

GAISSF Retail Sector Implementation Guide - Technical Report

Operational interpretation, evidence and assessment package

SEC-046 | Version 1.0 | Publication Candidate - Open Review Gates | 1 July 2026

Field	Value
Document ID	SEC-046
Version	1.0
Classification	Informative sector implementation guidance
Status	Publication Candidate - Open Review Gates
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
Authoritative source	GAISSF-NOR-001 v1.0, Corrected Final Publication Edition
Control baseline	59 controls across nine domains
Publication channel	ODA3 Institute website and GitHub

Table of Contents

Contents: Executive overview; Start Here; Methodology; 1 Scope; 2 Retail context; 3 AI taxonomy; 4 Threat landscape; 5 Control profiles; 6 Complete control interpretation; 7 Data governance; 8 Supply chain; 9 Lifecycle; 10 Testing; 11 Human oversight; 12 Consumer protection; 13 Metrics; 14 Incident management; 15 Roles; 16 Roadmap; 17 Evidence; 18 Maturity; 19 Failures; 20 Scenarios; 21 Crosswalk; 22 Notably Absent; 23 Limitations; Appendices A-F.

Copyright, licence and reliance notice

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute. Use, reproduction, adaptation, certification, credential and trademark rights are governed by the applicable GAISSF publication terms and licensing instruments.

This guide is informative. It does not create or modify GAISSF requirements, constitute legal advice, guarantee security or safety, establish payment-card compliance, authorise biometric processing, or provide accredited certification.

How to use this guide

Use this guide to scope retail AI systems, interpret the authoritative GAISSF controls, prioritise implementation, collect evidence and prepare for internal or independent assessment. GAISSF-NOR-001 remains authoritative where wording differs.

Evidence tiers

Tier	Meaning
T1	Primary authoritative evidence: legislation, regulation, official standards and government or regulator material.
T2	Strong secondary evidence: peer-reviewed research, recognised industry bodies and independently verified technical research.
T3	Contextual evidence: vendor disclosures, credible reporting, practitioner case studies and limited datasets.
T4	Illustrative material: hypothetical scenarios and implementation examples; not evidence of prevalence.

Executive overview

Retail AI operates across customer-facing digital services, payment and fraud systems, distributed stores, warehouses, workforce systems, marketplaces and supplier platforms. The practical risk is not simply model accuracy. It is whether AI behaviour, data use, tool access, model changes, human escalation and fallback remain controlled across a fragmented operating environment.

- Highest-consequence profiles commonly include payment and fraud decisions, biometric identification, hiring, autonomous stores and warehouse robotics.
- High-volume moderate-consequence systems can still create material aggregate harm through pricing errors, misleading product content, discriminatory targeting or uncontrolled provider changes.
- Assurance requires operating evidence: approved scope, tested safeguards, monitoring, exceptions, incident records and supplier evidence rights.
- This package does not claim that one control set proves legal compliance, payment compliance, employment-law compliance, biometric legality or consumer-protection compliance.

1. Inventory every production and pilot AI system, including embedded software-as-a-service, franchise and store-edge deployments.
2. Approve accountable owners and a 59-control Statement of Applicability.
3. Implement the P1 controls first: data provenance, drift, prompt/tool boundaries, supplier governance, personal-data protection, human review, complete audit trails, incident readiness and continuity.
4. Apply D9 only where physical AI is in scope; apply biometric, workforce and other high-impact safeguards when the use-case trigger exists.
5. Collect operating evidence before describing a control as implemented.

Start Here - first implementation decisions

Analysis of public disclosures and authoritative standards informs the external context [T1-T2]. Peer-reviewed and technical research supports demonstrated attack classes [T2], while practitioner patterns and illustrative scenarios are contextual [T3-T4]. No proprietary retailer telemetry or internal incident dataset was used. Threat frequency and loss magnitude are not inferred where public evidence is insufficient.

Methodology and evidence boundary

1. Scope and normative boundary

The guide applies to retailers, marketplaces, direct-to-consumer businesses, franchise systems, fulfilment operations and retail technology functions that develop, acquire, integrate, deploy, operate, monitor or retire AI systems. It covers internally developed systems, commercial AI, embedded AI, generative AI, agentic systems, computer vision, predictive models and physical AI.

GAISSF conformance scope remains authoritative: D1-D8 are the 52-control canonical Foundational scope; D9 contains seven additional controls that apply where physical AI is in scope. The P1/P2/P3 labels in this guide are implementation sequencing aids only and do not change normative applicability.

