

**ODA3 INSTITUTE**

**Crosswalk — Website Summary**

---

# **GAISSF–OWASP LLM Top 10 Mapping**

Website & Executive Summary — Practitioner Crosswalk for LLM Application Security

DocID: CRO-024

Classification: Public

## 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 is the public Website Summary: methodology, key findings, and a representative sample of the crosswalk. The complete crosswalk register (all documented mapping relationships, confidence and rationale fields) is a Controlled Publication — request full access at <https://oda3.org/>.

|                  |                       |
|------------------|-----------------------|
| 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.***

## A practitioner crosswalk for LLM application security

CRO-024 maps the complete GAISSF v1.0 control baseline to the OWASP Top 10 for LLM Applications 2025. It helps security, governance, engineering, and assurance teams connect prioritized LLM vulnerability classes to auditable controls and evidence.

## What the package contains

- 59 GAISSF controls assessed against all ten OWASP 2025 risk categories.
- 59 documented forward mapping relationships.
- A complete OWASP-to-GAISSF reverse coverage register.
- Residual-gap, evidence, confidence, and source-baseline fields.
- DOCX, XLSX, Markdown, and JSON publication formats.

## Key interpretation

OWASP identifies high-priority vulnerability classes. GAISSF supplies an auditable control and evidence architecture. Mapping supports control selection and assurance planning, but does not prove mitigation effectiveness or vulnerability absence.

## 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 GAISSF conformance
- Proof that vulnerabilities are absent
- A replacement for testing or secure engineering
- Regulatory compliance or safe harbour