GAISSF® v1.0

Defence Sector Executive Brief

SEC-040 | Version 1.0 | Board, executive and risk-committee briefing

PUBLICATION GATE: OPEN - CONTROLLED PRE-RELEASE DRAFT FOR PEER REVIEW

Methodology Note: This brief synthesises the technical guide and official contextual sources for governance decision-making. It contains no inline evidence-tier tags. Detailed source verification, control mapping and limitations are maintained in the Technical Guide, Source Register and Workbook.

Decision Context

Defence AI changes operational risk through speed, scale, opacity, supplier dependency and reduced intervention time. The principal governance question is not whether a model is accurate in isolation, but whether the complete system remains within approved authority under realistic mission, adversarial and degraded conditions.

Board and Executive Exposure

Exposure	What can go wrong	Executive question
Operational continuity	Model, API, sensor or supplier failure disrupts mission support	What is the tested fallback and who can invoke it?
Human and safety	Automation bias or unsafe actuation causes harm	Is human authority effective within the intervention window?
Security and sovereignty	Models, data or dependencies are compromised or externally controlled	Which critical capabilities can be independently operated, tested and exited?
Legal and policy	Use exceeds approved purpose or applicable authority	Which decisions require qualified legal, IHL, safety or command review?
Programme and financial	Rework, failed acceptance, lock-in and sustainment cost	Are evidence and exit rights contractually enforceable?

Five Governance Decisions Required Before Deployment

- Approve the intended and prohibited uses, including explicit authority boundaries.
- Name the System Authority, Mission Owner, Security Authority, Safety Authority, Acquisition Authority and suspension/abort authority.
- Require mission-representative evidence rather than supplier claims or generic benchmarks.
- Approve fallback, downgrade and suspension conditions before operational use.
- Maintain reauthorisation triggers for material changes to mission, model, data, supplier, environment or autonomy.

Supplier Assurance: What the Board Should Not Accept

Do not accept	Require instead
“Certified model” as a substitute for programme testing	Independent access to representative testing, limitations and residual risk
Opaque automatic updates	Material-change notice, version pinning, regression evidence and rollback
Generic provenance claims	Versioned model, data, adapter, dependency and custody records
No practical exit route	Export, deletion, continuity, replacement and dependency-removal plan

Financial and Programme Control

The strongest financial controls are preventive: evidence rights before contract signature, staged acceptance, testable performance obligations, update/change clauses, incident notification, supportability, continuity and exit. Uncontrolled model changes and hidden dependencies convert technical uncertainty into programme delay and rework.

Operational Assurance Model

Stage	Executive evidence
Scope and classification	Approved mission context, consequence profile and authority state
Acquisition	Supplier evidence schedule, test rights, update and exit clauses
Acceptance	Independent security, safety, human-factor and operational test results
Deployment	Approved baseline, fallback, monitoring and suspension thresholds
Operation	Trend, incident, override, change and residual-risk reports
Retirement	Dependency removal, record preservation and data/model disposal

Escalation and Downgrade

A system should be downgraded to a lower-risk role or suspended when evidence becomes stale, a material supplier or mission change occurs, monitoring crosses an approved threshold, or control effectiveness cannot be demonstrated. Authority to downgrade must be named in advance; it should not depend on ad hoc programme negotiation during an incident.

Notably Absent

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

Publication Status

Controlled pre-release candidate. Defence technical, cybersecurity, safety, human-factors, operational T&E, autonomy, legal/IHL, export-control, classified-handling and final publication approvals remain open. IHL review is planned before full publication; findings will be incorporated or documented as limitations.