OWASP Agentic Top 10 MVG Controls Map (v1.1.1)

Procurement-friendly crosswalk: OWASP Agentic Top 10 (ASI01–ASI10) risk categories mapped to MVG mechanisms (Verify -> Permit -> Gate; fail-closed), with evidence pointers and offline verification hints.

Disposition glossary

PASS — verified; execution permitted only within declared scope/lease.	HOLD — evidence missing/ambiguous or human approval required; execution MUST NOT proceed.
FAIL — integrity mismatch or policy violation; execution blocked; incident MUST be logged.	DENY — explicitly prohibited action; execution blocked; record MUST be written.

Generated: 2026-02-26 01:17 UTC | Scope: Public, procurement-safe • Informational only; not a certification or audit opinion.
Baseline (pinned): OWASP Top 10 For Agentic Applications 2026 (Version 2026, Dec 2025, CC BY-SA 4.0).
Baseline digest (SHA-256, canonical PDF): `a2db94cd00b08e0b3a5e5b619afe024bdbcd74503111085705e4f3dd886fcb5c`

Canonical evidence entry points	`/.well-known/mvg-procurement-ticket-pack.dsse.json` | `/verify/` | `/trust-center/` | `/trust/transparency/`

Full table (CSV): `/downloads/controls-mapping/owasp_agentic_mvg_map_v1_1_1.csv` • Metadata (JSON): `/downloads/controls-mapping/owasp_agentic_mvg_map_v1_1_1.meta.json`

Signed, content-addressed mapping: `controls-mapping.csv` + `meta.json` are content-addressed and DSSE-signed; any divergence from the canonical Trust Index triggers HOLD/FAIL.

Legend

Evidence IDs: Each row MUST include ≥1 row-specific Evidence ID that resolves to a replayable receipt/test vector; shared entry points alone are insufficient.

Primary/Complementary/Partial describe control coverage level; MVG/CUST/SHARED describe operational responsibility boundaries (integration, runtime enforcement, policy ownership).

Responsibility tags: MVG (provided by MVG), CUST (customer-owned), SHARED (joint). Coverage labels are abbreviated to prevent line-break artifacts: Primary | Complement. | Partial. "Partial" indicates MVG supplies audit/receipt rails while enforcement scope may be customer-configured.

Offline verify: (1) download Evidence Pack + SHA256SUMS, (2) verify DSSE signature bundle, (3) verify pointers/hashes match the Trust Index. Offline verify requires matching Trust Index pointers/hashes; any mismatch or missing artifact -> HOLD/FAIL and execution MUST NOT proceed.

Canonical DSSE signature bundle: `/.well-known/mvg/controls-map/v1.1.1/dsse.json` (exact path; no placeholders)

Controls map: ASI01–ASI05

Table legend: Evidence IDs are row-specific; responsibility tags: MVG / CUST / SHARED.

OWASP Category	MVG mechanism	Evidence & offline verify (hint)	Coverage
ASI01 Agent Goal Hijack	Permit (signed intent capsule) + Gate (drift guard; fail-closed)	Evidence: /verify/ | /.well-known/mvg-procurement-ticket-pack.dsse.json | /trust/transparency/ Verify: run the offline verifier; missing/invalid intent binding or pointers HOLD. Evidence ID: EVID-ASI01-INTENTCAPSULE-0001	**Primary** MVG
ASI02 Tool Misuse & Exploitation	Permit (policy-enforced tool call) Gate (PEP/PDP; schema + TTL; fail-closed)	Evidence: /verify/ | /.well-known/mvg-procurement-ticket-pack.dsse.json | /trust/transparency/ Verify: tool/egress actions require permits; missing permits/signatures HOLD. Evidence ID: EVID-ASI02-TOOLGATE-0007	**Primary** MVG
ASI03 Identity & Privilege Abuse	Permit (task-scoped authority) + Gate (privileged action boundary) + Govern (stop authority)	Evidence: /trust-center/ | /.well-known/mvg-governance.json | /verify/ Verify: confirm scope authority + fail-closed outcomes; missing governance receipts HOLD. Note: IAM integration is program-owned. Evidence ID: EVID-ASI03-AUTHBOUNDARY-0003	**Complement.** SHARED
ASI04 Agentic Supply Chain Vulnerabilities	Verify (pinned artifacts + signed publication chain) + FAIL/HOLD semantics	Evidence: /trust/site-release/ | /trust/transparency/ Verify: verify signed release manifests + pinned hashes offline; mismatches FAIL; missing signatures HOLD. Evidence ID: EVID-ASI04-RELEASEMANIFEST-0012	**Primary** MVG
ASI05 Unexpected Code Execution (RCE)	Gate (high-risk execution/egress boundary) + Receipts (non-repudiation); fail-closed	Evidence: /verify/ | /safety/incident-response/ Verify: MVG proves gating/receipts; execution sandboxing is typically provided by your runtime. Missing evidence HOLD. Evidence ID: EVID-ASI05-RCEGATE-0004	**Complement.** SHARED

