

ODA3 INSTITUTE

CROSSWALK

GAISSF™–OWASP Top 10 for LLM Applications 2025 Mapping

AI Security Risk and Control Crosswalk

GAISSF-CRO-024 | Informative crosswalk | Draft for Publication

Candidate 29 June 2026 | Updated 5 October 2026

© 2026 ODA3 Pvt Ltd

LICENCE NOTICE — GEL v1.0 | GAISSF-CRO-024

This document is part of the GAISSF Ecosystem published by ODA3 Institute (ODA3 Pvt Ltd) under the GAISSF Ecosystem Licence (GEL) v1.0. OWASP names, publication identifiers and marks are used solely for identification. No endorsement, affiliation, certification credit, recognition, equivalence, evidence sufficiency, vulnerability absence, legal compliance, operating effectiveness or automatic conformance is implied.

GAISSF™ is a trademark of ODA3 Pvt Ltd. GAISSF certification is not currently offered; any future certification scheme would require separately approved and published governance.

This document is provided “AS IS” and is informative. It does not replace application threat modelling, secure engineering, penetration testing, red teaming, or verification of deployed controls.

Public Access & Publication Status

This full crosswalk is intended for public release through docs.oda3.org / official ODA3 publication channels. It is an informative mapping to the OWASP Top 10 for LLM Applications 2025 edition, not a substitution or certification mechanism. Technical reconciliation was updated 5 October 2026; independent crosswalk review and explicit publication approval remain open. OWASP released a 2026 edition in August 2026; that later edition is not mapped by this document and requires a separate revalidation or crosswalk.

Field	Controlled value
Document ID	GAISSF-CRO-024
Title	GAISSF™–OWASP Top 10 for LLM Applications 2025 Mapping
Version	1.0
Status	Draft for Publication
Classification	Crosswalk — informative / public
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
GAISSF baseline	GAISSF™ v1.0: 59 controls / 9 domains; Applicable-Control Baseline = 52 D1-D8 + applicable D9
OWASP target baseline	OWASP Top 10 for LLM Applications 2025 — released 17 November 2024
Current-source note	OWASP Top 10 for LLM Applications 2026 is a later edition (August 2026) and is not mapped here
Verification date	Technical reconciliation updated 5 October 2026
Distribution	Public — docs.oda3.org / official ODA3 publication channels

Reliance notice: This document records analytical relationships only. It does not establish OWASP endorsement, certification, equivalence, vulnerability absence, legal compliance, or operating effectiveness.

Document control and source baseline

Source	Version / date	Role
GAISSF Framework Standard	GAISSF-NOR-001 v1.0 — published 1 Jul 2026; updated 4 Oct 2026	Authoritative framework architecture, conformance model and Applicable-Control Baseline
GAISSF Control Catalogue	GAISSF-NOR-004 v1.0 — published 1 Jul 2026; updated 4 Oct 2026	Authoritative 59-control catalogue; D9 additional/conditional
OWASP Top 10 for LLM Applications	2025 edition — released 17 Nov 2024	Ten risk categories used as the edition-bound external mapping target
OWASP Top 10 for LLM Applications	2026 edition — released Aug 2026	Later edition / change trigger only; not

Source	Version / date	Role
		mapped in GAISSF-CRO-024 v1.0

1. Executive summary

This Draft for Publication assesses all 59 GAISSF™ v1.0 controls against the ten OWASP Top 10 for LLM Applications 2025 risk categories. It retains 59 control-assessment records, including explicit no-material-mapping and outside-scope outcomes, plus a complete ten-risk reverse coverage register. The mapping is edition-bound to the 2025 OWASP list; OWASP released a 2026 edition in August 2026, which is not mapped here.

GAISSF supplies a broader auditable control architecture across model integrity, runtime security, agents, supply chain, content safety, governance, societal harm, regulatory alignment, and physical AI. The OWASP 2025 Top 10 supplies a focused application-risk prioritization resource. The artefacts are complementary but not equivalent, and several GAISSF controls intentionally fall outside the OWASP Top 10 scope.

2. Purpose, scope and intended use

- Support AI application threat modelling and control selection.
- Identify reusable GAISSF evidence for OWASP-oriented reviews.
- Expose residual implementation and testing gaps.
- Support assessment planning without claiming OWASP certification or vulnerability elimination.

