implementation Consequences

The reverse register demonstrates mapping coverage only; it does not show legal completeness or conformance. Classification, prohibited-practice analysis, economic-operator duties, Article 2 sectoral-law interactions, conformity assessment, registration, fundamental-rights impact assessment, transparency, post-market monitoring, incident reporting and authority cooperation require actor-specific implementation. Article 73 reporting is immediate once its statutory trigger is met, with outer limits of 15 days ordinarily, 2 days for widespread infringement or Article 3(49)(b) incidents, and 10 days where death occurs; Article 74(1a) can redirect reports to the AI Office for systems under its competence. Article 99 penalty maxima are enforcement ceilings, not predicted outcomes.

8. Evidence Reuse

Potentially reusable evidence includes AI inventories, risk registers, threat models, data provenance records, test and validation reports, technical documentation, logs, human-oversight procedures, supplier assessments, incident records, post-market monitoring plans, corrective-action records, training records and management approvals. Reuse is conditional on scope, currency, ownership, integrity, provenance and legal sufficiency; this crosswalk does not determine evidence sufficiency.

9. Limitations

- Mapping does not establish legal equivalence, compliance, automatic conformance, a presumption of conformity, certification credit, evidence sufficiency or operating effectiveness.
- The crosswalk covers 51 selected material provisions rather than every recital, paragraph, annex or enforcement provision. Current-law dependencies outside the standalone mapping set include Article 4a, Article 60a, amended Article 75, Articles 75a-75d, Article 42(3) and Article 101; their absence from standalone mapping records must not be read as legal irrelevance.
- GAISSF is an implementation and assurance framework; the EU AI Act also imposes legal, procedural, market-surveillance and economic-operator duties.
- The current legal baseline is the consolidated text of 27 July 2026; later amendments, application dates, delegated/implementing acts, harmonised standards, common specifications, codes of practice, Commission guidelines and competent-authority practice must be revalidated.
- The applicability of the Act depends on territory, actor role, system/model classification, intended purpose, Article 2 sectoral-law interactions, exceptions and transitional provisions.

Physical-AI boundary: D9 is additional/conditional where Physical AI or cyber-physical actuation is in scope. PAI-SF™ and CSX-PAISF-004 provide mapping/context only and do not establish equivalence, evidence sufficiency or automatic conformance.

10. Notably Absent

No evidence was identified that GAISSE certification automatically establishes EU AI Act conformity; GAISSE certification is not currently offered. Nothing in this mapping replaces legal classification, conformity assessment, CE marking, registration, competent-authority determinations or actor-specific legal analysis. The mapping does not establish equivalence, automatic conformance, certification credit, evidence sufficiency or operating effectiveness. No held/internal VTS asset, unpublished benchmark suite, test harness or schema tooling is a public-package dependency. Current-law provisions and dependencies not separately mapped include Article 4a, Article 60a, amended Article 75, Articles 75a-75d, Article 42(3) and Article 101. Article 2 sectoral-law interactions and future Article 2(13) delegated acts may materially change which requirements apply to Article 6(1) product systems. Article 73 reporting windows and Article 99 penalty maxima are legal requirements, not GAISSE control outcomes.

Annex A — Source URLs

<https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27>

<https://eur-lex.europa.eu/eli/reg/2026/1744/oj>

<https://digital-strategy.ec.europa.eu/en/policies/enforcement-ai-act>

<https://digital-strategy.ec.europa.eu/en/policies/guidelines-ai-high-risk-systems>