

ODA3 INSTITUTE

EXECUTIVE BRIEF

GAISSF™ Retail Sector Executive Brief

Leadership decisions for retail AI security and assurance

GAISSF-SEC-046 | Public | Draft for Publication — External Review Open

Issued 1 July 2026 | Updated 5 October 2026

© 2026 ODA3 Pvt Ltd

Methodology Note

This brief summarises the GAISSF-SEC-046 technical report and the authoritative GAISSF™ - Global AI Safety and Security Framework v1.0 baseline. The Applicable-Control Baseline is all 52 D1-D8 controls plus D9 where Physical AI or cyber-physical actuation is in scope. Where D9 applies, use GAISSF D9 alongside PAI-SF™ v1.0 as applicable; CSX-PAISF-004 is mapping only. The brief uses no proprietary retailer telemetry and makes no sector-wide frequency, loss, compliance, evidence-sufficiency, conformance or certification claim. GAISSF certification is not currently offered.

Why integrated retail AI assurance is required

Retail AI can influence prices, promotions, payment and fraud decisions, product information, customer access, worker outcomes and physical store or warehouse operations. Governance must therefore connect AI security with cybersecurity, privacy, payment security, consumer protection, employment, accessibility, resilience and supplier management. No single discipline proves the others.

Where risk concentrates

- Systems with authority to deny payment, block accounts, reject returns, identify people, affect employment or control physical equipment.
- High-volume systems whose small error rates aggregate into widespread customer, worker or financial impact.
- Third-party models and APIs that can change behaviour, data use or availability without retailer control.
- Distributed store, franchise, marketplace and edge environments where evidence and enforcement are inconsistent.
- Generative and agentic systems that can disclose data, create misleading content or invoke business actions.

Decisions leadership must make

- Who can approve, constrain, suspend or retire each high-impact AI system?
- What evidence is mandatory before deployment and after material change?
- Which supplier evidence, notification, data-use and exit rights are non-negotiable?
- What customer, worker and operational outcomes trigger escalation?
- Which uses require legal, privacy, payment, biometric, employment or accessibility review?
- Which claims are prohibited until independent review closes the open gates?

180-day implementation sequence

Window	Leadership outcome
Days 0-30	Approve governance, inventory, scope, owners, suppliers and criticality.
Days 31-60	Approve Applicable-Control Baseline, risk priorities, threat analysis and remediation funding.
Days 61-120	Implement controls, supplier clauses, testing, monitoring, fallback and incident capability.
Days 121-180	Review evidence, close high-risk gaps, conduct independent readiness review and accept residual risk.

Evidence boundaries and Notably Absent

The package maps all 59 Global AI Safety and Security Framework (GAISSF) controls and provides retail use cases, threats, evidence, metrics, scenarios and readiness materials. It does not establish legal compliance, Payment Card Industry Data Security Standard compliance, biometric legality, employment-law compliance, accredited certification or prevention of harm. Retail-specific performance and incident prevalence were not independently measured.