3. Mapping methodology

Mappings were made at GAISSF-control-to-OWASP-risk level using shared attack surface, preventive or detective outcome, lifecycle position, evidence expectations, and residual application-specific work. Similar terminology alone was insufficient. Every GAISSF control was assessed, but a positive mapping was not forced: N records no material relationship and O records a concern outside the OWASP 2025 Top 10 scope. D9 mappings are conditional on the D9 control being included in the Applicable-Control Baseline. Where Physical AI is in scope, PAI-SF™ v1.0 may be used alongside GAISSF; CSX-PAISF-004 is mapping only and does not establish equivalence, evidence sufficiency, or automatic conformance.

Code	Meaning
SP	Strong partial: substantial risk-reduction relationship; material implementation work remains.
P	Partial: meaningful overlap with unmatched elements.
S	Supporting: indirect or enabling contribution.
N	No material relationship.
O	Outside scope.
U	Unable to determine.

4. OWASP 2025 risk inventory

Identifier	Risk	Working summary
LLM01:2025	Prompt Injection	Crafted direct or indirect inputs can alter model behavior, bypass instructions, expose data, or trigger unauthorized actions.
LLM02:2025	Sensitive Information Disclosure	Models and applications can reveal confidential, personal, proprietary, credential, or otherwise sensitive information.
LLM03:2025	Supply Chain	Compromised models, datasets, components, services, dependencies, or provenance can undermine application security and integrity.
LLM04:2025	Data and Model Poisoning	Manipulated pre-training, fine-tuning, retrieval, embedding, or model data can introduce backdoors, bias, unsafe behavior, or integrity failures.
LLM05:2025	Improper Output Handling	Insufficient validation, sanitization, encoding, or contextual handling of model outputs can create downstream exploits.
LLM06:2025	Excessive Agency	Excessive functionality, permissions, autonomy, or insufficient human approval can allow harmful or unintended actions.
LLM07:2025	System Prompt Leakage	System prompts or embedded instructions may be exposed and reveal sensitive logic, controls,

Identifier	Risk	Working summary
LLM08:2025	Vector and Embedding Weaknesses	Weaknesses in retrieval, vector stores, embeddings, access controls, segmentation, and data provenance can cause disclosure or manipulation.
LLM09:2025	Misinformation	Incorrect, fabricated, misleading, or insufficiently verified model outputs can undermine decisions and safety.
LLM10:2025	Unbounded Consumption	Uncontrolled model, token, tool, compute, or service consumption can cause denial of service, cost escalation, degradation, or theft-related abuse.

5. Reverse coverage register

OWASP risk	Mapped GAISSE controls	Coverage	Confidence	Residual limitation
LLM01:2025 Prompt Injection	D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D6-CTL-02, D9-CTL-04	Partially Addressed	High	Application-specific architecture, threat modelling, testing depth, and operating-effectiveness evidence remain necessary. Mapping alone does not demonstrate mitigation.
LLM02:2025 Sensitive Information Disclosure	D3-CTL-06, D3-CTL-07, D5-CTL-02, D5-CTL-05, D5-CTL-06	Partially Addressed	High	Application-specific architecture, threat modelling, testing depth, and operating-effectiveness evidence remain necessary. Mapping alone does not demonstrate mitigation.
LLM03:2025 Supply Chain	D1-CTL-06, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D6-CTL-05, D6-CTL-06	Substantially Addressed	High	Application-specific architecture, threat modelling, testing depth, and operating-effectiveness evidence remain necessary. Mapping alone does not demonstrate mitigation.
LLM04:2025 Data and Model Poisoning	D1-CTL-01, D1-CTL-04, D1-CTL-07, D1-CTL-08, D1-CTL-09	Substantially Addressed	High	Application-specific architecture, threat modelling, testing depth, and operating-effectiveness evidence remain necessary. Mapping alone does not demonstrate mitigation.
LLM05:2025 Improper Output Handling	D5-CTL-01	Supporting only	Low	GAISSE content/output controls do not substitute for application-layer encoding, sanitization, sink controls, downstream interpreter security or secure software engineering.
LLM06:2025 Excessive Agency	D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D6-CTL-01, D9-CTL-	Partially Addressed	High	Agent permissions, tool design, human approval, and application-specific

