

ODA3 INSTITUTE

Crosswalk — Controlled Publication

GAISSF–OWASP LLM Top 10 Mapping

AI Security Risk and Control Crosswalk

DocID: CRO-024

Classification: Controlled Publication

LICENCE NOTICE — GEL v1.0 | 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), effective 1 June 2026. OWASP names and publication identifiers are used solely for identification. This document records analytical relationships only and does not establish OWASP endorsement, certification, equivalence, vulnerability absence, legal compliance, or operating effectiveness.

Commercial Use (GEL §3.4):

Use of this document as the basis for consulting, advisory, audit, assessment, certification, compliance, SaaS, training, or managed services requires a separate written commercial licence from ODA3 Institute.

Trademarks (GEL §9.1, §6):

GAISSF™ is a trademark of ODA3 Pvt Ltd, asserted on a common-law / use-in-commerce basis (registration applications pending). Third-party framework names (NIST, OWASP) are used solely for identification; no endorsement, affiliation, certification credit, or equivalence is implied.

Disclaimer (GEL §12): This document is provided “AS IS” without warranties of any kind. All enquiries: <https://oda3.org/> — Attribution (GEL §6): GAISSF™ is a framework of ODA3 Institute, referenced under the GAISSF Ecosystem Licence (GEL) v1.0.

Access & Publication Status

This document is the full crosswalk register and is a Controlled Publication. Distribution is limited to parties with an approved access request. The corresponding public Website Summary (methodology, key findings, and a representative sample) is available at <https://oda3.org/> — request full Controlled Publication access via the same site.

Document ID	CRO-024
Version	1.0
Status	Publication Candidate
Classification	Crosswalk
Publication date	29 June 2026
Publisher	ODA3 Institute

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	Normative framework and conformance baseline
GAISSF Control Catalogue	GAISSF-NOR-004 v1.0	Authoritative 59-control source
OWASP Top 10 for LLM Applications	2025 edition; 17 November 2024	Ten risk categories used as external mapping targets

1. Executive summary

This crosswalk evaluates all 59 GAISSF v1.0 controls against the ten OWASP Top 10 for LLM Applications 2025 risk categories. It contains 59 forward mapping records and a complete ten-risk reverse coverage register.

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. OWASP supplies a concise vulnerability-oriented prioritization resource. The two artefacts are complementary but not equivalent.

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 level to OWASP risk-category level. Decisions considered shared attack surface, preventive and detective outcomes, lifecycle position, evidence expectations, and residual application-specific work. Similar terminology alone was not sufficient.

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, or operational context.
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 GAISSF controls	Coverage	Confidence	Residual limitation
LLM01:2025 Prompt Injection	D1-CTL-03, D1-CTL-05, D1-CTL-06, D1-CTL-08, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D6-CTL-02, D6-CTL-03	Indirectly Supported	Low	OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational effectiveness; documentary mapping alone cannot demonstrate mitigation.
LLM02:2025 Sensitive Information Disclosure	D5-CTL-05	Indirectly Supported	Low	OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational effectiveness; documentary mapping alone cannot demonstrate mitigation.
LLM03:2025 Supply Chain	D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D6-CTL-06, D8-CTL-02	Indirectly Supported	Low	OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational effectiveness; documentary mapping alone cannot demonstrate mitigation.
LLM04:2025 Data and Model Poisoning	D1-CTL-01, D1-CTL-04, D1-CTL-07, D1-CTL-09, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-06, D8-CTL-03, D9-CTL-07	Indirectly Supported	Low	OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational effectiveness; documentary mapping alone cannot demonstrate mitigation.
LLM05:2025 Improper Output Handling		Indirectly Supported	Low	OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational effectiveness; documentary mapping alone cannot demonstrate mitigation.
LLM06:2025 Excessive Agency	D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D6-CTL-01, D9-CTL-02	Indirectly Supported	Low	OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational effectiveness; documentary mapping alone cannot demonstrate mitigation.
LLM07:2025 System Prompt Leakage		Indirectly Supported	Low	OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational effectiveness; documentary mapping alone cannot demonstrate mitigation.
LLM08:2025 Vector and Embedding Weaknesses	D7-CTL-H01	Indirectly Supported	Low	OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational effectiveness; documentary mapping alone cannot demonstrate mitigation.
LLM09:2025 Misinformation	D7-CTL-H03, D7-CTL-H04	Indirectly Supported	Low	OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational effectiveness; documentary mapping alone cannot demonstrate mitigation.
LLM10:2025 Unbounded Consumption	D1-CTL-02, D6-CTL-04, D6-CTL-07, D7-CTL-H02	Indirectly Supported	Low	OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational effectiveness; documentary mapping alone cannot 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 GAISSF controls: D1-CTL-03, D1-CTL-05, D1-CTL-06, D1-CTL-08, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D6-CTL-02, D6-CTL-03

