

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

GAISSF-CRO-024 — Website and Executive Summary

A practitioner crosswalk for LLM application security

GAISSF-CRO-024 assesses all 59 GAISSF™ v1.0 controls against the ten OWASP Top 10 for LLM Applications 2025 risk categories. It is edition-bound to the 2025 OWASP set and supports threat modelling, control selection, evidence-reuse analysis, and gap identification.

Document control

Document ID	GAISSF-CRO-024
Version	1.0
Status	Draft for Publication
Classification	Informative crosswalk / public
Candidate date	29 June 2026
Updated	5 October 2026
Publisher	ODA3 Institute
OWASP target	Top 10 for LLM Applications 2025

What the package contains

- 59 GAISSF control assessments against all ten OWASP 2025 risk categories.
- 59 control-assessment records: 44 positive relationships, 3 no-material relationships, and 12 outside-scope assessments.
- A complete ten-risk OWASP-to-GAISSF reverse coverage register.
- Relationship, confidence, residual-gap, source-baseline, and edition-boundary fields.
- DOCX, PDF, XLSX, Markdown, and JSON publication formats.

Key interpretation

OWASP identifies prioritized LLM application risk classes. GAISSF supplies an auditable AI control and evidence architecture. Mapping can support control selection and assurance planning, but it does not prove mitigation effectiveness, evidence sufficiency, vulnerability absence, or automatic conformance.

Edition note: this document maps the OWASP 2025 edition only. OWASP released a 2026 edition in August 2026; that edition requires separate revalidation and is not silently substituted here.

The ten OWASP 2025 risks

ID	Risk
LLM01:2025	Prompt Injection
LLM02:2025	Sensitive Information Disclosure
LLM03:2025	Supply Chain
LLM04:2025	Data and Model Poisoning
LLM05:2025	Improper Output Handling
LLM06:2025	Excessive Agency
LLM07:2025	System Prompt Leakage
LLM08:2025	Vector and Embedding Weaknesses
LLM09:2025	Misinformation
LLM10:2025	Unbounded Consumption

Appropriate uses

- AI application threat modelling
- Control selection and gap analysis
- Evidence reuse and assessment scoping

- Red-team and penetration-test planning
- Board, risk, and assurance reporting

Not established

- OWASP endorsement or certification
- Automatic GAISSE or OWASP conformance
- Evidence sufficiency or proof that vulnerabilities are absent
- A replacement for testing or secure engineering
- Regulatory compliance, equivalence, certification, or safe harbour