OWASP risk	Mapped GAISSF controls	Coverage	Confidence	Residual limitation
	01, D9-CTL-02, D9-CTL-03, D9-CTL-06			authorization remain necessary; D9 mappings are conditional when Physical AI is in scope.
LLM07:2025 System Prompt Leakage	D2-CTL-06	Supporting only	Low-Medium	GAISSF provides supporting context-isolation and disclosure controls, but does not contain a dedicated system-prompt-secrecy control in this baseline.
LLM08:2025 Vector and Embedding Weaknesses	D1-CTL-05	Partially Addressed	High	Application-specific architecture, threat modelling, testing depth, and operating-effectiveness evidence remain necessary. Mapping alone does not demonstrate mitigation.
LLM09:2025 Misinformation	D1-CTL-03	Supporting only	Medium-Low	GAISSF includes supporting drift/content controls, but the source control set does not directly implement the full application-specific misinformation and grounding problem.
LLM10:2025 Unbounded Consumption	D1-CTL-02, D6-CTL-04, D6-CTL-07	Partially Addressed	Medium	Application-specific architecture, threat modelling, testing depth, and operating-effectiveness evidence remain necessary. Mapping alone does not demonstrate mitigation.

6. Risk-by-risk analysis

LLM01:2025 Prompt Injection

Crafted direct or indirect inputs can alter model behavior, bypass instructions, expose data, or trigger unauthorized actions.

Primary / supporting GAISSF controls: D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D6-CTL-02, D9-CTL-04

Assessment conclusion: Partially Addressed; confidence High.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operating effectiveness; documentary mapping alone cannot demonstrate mitigation.

LLM02:2025 Sensitive Information Disclosure

Models and applications can reveal confidential, personal, proprietary, credential, or otherwise sensitive information.

Primary / supporting GAISSF controls: D3-CTL-06, D3-CTL-07, D5-CTL-02, D5-CTL-05, D5-CTL-06

Assessment conclusion: Partially Addressed; confidence High.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operating effectiveness; documentary mapping alone cannot demonstrate mitigation.

LLM03:2025 Supply Chain

Compromised models, datasets, components, services, dependencies, or provenance can undermine application security and integrity.

Primary / supporting GAISSE controls: D1-CTL-06, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D6-CTL-05, D6-CTL-06

Assessment conclusion: Substantially Addressed; confidence High.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operating effectiveness; documentary mapping alone cannot demonstrate mitigation.

LLM04:2025 Data and Model Poisoning

Manipulated pre-training, fine-tuning, retrieval, embedding, or model data can introduce backdoors, bias, unsafe behavior, or integrity failures.

Primary / supporting GAISSE controls: D1-CTL-01, D1-CTL-04, D1-CTL-07, D1-CTL-08, D1-CTL-09

Assessment conclusion: Substantially Addressed; confidence High.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operating effectiveness; documentary mapping alone cannot demonstrate mitigation.

LLM05:2025 Improper Output Handling

Insufficient validation, sanitization, encoding, or contextual handling of model outputs can create downstream exploits.

Primary / supporting GAISSE controls: D5-CTL-01

Assessment conclusion: Supporting only; confidence Low.

Residual gap: application-layer output encoding, sanitization, parser/interpreter controls and downstream sink security remain outside the direct GAISSE control set represented here.

LLM06:2025 Excessive Agency

Excessive functionality, permissions, autonomy, or insufficient human approval can allow harmful or unintended actions.

Primary / supporting GAISSE controls: D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D6-CTL-01, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-06

Assessment conclusion: Partially Addressed; confidence High.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operating effectiveness; documentary mapping alone cannot demonstrate mitigation.

LLM07:2025 System Prompt Leakage

System prompts or embedded instructions may be exposed and reveal sensitive logic, controls, or operational context.

Primary / supporting GAISSE controls: D2-CTL-06

Assessment conclusion: Supporting only; confidence Low-Medium.

Residual gap: the GAISSE baseline provides supporting context-isolation and disclosure controls but no dedicated system-prompt-secrecy control.

LLM08:2025 Vector and Embedding Weaknesses

Weaknesses in retrieval, vector stores, embeddings, access controls, segmentation, and data provenance can cause disclosure or manipulation.

Primary / supporting GAISSF controls: D1-CTL-05

Assessment conclusion: Partially Addressed; confidence High.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operating effectiveness; documentary mapping alone cannot demonstrate mitigation.

LLM09:2025 Misinformation

Incorrect, fabricated, misleading, or insufficiently verified model outputs can undermine decisions and safety.

Primary / supporting GAISSF controls: D1-CTL-03

Assessment conclusion: Supporting only; confidence Medium-Low.