Assessment conclusion: Indirectly Supported; confidence Low.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational 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 GAISSF controls: D5-CTL-05

Assessment conclusion: Indirectly Supported; confidence Low.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational 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 GAISSF controls: D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D6-CTL-06, D8-CTL-02

Assessment conclusion: Indirectly Supported; confidence Low.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational 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 GAISSF controls: D1-CTL-01, D1-CTL-04, D1-CTL-07, D1-CTL-09, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-06, D8-CTL-03, D9-CTL-07

Assessment conclusion: Indirectly Supported; confidence Low.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational 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 GAISSF controls:

Assessment conclusion: Indirectly Supported; confidence Low.

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

LLM06:2025 Excessive Agency

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

Primary GAISSF controls: D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D6-CTL-01, D9-CTL-02

Assessment conclusion: Indirectly Supported; confidence Low.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational 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 GAISSF controls:

Assessment conclusion: Indirectly Supported; confidence Low.

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

LLM08:2025 Vector and Embedding Weaknesses

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

Primary GAISSF controls: D7-CTL-H01

Assessment conclusion: Indirectly Supported; confidence Low.

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

LLM09:2025 Misinformation

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

Primary GAISSF controls: D7-CTL-H03, D7-CTL-H04

Assessment conclusion: Indirectly Supported; confidence Low.

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

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 GAISSF controls: D1-CTL-02, D6-CTL-04, D6-CTL-07, D7-CTL-H02

Assessment conclusion: Indirectly Supported; confidence Low.

Residual gap: OWASP risk exposure depends on architecture, implementation, threat context, testing depth, and operational 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, or proof of secure implementation.
- OWASP Top 10 is a prioritized risk-awareness resource, not a complete security standard or exhaustive threat catalogue.
- GAISF 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 GAISF or OWASP source baselines change.

9. Notably absent

- No OWASP certification or endorsement mechanism for this crosswalk was identified.
- 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 GAISF-to-OWASP mapping register

Record	GAISF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
CRO024-MAP-0001	D1-CTL-01 Dataset Provenance & Poisoning Prevention	LLM04:2025 Data and Model Poisoning	S	Low	GAISF D1-CTL-01 establishes AI-system controls or evidence that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0002	D1-CTL-02 Model Extraction Resistance	LLM10:2025 Unbounded Consumption	S	Low	GAISF D1-CTL-02 establishes AI-system controls or evidence that materially reduce exposure to LLM10:2025 Unbounded Consumption. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0003	D1-CTL-03 Behavioral Drift Detection	LLM01:2025 Prompt Injection	S	Low	GAISF D1-CTL-03 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0004	D1-CTL-04 Federated Learning Poisoning Prevention	LLM04:2025 Data and Model Poisoning	S	Low	GAISF D1-CTL-04 establishes AI-system controls or evidence	Application-specific threat modelling, adversarial testing,

