

ODA3 INSTITUTE

EXECUTIVE BRIEF

GAISSF™ Defence Sector Executive Brief

Global AI Safety and Security Framework

Document ID: GAISSF-SEC-040

Version: 1.0

Status: Draft for Publication — Public — External Review Open

Issued: 29 June 2026

Updated: 5 October 2026

© 2026 ODA3 Pvt Ltd

Decision Context

Defence AI changes operational risk through speed, scale, opacity, supplier dependency and reduced intervention time. The governance question is whether the complete system remains within approved authority under realistic mission, adversarial and degraded conditions.

Applicable-Control Baseline

GAISSF v1.0 contains 59 controls across nine domains. The canonical Foundational scope is 52 controls in D1-D8. D9 contains seven additional/conditional controls and applies where Physical AI or cyber-physical actuation is in scope. Operational and Optimized use the same applicable control scope with stronger evidence and assurance expectations.

Physical AI Boundary

Where Physical AI or cyber-physical actuation is in scope, use GAISSF D9 alongside PAI-SF™ v1.0 as applicable. CSX-PAISF-004 provides mapping only; it does not establish equivalence, evidence sufficiency or automatic conformance.

Five Governance Decisions Required Before Deployment

1. Approve intended and prohibited uses and authority boundaries.
2. Name accountable system, mission, security, safety, acquisition and suspension/abort authorities.
3. Require mission-representative evidence rather than supplier assertions or generic benchmarks.
4. Approve fallback, downgrade and suspension conditions before operational use.
5. Maintain reauthorisation triggers for material mission, model, data, supplier, environment or autonomy changes.

Supplier Assurance

Do not accept a “certified model” as a substitute for programme testing. Require evidence rights, representative test access, update/change notice, incident notification, supportability, continuity, rollback and exit provisions. GAISSF certification is not currently offered; any future scheme would be separately governed.

Public / Classified Information Boundary

This public brief must not contain or store classified operational data, mission parameters, target information or controlled technical data. Those records belong only in approved environments.

Notably Absent

This brief does not establish legal, IHL, regulatory or export-control compliance; provide rules of engagement; authorise weapons employment; establish universal acceptance thresholds; or claim that testing, logging, certification or human presence eliminates operational risk.

Publication Status

Draft for Publication — Public — External Review Open. Defence technical, cybersecurity/adversarial-ML, systems-safety, human-factors, operational T&E, autonomy, legal/IHL, national-law/export-control, classified-information-handling and final publication approvals remain open unless separately evidenced.

Exposure	Executive question
Operational continuity	What is the tested fallback and who can invoke it?
Human and safety	Is human authority effective within the intervention window?
Security and sovereignty	Which critical capabilities can be independently operated, tested and exited?
Legal and policy	Which decisions require qualified legal, IHL, safety or command review?
Programme and financial	Are evidence and exit rights contractually enforceable?