Residual gap: application-specific grounding, factuality evaluation, provenance and human-review design remain necessary; mapping does not establish output truthfulness.

LLM10:2025 Unbounded Consumption

Uncontrolled model, token, tool, compute, or service consumption can cause denial of service, cost escalation, degradation, or theft-related abuse.

Primary / supporting GAISSF controls: D1-CTL-02, D6-CTL-04, D6-CTL-07

Assessment conclusion: Partially Addressed; confidence Medium.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operating effectiveness; documentary mapping alone cannot demonstrate mitigation.

7. Evidence reuse guidance

- Threat models and abuse-case registers
- Prompt-injection and adversarial test results
- Data classification and disclosure-control records
- Supplier, model, dataset, and component provenance records
- Poisoning and integrity validation reports
- Output-validation and downstream-execution controls
- Agent tool inventories, permission models, and human-approval records
- RAG, vector-store, embedding, and tenant-isolation tests
- Accuracy, grounding, provenance, and human-review evidence
- Rate-limit, quota, cost-monitoring, availability, and abuse-detection records

8. Limitations

- Mapping is not OWASP endorsement, certification, equivalence, evidence sufficiency, automatic conformance, vulnerability absence, or proof of secure implementation.
- OWASP Top 10 is a prioritized risk-awareness resource, not a complete security standard or exhaustive threat catalogue.
- GAISSF controls can support multiple risks; actual mitigation depends on architecture, implementation, testing, monitoring, and evidence.
- The crosswalk does not replace application threat modelling, penetration testing, red teaming, or secure software engineering.
- Revalidation is required when GAISSF or the mapped OWASP source baseline changes. OWASP released a 2026 Top 10 edition in August 2026; this v1.0 crosswalk remains explicitly bound to the 2025 edition.

9. Notably absent

- No OWASP certification or endorsement mechanism for this crosswalk is claimed or implied.
- No basis exists for claiming that documentary mapping proves a vulnerability is absent.

- No basis exists for treating the Top 10 as an exhaustive security standard.
- No universal compliance percentage, safe harbour, or automatic regulatory conclusion is asserted.

Annex A - Complete GAISSF-to-OWASP mapping register

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-024-MAP-0001	D1-CTL-01 Dataset Provenance & Poisoning Prevention	LLM04:2025 Data and Model Poisoning	SP	High	D1-CTL-01 Dataset Provenance & Poisoning Prevention has an outcome-level relationship to LLM04:2025 Data and Model Poisoning. The relationship is classified SP because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0002	D1-CTL-02 Model Extraction Resistance	LLM10:2025 Unbounded Consumption	S	Low	D1-CTL-02 Model Extraction Resistance has an outcome-level relationship to LLM10:2025 Unbounded Consumption. The relationship is classified S because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0003	D1-CTL-03 Behavioral Drift Detection	LLM09:2025 Misinformation	S	Medium-Low	D1-CTL-03 Behavioral Drift Detection has an outcome-level relationship to LLM09:2025 Misinformation. The relationship is classified S because the	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary;

Record	GAISSE control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					GAISSE control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	documentary mapping is not evidence sufficiency or automatic conformance.
GAISSE-CRO-024-MAP-0004	D1-CTL-04 Federated Learning Poisoning Prevention	LLM04:2025 Data and Model Poisoning	SP	High	D1-CTL-04 Federated Learning Poisoning Prevention has an outcome-level relationship to LLM04:2025 Data and Model Poisoning. The relationship is classified SP because the GAISSE control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSE-CRO-024-MAP-0005	D1-CTL-05 Embedding Space Robustness	LLM08:2025 Vector and Embedding Weaknesses	SP	High	D1-CTL-05 Embedding Space Robustness has an outcome-level relationship to LLM08:2025 Vector and Embedding Weaknesses. The relationship is classified SP because the GAISSE control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSE-CRO-024-MAP-0006	D1-CTL-06 Post-Quantum Model Signing & Crypto Hardening	LLM03:2025 Supply Chain	S	Medium	D1-CTL-06 Post-Quantum Model Signing & Crypto Hardening has an outcome-level relationship to LLM03:2025	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					Supply Chain. The relationship is classified S because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0007	D1-CTL-07 Lora/Adapter Integrity Verification	LLM04:2025 Data and Model Poisoning	P	Medium-High	D1-CTL-07 Lora/Adapter Integrity Verification has an outcome-level relationship to LLM04:2025 Data and Model Poisoning. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0008	D1-CTL-08 Model Merge Attack Detection	LLM04:2025 Data and Model Poisoning	P	Medium	D1-CTL-08 Model Merge Attack Detection has an outcome-level relationship to LLM04:2025 Data and Model Poisoning. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0009	D1-CTL-09 Quantization Backdoor Screening	LLM04:2025 Data and Model Poisoning	P	Medium-High	D1-CTL-09 Quantization Backdoor Screening has an outcome-level	Application-specific threat modelling, adversarial testing, implementation