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0005	D1-CTL-05 Embedding Space Robustness	LLM01:2025 Prompt Injection	S	Low	GAISSF D1-CTL-05 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0006	D1-CTL-06 Post-Quantum Model Signing & Crypto Hardening	LLM01:2025 Prompt Injection	S	Low	GAISSF D1-CTL-06 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0007	D1-CTL-07 Lora/Adapter Integrity Verification	LLM04:2025 Data and Model Poisoning	S	Low	GAISSF D1-CTL-07 establishes AI-system controls or evidence that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0008	D1-CTL-08 Model Merge Attack Detection	LLM01:2025 Prompt Injection	S	Low	GAISSF D1-CTL-08 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0009	D1-CTL-09 Quantization Backdoor Screening	LLM04:2025 Data and Model Poisoning	S	Low	GAISSF D1-CTL-09 establishes AI-system controls or evidence that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0010	D2-CTL-01 Direct Prompt Injection Prevention	LLM01:2025 Prompt Injection	S	Low	GAISSF D2-CTL-01 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0011	D2-CTL-02 Indirect Prompt Injection Prevention	LLM01:2025 Prompt Injection	S	Low	GAISSF D2-CTL-02 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0012	D2-CTL-03 Jailbreak Resistance Testing	LLM01:2025 Prompt Injection	S	Low	GAISSF D2-CTL-03 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0013	D2-CTL-04 Multi-Modal	LLM01:2025 Prompt	S	Low	GAISSF D2-CTL-04	Application-specific

