

SEC-051 - GAISSE Automotive Executive Brief

Leadership Brief

Document ID	SEC-051
Status	Publication Candidate - Open Review Gates
Version	1.0
Edition date	1 July 2026

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute.

Methodology Note: This brief translates 59 authoritative GAISSF controls into automotive decision contexts. The authoritative control baseline is [T1]; automotive risk interpretation and illustrative scenarios are analytical [T3]. The brief does not rely on proprietary vehicle telemetry, client data, or internal incident datasets. Detailed evidence tiers appear in the technical report.

1. Why this matters to leadership

Automotive AI can create compounding exposure across product liability, warranty and recall cost, type-approval schedules, supplier disputes, service availability, customer trust, and regulatory scrutiny. The central governance question is not merely whether a model performs; it is whether the organisation can prove who authorised it, what changed, which assumptions remain valid, how fleet-wide effects will be detected, and when release or continued operation must stop.

Leadership should treat AI assurance as part of release authority. AI security must be coordinated with vehicle cybersecurity, functional safety, Safety of the Intended Functionality (SOTIF), product safety, privacy, software assurance, and legal obligations.

2. Where risk concentrates

Risk increases where systems can influence vehicle behaviour, safety-relevant engineering decisions, remote functions, connected services, software or model release, fleet-wide configuration, sensitive driver or occupant data, or supplier-controlled components.

Priority concentration points include model and data provenance; common-mode fleet failure; supplier evidence; signed Over-the-Air (OTA) updates; backend and credential compromise; insufficient monitoring; weak fallback; and engineering assistants with excessive authority.

3. Decisions leadership must make

1. Which AI-enabled systems fall within governed release authority?
2. Which systems can cause human, safety, legal, strategic, or fleet-scale consequence?
3. Who owns residual risk where cybersecurity and safety assumptions conflict?
4. What evidence is mandatory before release, update, or continued operation?
5. Which suppliers must provide provenance, security, change, incident, and end-of-life evidence?
6. What conditions trigger deployment suspension, rollback, field action, or recall assessment?
7. Which independent specialist reviews are required before public assurance claims?

4. 90-day action sequence

Days 0-30: establish accountable governance; inventory systems and dependencies; classify authority and consequence; identify critical suppliers; open evidence repositories and specialist review gates.

Days 31-60: complete priority control mappings; conduct integrated AI-security, cybersecurity, safety, privacy, and supplier analysis; verify model and data provenance; define monitoring, incident, and OTA controls.

Days 61-90: test operating effectiveness; execute representative scenarios; validate escalation and rollback; close critical evidence gaps; document residual risk; conduct independent readiness review.

5. Evidence boundaries and Notably Absent

This package provides an operational implementation layer and evidence model. It does not establish legal compliance, homologation, type approval, functional-safety or SOTIF approval, cybersecurity approval, accredited certification, or prevention of harm.

Notably absent are proprietary fleet telemetry, client incident data, confirmed field exploitation claims for illustrative scenarios, regulator-endorsed crosswalks, completed specialist reviews, and independent field validation.

6. Current release decision

The package is suitable for structured specialist review. It is not approved for final publication while 16 review gates remain open, including automotive cybersecurity, functional safety, SOTIF, legal and regulatory, homologation and type approval, privacy, accessibility, technical editing, and final publication approval.