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					relationship to LLM04:2025 Data and Model Poisoning. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0010	D2-CTL-01 Direct Prompt Injection Prevention	LLM01:2025 Prompt Injection	SP	High	D2-CTL-01 Direct Prompt Injection Prevention has an outcome-level relationship to LLM01:2025 Prompt Injection. The relationship is classified SP because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0011	D2-CTL-02 Indirect Prompt Injection Prevention	LLM01:2025 Prompt Injection	SP	High	D2-CTL-02 Indirect Prompt Injection Prevention has an outcome-level relationship to LLM01:2025 Prompt Injection. The relationship is classified SP because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0012	D2-CTL-03 Jailbreak Resistance Testing	LLM01:2025 Prompt Injection	P	Medium-High	D2-CTL-03 Jailbreak Resistance Testing has an outcome-level	Application-specific threat modelling, adversarial testing,

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					relationship to LLM01:2025 Prompt Injection. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0013	D2-CTL-04 Multi-Modal Injection Defense	LLM01:2025 Prompt Injection	P	Medium-High	D2-CTL-04 Multi-Modal Injection Defense has an outcome-level relationship to LLM01:2025 Prompt Injection. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0014	D2-CTL-05 Function Call/Tool Call Injection Prevention	LLM01:2025 Prompt Injection	P	Medium-High	D2-CTL-05 Function Call/Tool Call Injection Prevention has an outcome-level relationship to LLM01:2025 Prompt Injection. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0015	D2-CTL-06 Cross-Context Hijacking Mitigation	LLM07:2025 System Prompt Leakage	S	Medium-Low	D2-CTL-06 Cross-Context Hijacking Mitigation has an outcome-	Application-specific threat modelling, adversarial testing,

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					level relationship to LLM07:2025 System Prompt Leakage. The relationship is classified S because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0016	D3-CTL-01 Least Agency Enforcement	LLM06:2025 Excessive Agency	SP	High	D3-CTL-01 Least Agency Enforcement has an outcome-level relationship to LLM06:2025 Excessive Agency. The relationship is classified SP because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0017	D3-CTL-02 Inter-Agent Communication Security	LLM06:2025 Excessive Agency	P	Medium	D3-CTL-02 Inter-Agent Communication Security has an outcome-level relationship to LLM06:2025 Excessive Agency. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0018	D3-CTL-03 Agentic Prompt Chaining Detection	LLM06:2025 Excessive Agency	P	Medium-High	D3-CTL-03 Agentic Prompt Chaining Detection has an outcome-level relationship to	Application-specific threat modelling, adversarial testing, implementation verification,

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					LLM06:2025 Excessive Agency. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0019	D3-CTL-04 Embodied Ai Safety Controls	LLM06:2025 Excessive Agency	S	Medium-Low	D3-CTL-04 Embodied Ai Safety Controls has an outcome-level relationship to LLM06:2025 Excessive Agency. The relationship is classified S because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0020	D3-CTL-05 Multi-Agent Trust Chain Attestation	LLM06:2025 Excessive Agency	P	Medium	D3-CTL-05 Multi-Agent Trust Chain Attestation has an outcome-level relationship to LLM06:2025 Excessive Agency. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0021	D3-CTL-06 Persistent Memory Exfiltration Prevention	LLM02:2025 Sensitive Information Disclosure	P	Medium-High	D3-CTL-06 Persistent Memory Exfiltration Prevention has an outcome-level relationship to	Application-specific threat modelling, adversarial testing, implementation verification, and operating-