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
	Injection Defense	Injection			establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0014	D2-CTL-05 Function Call/Tool Call Injection Prevention	LLM01:2025 Prompt Injection	S	Low	GAISSF D2-CTL-05 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0015	D2-CTL-06 Cross-Context Hijacking Mitigation	LLM01:2025 Prompt Injection	S	Low	GAISSF D2-CTL-06 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0016	D3-CTL-01 Least Agency Enforcement	LLM06:2025 Excessive Agency	S	Low	GAISSF D3-CTL-01 establishes AI-system controls or evidence that materially reduce exposure to LLM06:2025 Excessive Agency. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0017	D3-CTL-02 Inter-Agent Communication Security	LLM06:2025 Excessive Agency	S	Low	GAISSF D3-CTL-02 establishes AI-system controls or evidence that materially reduce exposure to LLM06:2025 Excessive Agency. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0018	D3-CTL-03 Agentic Prompt Chaining Detection	LLM06:2025 Excessive Agency	S	Low	GAISSF D3-CTL-03 establishes AI-system controls or evidence that materially reduce exposure to LLM06:2025 Excessive Agency. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0019	D3-CTL-04 Embodied AI Safety Controls	LLM06:2025 Excessive Agency	S	Low	GAISSF D3-CTL-04 establishes AI-system controls or evidence that materially reduce exposure to LLM06:2025 Excessive Agency. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0020	D3-CTL-05 Multi-Agent Trust Chain Attestation	LLM06:2025 Excessive Agency	S	Low	GAISSF D3-CTL-05 establishes AI-system controls or evidence that materially reduce exposure to LLM06:2025 Excessive Agency. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0021	D3-CTL-06 Persistent Memory Exfiltration Prevention	LLM06:2025 Excessive Agency	S	Low	GAISSF D3-CTL-06 establishes AI-system controls or evidence that materially reduce exposure to LLM06:2025 Excessive Agency. The relationship is preventive or detective support; it is not proof that the	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
CRO024-MAP-0022	D3-CTL-07 Secure Memory Lifecycle Management	LLM06:2025 Excessive Agency	S	Low	vulnerability is absent. GAISSF D3-CTL-07 establishes AI-system controls or evidence that materially reduce exposure to LLM06:2025 Excessive Agency. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0023	D4-CTL-01 Ai Bill Of Materials (Ai Bom) Maintenance	LLM03:2025 Supply Chain	S	Low	GAISSF D4-CTL-01 establishes AI-system controls or evidence that materially reduce exposure to LLM03:2025 Supply Chain. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0024	D4-CTL-02 Model File & Artifact Scanning	LLM03:2025 Supply Chain	S	Low	GAISSF D4-CTL-02 establishes AI-system controls or evidence that materially reduce exposure to LLM03:2025 Supply Chain. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0025	D4-CTL-03 Model Hub & Registry Vetting	LLM03:2025 Supply Chain	S	Low	GAISSF D4-CTL-03 establishes AI-system controls or evidence that materially reduce exposure to LLM03:2025 Supply Chain. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0026	D4-CTL-04 Mcp Server Behavioral Monitoring	LLM03:2025 Supply Chain	S	Low	GAISSF D4-CTL-04 establishes AI-system controls or evidence that materially reduce exposure to LLM03:2025 Supply Chain. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0027	D4-CTL-05 Third-Party Ai Api Security Assessment	LLM03:2025 Supply Chain	S	Low	GAISSF D4-CTL-05 establishes AI-system controls or evidence that materially reduce exposure to LLM03:2025 Supply Chain. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0028	D4-CTL-06 Shadow Ai Discovery & Governance	LLM03:2025 Supply Chain	S	Low	GAISSF D4-CTL-06 establishes AI-system controls or evidence that materially reduce exposure to LLM03:2025 Supply Chain. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0029	D4-CTL-07 Ai Software Composition Analysis (Sca)	LLM03:2025 Supply Chain	S	Low	GAISSF D4-CTL-07 establishes AI-system controls or evidence that materially reduce exposure to LLM03:2025 Supply Chain. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0030	D5-CTL-01 Harmful Content Blocking	LLM04:2025 Data and Model Poisoning	S	Low	GAISSF D5-CTL-01 establishes AI-system controls or evidence that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					detective support; it is not proof that the vulnerability is absent.	
CRO024-MAP-0031	D5-CTL-02 Pii Leakage Prevention	LLM04:2025 Data and Model Poisoning	S	Low	GAISSF D5-CTL-02 establishes AI-system controls or evidence that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0032	D5-CTL-03 Copyright Detection	LLM04:2025 Data and Model Poisoning	S	Low	GAISSF D5-CTL-03 establishes AI-system controls or evidence that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0033	D5-CTL-04 Ai Watermarking Robustness	LLM04:2025 Data and Model Poisoning	S	Low	GAISSF D5-CTL-04 establishes AI-system controls or evidence that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0034	D5-CTL-05 Privacy-By-Design Verification	LLM02:2025 Sensitive Information Disclosure	S	Low	GAISSF D5-CTL-05 establishes AI-system controls or evidence that materially reduce exposure to LLM02:2025 Sensitive Information Disclosure. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0035	D5-CTL-06 Privacy-Preserving MI Validation	LLM04:2025 Data and Model Poisoning	S	Low	GAISSF D5-CTL-06 establishes AI-system controls or evidence that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0036	D6-CTL-01 Human-In-The-Loop For High-Risk Actions	LLM06:2025 Excessive Agency	S	Low	GAISSF D6-CTL-01 establishes AI-system controls or evidence that materially reduce exposure to LLM06:2025 Excessive Agency. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0037	D6-CTL-02 Audit Trail Completeness	LLM01:2025 Prompt Injection	S	Low	GAISSF D6-CTL-02 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0038	D6-CTL-03 Ai Model Card Completeness	LLM01:2025 Prompt Injection	S	Low	GAISSF D6-CTL-03 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0039	D6-CTL-04 Ai Incident Response Readiness	LLM10:2025 Unbounded Consumption	S	Low	GAISSF D6-CTL-04 establishes AI-system controls or evidence that materially reduce exposure to LLM10:2025	Application-specific threat modelling, adversarial testing, implementation verification, and operating-