Offline verify: (1) download Evidence Pack + SHA256SUMS, (2) verify DSSE signature bundle, (3) verify pointers/hashes match the Trust Index. Offline verify requires matching Trust Index pointers/hashes; any mismatch or missing artifact -> HOLD/FAIL and execution MUST NOT proceed.

Canonical DSSE signature bundle: `/.well-known/mvg/controls-map/v1.1.1/dsse.json` (exact path; no placeholders)

Controls map (continued): ASI06–ASI10

Table legend: Evidence IDs are row-specific; responsibility tags: MVG / CUST / SHARED.

OWASP Category	MVG mechanism	Evidence & offline verify (hint)	Coverage
ASI06 Memory & Context Poisoning	Verify (provenance + pinning) + Gate (memory/RAG policy; fail-closed on untrusted context)	Evidence: /verify/ | /aims/ | /trust/transparency/ Verify: confirm provenance requirements and HOLD semantics for untrusted context; storage-layer controls are program-specific. Evidence ID: EVID-ASI06-RAGPOLICY-0009	**Partial** CUST
ASI07 Insecure Inter-Agent Communication	Verify (message binding receipts: hash/nonce) + Gate (dispatch boundary); fail-closed	Evidence: /verify/ | /trust/transparency/ Verify: inter-agent calls can be receipted and replay-checked; transport security (mTLS/E2E) is typically infra-owned. Evidence ID: EVID-ASI07-MSGRECEIPT-0006	**Complement.** SHARED
ASI08 Cascading Failures	Govern + Gate (blast-radius guardrails; HOLD-first) + Receipts (deterministic reason codes)	Evidence: /safety/incident-response/ | /.well-known/mvg-safety-ir.json | /verify/ Verify: confirm stop/HOLD triggers + replayable decision trail; missing IR receipts HOLD. Note: reliability controls are program-owned; MVG provides fail-closed semantics + receipts. Evidence ID: EVID-ASI08-HOLDFIRST-0011	**Primary** SHARED
ASI09 Human-Agent Trust Exploitation	Verify (provenance receipts) + Gate (preview ≠ effect; signature required)	Evidence: /verify/ | /trust/transparency/ | /trust-center/ Verify: require signed provenance before side effects; unverifiable recommendations HOLD. Evidence ID: EVID-ASI09-PROVENANCE-0008	**Primary** MVG
ASI10 Rogue Agents	Govern (revocation / kill-switch) + Verify (identity receipts) + Gate (no permit, no action)	Evidence: /safety/incident-response/ | /governance/ | /verify/ Verify: confirm revocation/stop authority and fail-closed gating; missing receipts HOLD. Note: detection/containment is program-owned; MVG provides revocation authority + gating. Evidence ID: EVID-ASI10-KILLSWITCH-0005	**Primary** SHARED

Offline verify: (1) download Evidence Pack + SHA256SUMS, (2) verify DSSE signature bundle, (3) verify pointers/hashes match the Trust Index. Offline verify requires matching Trust Index pointers/hashes; any mismatch or missing artifact -> HOLD/FAIL and execution MUST NOT proceed.

Canonical DSSE signature bundle: `/.well-known/mvg/controls-map/v1.1.1/dsse.json` (exact path; no placeholders)