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					LLM02:2025 Sensitive Information Disclosure. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0022	D3-CTL-07 Secure Memory Lifecycle Management	LLM02:2025 Sensitive Information Disclosure	S	Medium	D3-CTL-07 Secure Memory Lifecycle Management has an outcome-level relationship to LLM02:2025 Sensitive Information Disclosure. The relationship is classified S because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0023	D4-CTL-01 Ai Bill Of Materials (Ai Bom) Maintenance	LLM03:2025 Supply Chain	SP	High	D4-CTL-01 Ai Bill Of Materials (Ai Bom) Maintenance has an outcome-level relationship to LLM03:2025 Supply Chain. The relationship is classified SP because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0024	D4-CTL-02 Model File & Artifact Scanning	LLM03:2025 Supply Chain	SP	High	D4-CTL-02 Model File & Artifact	Application-specific threat modelling,

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					Scanning has an outcome-level relationship to LLM03:2025 Supply Chain. The relationship is classified SP because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0025	D4-CTL-03 Model Hub & Registry Vetting	LLM03:2025 Supply Chain	SP	High	D4-CTL-03 Model Hub & Registry Vetting has an outcome-level relationship to LLM03:2025 Supply Chain. The relationship is classified SP because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0026	D4-CTL-04 Mcp Server Behavioral Monitoring	LLM03:2025 Supply Chain	P	Medium	D4-CTL-04 Mcp Server Behavioral Monitoring has an outcome-level relationship to LLM03:2025 Supply Chain. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0027	D4-CTL-05 Third-Party Ai Api Security Assessment	LLM03:2025 Supply Chain	SP	High	D4-CTL-05 Third-Party Ai Api Security Assessment	Application-specific threat modelling, adversarial

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					has an outcome-level relationship to LLM03:2025 Supply Chain. The relationship is classified SP because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0028	D4-CTL-06 Shadow Ai Discovery & Governance	LLM03:2025 Supply Chain	P	Medium-High	D4-CTL-06 Shadow Ai Discovery & Governance has an outcome-level relationship to LLM03:2025 Supply Chain. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0029	D4-CTL-07 Ai Software Composition Analysis (Sca)	LLM03:2025 Supply Chain	SP	High	D4-CTL-07 Ai Software Composition Analysis (Sca) has an outcome-level relationship to LLM03:2025 Supply Chain. The relationship is classified SP because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0030	D5-CTL-01 Harmful Content Blocking	LLM05:2025 Improper Output Handling	S	Low	D5-CTL-01 Harmful Content Blocking has	Application-specific threat modelling, adversarial

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					an outcome-level relationship to LLM05:2025 Improper Output Handling. The relationship is classified S because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0031	D5-CTL-02 Pii Leakage Prevention	LLM02:2025 Sensitive Information Disclosure	SP	High	D5-CTL-02 Pii Leakage Prevention has an outcome-level relationship to LLM02:2025 Sensitive Information Disclosure. The relationship is classified SP because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0032	D5-CTL-03 Copyright Detection	No material OWASP 2025 mapping	N	Not Rated	D5-CTL-03 Copyright Detection does not have a sufficiently direct outcome-level relationship to a specific OWASP Top 10 for LLM Applications 2025 risk category for this edition-bound crosswalk.	Do not infer absence of security relevance. Address the GAISSF control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSF-CRO-024-MAP-0033	D5-CTL-04 Ai Watermarking Robustness	No material OWASP 2025 mapping	N	Not Rated	D5-CTL-04 Ai Watermarking Robustness does not have a sufficiently direct outcome-	Do not infer absence of security relevance. Address the GAISSF control

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					level relationship to a specific OWASP Top 10 for LLM Applications 2025 risk category for this edition-bound crosswalk.	on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSF-CRO-024-MAP-0034	D5-CTL-05 Privacy-By-Design Verification	LLM02:2025 Sensitive Information Disclosure	P	Medium-High	D5-CTL-05 Privacy-By-Design Verification has an outcome-level relationship to LLM02:2025 Sensitive Information Disclosure. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0035	D5-CTL-06 Privacy-Preserving MI Validation	LLM02:2025 Sensitive Information Disclosure	S	Medium	D5-CTL-06 Privacy-Preserving MI Validation has an outcome-level relationship to LLM02:2025 Sensitive Information Disclosure. The relationship is classified S because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0036	D6-CTL-01 Human-In-The-Loop For High-Risk Actions	LLM06:2025 Excessive Agency	P	Medium-High	D6-CTL-01 Human-In-The-Loop For High-Risk Actions has an outcome-level relationship to	Application-specific threat modelling, adversarial testing, implementation verification,