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					Unbounded Consumption. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	effectiveness evidence remain necessary.
CRO024-MAP-0040	D6-CTL-05 Model Deprecation & Decommissioning	LLM01:2025 Prompt Injection	S	Low	GAISSF D6-CTL-05 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0041	D6-CTL-06 Third-Party Ai Vendor Governance	LLM03:2025 Supply Chain	S	Low	GAISSF D6-CTL-06 establishes AI-system controls or evidence that materially reduce exposure to LLM03:2025 Supply Chain. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0042	D6-CTL-07 Ai Resilience & Business Continuity	LLM10:2025 Unbounded Consumption	S	Low	GAISSF D6-CTL-07 establishes AI-system controls or evidence that materially reduce exposure to LLM10:2025 Unbounded Consumption. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0043	D7-CTL-H01 Ai-Generated Phishing Simulation	LLM08:2025 Vector and Embedding Weaknesses	S	Low	GAISSF D7-CTL-H01 establishes AI-system controls or evidence that materially reduce exposure to LLM08:2025 Vector and Embedding Weaknesses. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0044	D7-CTL-H02 Deepfake Detection Training	LLM10:2025 Unbounded Consumption	S	Low	GAISSF D7-CTL-H02 establishes AI-system controls or evidence that materially reduce exposure to LLM10:2025 Unbounded Consumption. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0045	D7-CTL-H03 Out-Of-Band Authentication	LLM09:2025 Misinformation	S	Low	GAISSF D7-CTL-H03 establishes AI-system controls or evidence that materially reduce exposure to LLM09:2025 Misinformation. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0046	D7-CTL-H04 Ai Social Engineering Ir	LLM09:2025 Misinformation	S	Low	GAISSF D7-CTL-H04 establishes AI-system controls or evidence that materially reduce exposure to LLM09:2025 Misinformation. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0047	D7-CTL-H05 Ai-Enhanced External Attack Defense	LLM01:2025 Prompt Injection	S	Low	GAISSF D7-CTL-H05 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
CRO024-MAP-0048	D8-CTL-01 Eu Ai Act Risk Tier Mapping	LLM01:2025 Prompt Injection	S	Low	GAISSF D8-CTL-01 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0049	D8-CTL-02 Iso 42001 Gap Analysis	LLM03:2025 Supply Chain	S	Low	GAISSF D8-CTL-02 establishes AI-system controls or evidence that materially reduce exposure to LLM03:2025 Supply Chain. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0050	D8-CTL-03 Gpai Technical Documentation Verification	LLM04:2025 Data and Model Poisoning	S	Low	GAISSF D8-CTL-03 establishes AI-system controls or evidence that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0051	D8-CTL-04 Dora Ict Incident Reporting (Financial Sector)	LLM01:2025 Prompt Injection	S	Low	GAISSF D8-CTL-04 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0052	D8-CTL-05 Nist Sp 800-218A Compliance Check	LLM01:2025 Prompt Injection	S	Low	GAISSF D8-CTL-05 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0053	D9-CTL-01 Physical Harm Boundary Enforcement	LLM01:2025 Prompt Injection	S	Low	GAISSF D9-CTL-01 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0054	D9-CTL-02 Safe State And Graceful Degradation	LLM06:2025 Excessive Agency	S	Low	GAISSF D9-CTL-02 establishes AI-system controls or evidence that materially reduce exposure to LLM06:2025 Excessive Agency. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0055	D9-CTL-03 Human Override And Emergency Stop	LLM01:2025 Prompt Injection	S	Low	GAISSF D9-CTL-03 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0056	D9-CTL-04 Cyber-Physical Attack Detection	LLM01:2025 Prompt Injection	S	Low	GAISSF D9-CTL-04 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.

Record	GAISSF control	OWASP risk	Rel.	Confidence	Rationale	Residual gap
					not proof that the vulnerability is absent.	
CRO024-MAP-0057	D9-CTL-05 Physical Environment Integrity Monitoring	LLM01:2025 Prompt Injection	S	Low	GAISSF D9-CTL-05 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0058	D9-CTL-06 Actuator Command Verification	LLM01:2025 Prompt Injection	S	Low	GAISSF D9-CTL-06 establishes AI-system controls or evidence that materially reduce exposure to LLM01:2025 Prompt Injection. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.
CRO024-MAP-0059	D9-CTL-07 Physical Incident Evidence Preservation	LLM04:2025 Data and Model Poisoning	S	Low	GAISSF D9-CTL-07 establishes AI-system controls or evidence that materially reduce exposure to LLM04:2025 Data and Model Poisoning. The relationship is preventive or detective support; it is not proof that the vulnerability is absent.	Application-specific threat modelling, adversarial testing, implementation verification, and operating-effectiveness evidence remain necessary.

Annex B - Change and verification record

Item	Status
GAISSF controls inventoried	59
OWASP 2025 risks inventoried	10
Forward mappings	59
Reverse records	10
Old 2023/24 numbering mixed into baseline	No
Independent SME approval	Required before final publication