Record	GAISSE control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					LLM06:2025 Excessive Agency. The relationship is classified P because the GAISSE control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSE-CRO-024-MAP-0037	D6-CTL-02 Audit Trail Completeness	LLM01:2025 Prompt Injection	S	Low	D6-CTL-02 Audit Trail Completeness has an outcome-level relationship to LLM01:2025 Prompt Injection. The relationship is classified S because the GAISSE control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSE-CRO-024-MAP-0038	D6-CTL-03 Ai Model Card Completeness	No material OWASP 2025 mapping	N	Not Rated	D6-CTL-03 Ai Model Card Completeness does not have a sufficiently direct outcome-level relationship to a specific OWASP Top 10 for LLM Applications 2025 risk category for this edition-bound crosswalk.	Do not infer absence of security relevance. Address the GAISSE control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSE-CRO-024-MAP-0039	D6-CTL-04 Ai Incident Response Readiness	LLM10:2025 Unbounded Consumption	S	Low	D6-CTL-04 Ai Incident Response Readiness has an outcome-level relationship to LLM10:2025 Unbounded Consumption. The	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					relationship is classified S because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0040	D6-CTL-05 Model Deprecation & Decommissioning	LLM03:2025 Supply Chain	S	Low	D6-CTL-05 Model Deprecation & Decommissioning has an outcome-level relationship to LLM03:2025 Supply Chain. The relationship is classified S because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0041	D6-CTL-06 Third-Party Ai Vendor Governance	LLM03:2025 Supply Chain	P	Medium-High	D6-CTL-06 Third-Party Ai Vendor Governance has an outcome-level relationship to LLM03:2025 Supply Chain. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0042	D6-CTL-07 Ai Resilience & Business Continuity	LLM10:2025 Unbounded Consumption	P	Medium-High	D6-CTL-07 Ai Resilience & Business Continuity has an outcome-level relationship to LLM10:2025 Unbounded Consumption.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence

Record	GAISSE control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					The relationship is classified P because the GAISSE control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation.	remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSE-CRO-024-MAP-0043	D7-CTL-H01 Ai-Generated Phishing Simulation	Outside OWASP 2025 Top 10 scope	O	Not Rated	D7-CTL-H01 Ai-Generated Phishing Simulation addresses a GAISSE concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	Do not infer absence of security relevance. Address the GAISSE control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSE-CRO-024-MAP-0044	D7-CTL-H02 Deepfake Detection Training	Outside OWASP 2025 Top 10 scope	O	Not Rated	D7-CTL-H02 Deepfake Detection Training addresses a GAISSE concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	Do not infer absence of security relevance. Address the GAISSE control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSE-CRO-024-MAP-0045	D7-CTL-H03 Out-Of-Band Authentication	Outside OWASP 2025 Top 10 scope	O	Not Rated	D7-CTL-H03 Out-Of-Band Authentication addresses a GAISSE concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	Do not infer absence of security relevance. Address the GAISSE control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
						concerns outside the OWASP Top 10 scope.
GAISSF-CRO-024-MAP-0046	D7-CTL-H04 Ai Social Engineering Ir	Outside OWASP 2025 Top 10 scope	O	Not Rated	D7-CTL-H04 Ai Social Engineering Ir addresses a GAISSF concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	Do not infer absence of security relevance. Address the GAISSF control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSF-CRO-024-MAP-0047	D7-CTL-H05 Ai-Enhanced External Attack Defense	Outside OWASP 2025 Top 10 scope	O	Not Rated	D7-CTL-H05 Ai-Enhanced External Attack Defense addresses a GAISSF concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	Do not infer absence of security relevance. Address the GAISSF control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSF-CRO-024-MAP-0048	D8-CTL-01 Eu Ai Act Risk Tier Mapping	Outside OWASP 2025 Top 10 scope	O	Not Rated	D8-CTL-01 Eu Ai Act Risk Tier Mapping addresses a GAISSF concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	Do not infer absence of security relevance. Address the GAISSF control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSF-CRO-024-MAP-0049	D8-CTL-02 Iso 42001 Gap Analysis	Outside OWASP 2025 Top 10 scope	O	Not Rated	D8-CTL-02 Iso 42001 Gap Analysis addresses a GAISSF	Do not infer absence of security relevance. Address the

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	GAISSF control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSF-CRO-024-MAP-0050	D8-CTL-03 Gpai Technical Documentation Verification	Outside OWASP 2025 Top 10 scope	O	Not Rated	D8-CTL-03 Gpai Technical Documentation Verification addresses a GAISSF concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	Do not infer absence of security relevance. Address the GAISSF control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSF-CRO-024-MAP-0051	D8-CTL-04 Dora lct Incident Reporting (Financial Sector)	Outside OWASP 2025 Top 10 scope	O	Not Rated	D8-CTL-04 Dora lct Incident Reporting (Financial Sector) addresses a GAISSF concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	Do not infer absence of security relevance. Address the GAISSF control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSF-CRO-024-MAP-0052	D8-CTL-05 Nist Sp 800-218A Compliance Check	Outside OWASP 2025 Top 10 scope	O	Not Rated	D8-CTL-05 Nist Sp 800-218A Compliance Check addresses a GAISSF concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk	Do not infer absence of security relevance. Address the GAISSF control on its own terms where it is in the Applicable-Control Baseline; use other threat models or

Record	GAISSE control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					inventory.	standards for concerns outside the OWASP Top 10 scope.
GAISSE-CRO-024-MAP-0053	D9-CTL-01 Physical Harm Boundary Enforcement	LLM06:2025 Excessive Agency	S	Low	D9-CTL-01 Physical Harm Boundary Enforcement has an outcome-level relationship to LLM06:2025 Excessive Agency. The relationship is classified S because the GAISSE control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation. For D9, this relationship is relevant only where the D9 control is in the Applicable-Control Baseline.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSE-CRO-024-MAP-0054	D9-CTL-02 Safe State And Graceful Degradation	LLM06:2025 Excessive Agency	P	Medium	D9-CTL-02 Safe State And Graceful Degradation has an outcome-level relationship to LLM06:2025 Excessive Agency. The relationship is classified P because the GAISSE control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation. For D9, this relationship is relevant only where the D9 control is in the Applicable-Control Baseline.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSE-CRO-	D9-CTL-03 Human Override And Emergency	LLM06:2025	P	Medium	D9-CTL-03	Application-

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
024-MAP-0055	Stop	Excessive Agency			Human Override And Emergency Stop has an outcome-level relationship to LLM06:2025 Excessive Agency. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation. For D9, this relationship is relevant only where the D9 control is in the Applicable-Control Baseline.	specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0056	D9-CTL-04 Cyber-Physical Attack Detection	LLM01:2025 Prompt Injection	S	Low	D9-CTL-04 Cyber-Physical Attack Detection has an outcome-level relationship to LLM01:2025 Prompt Injection. The relationship is classified S because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation. For D9, this relationship is relevant only where the D9 control is in the Applicable-Control Baseline.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0057	D9-CTL-05 Physical Environment Integrity Monitoring	Outside OWASP 2025 Top 10 scope	O	Not Rated	D9-CTL-05 Physical Environment Integrity Monitoring addresses a GAISSF	Do not infer absence of security relevance. Address the GAISSF control on its own

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.
GAISSF-CRO-024-MAP-0058	D9-CTL-06 Actuator Command Verification	LLM06:2025 Excessive Agency	P	Medium	D9-CTL-06 Actuator Command Verification has an outcome-level relationship to LLM06:2025 Excessive Agency. The relationship is classified P because the GAISSF control can reduce or evidence part of the OWASP risk but does not, by itself, demonstrate complete mitigation. For D9, this relationship is relevant only where the D9 control is in the Applicable-Control Baseline.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary; documentary mapping is not evidence sufficiency or automatic conformance.
GAISSF-CRO-024-MAP-0059	D9-CTL-07 Physical Incident Evidence Preservation	Outside OWASP 2025 Top 10 scope	O	Not Rated	D9-CTL-07 Physical Incident Evidence Preservation addresses a GAISSF concern that is materially outside the scope of the OWASP Top 10 for LLM Applications 2025 risk inventory.	Do not infer absence of security relevance. Address the GAISSF control on its own terms where it is in the Applicable-Control Baseline; use other threat models or standards for concerns outside the OWASP Top 10 scope.

Annex B - Change and verification record

Item	Status
GAISSE controls assessed	59
OWASP 2025 risks assessed	10
Positive mapping assessments	44
No-material / outside-scope assessments	3 no-material; 12 outside-scope
OWASP 2026 later edition identified	Yes — separate revalidation required; not mapped in this document
Independent crosswalk review	Required before publication approval