SHALL and SHALL NOT are used only when reproducing or referring to authoritative GAISSF requirements. Sector guidance uses should, may and can. A contractual or certification instrument may separately make defined guidance mandatory.

2. Retail operating context

- High transaction and customer-data volumes with low-latency availability requirements.
- Distributed store, edge, warehouse, mobile and cloud infrastructure, often combined with legacy systems.
- Substantial dependence on payment processors, e-commerce platforms, fraud vendors, customer-data platforms, logistics providers and foundation-model services.
- Seasonal demand shifts, promotion spikes, workforce turnover and franchise variation that can degrade controls or model performance.
- Direct consumer and worker impacts from pricing, fraud, biometric, recommendation, scheduling and hiring systems.

3. Retail AI system taxonomy

ID	Use case	Business area	Data	Authority	Criticality	Oversight
RET-UC-001	Personalised recommendations	Customer experience	Customer account, browsing, transaction and catalogue data	Decision support	Moderate	Risk-based review and escalation
RET-UC-002	Product search and ranking	E-commerce	Queries, clicks, catalogue and availability	Decision support	Moderate	Risk-based review and escalation
RET-UC-003	Dynamic pricing	Merchandising	Demand, inventory, competitor and customer context	Automated decision	High	Mandatory pre- or post-decision review
RET-UC-004	Promotion optimisation	Marketing	Campaign, customer, basket and margin data	Automated decision	Moderate	Risk-based review and escalation
RET-UC-005	Demand forecasting	Supply chain	Sales, seasonality, weather and events	Decision support	Moderate	Risk-based review and escalation
RET-UC-006	Inventory allocation	Supply chain	Stock, sales, lead time and store data	Automated decision	Moderate	Risk-based review and escalation
RET-UC-007	Automated replenishment	Store operations	Inventory, sales and supplier feeds	Automated action	Moderate	Risk-based review and escalation

SEC-046 | GAISSF Retail Sector Implementation Guide | v1.0 | Publication Candidate

ID	Use case	Business area	Data	Authority	Criticality	Oversight
RET-UC-008	Warehouse robotics	Fulfilment	Sensor, order and route data	Physical AI	Critical	Mandatory pre- or post-decision review
RET-UC-009	Route and delivery optimisation	Logistics	Address, location, capacity and traffic	Decision support	Moderate	Risk-based review and escalation
RET-UC-010	Self-checkout vision	Store operations	Video, item and payment events	Decision support	High	Mandatory pre- or post-decision review
RET-UC-011	Computer-vision loss prevention	Loss prevention	Video, behavioural and transaction signals	High-impact alerting	High	Mandatory pre- or post-decision review
RET-UC-012	Fraud detection	Payments and fraud	Payment, device, identity and transaction data	Automated decision	Critical	Mandatory pre- or post-decision review
RET-UC-013	Payment-risk scoring	Payments and fraud	Payment, identity and behavioural signals	High-impact decision	Critical	Mandatory pre- or post-decision review
RET-UC-014	Customer-service chatbot	Customer service	Conversation, account and product data	Conversational assistance	Moderate	Risk-based review and escalation
RET-UC-015	Generative product descriptions	Content operations	Catalogue, supplier and brand data	Content generation	Moderate	Risk-based review and escalation
RET-UC-016	Marketing-content generation	Marketing	Campaign, brand and audience data	Content generation	Moderate	Risk-based review and escalation
RET-UC-017	Customer segmentation	Marketing analytics	Demographic, behavioural and transaction data	Profiling	Moderate	Risk-based review and escalation
RET-UC-018	Loyalty analytics	Loyalty operations	Identity, purchases, rewards and location	Profiling	Moderate	Risk-based review and escalation
RET-UC-019	Retail media targeting	Retail media	Audience, purchase and browsing data	Automated targeting	Moderate	Risk-based review and escalation
RET-UC-020	Facial recognition	Store security	Biometric templates and video	Identification	Critical	Mandatory pre- or post-decision review
RET-UC-021	Age estimation	Restricted sales	Facial image or video	Decision support	High	Mandatory pre- or post-decision review
RET-UC-022	Workforce scheduling	Human resources	Availability, performance and demand	Employment decision support	Moderate	Risk-based review and escalation
RET-UC-023	Employee productivity monitoring	Human resources	Activity, location and performance data	Monitoring	Moderate	Risk-based review and escalation
RET-UC-024	Hiring and screening	Human resources	Applications, assessments and interviews	High-impact decision	Critical	Mandatory pre- or post-decision review
RET-UC-025	Returns-abuse detection	Returns and fraud	Returns, identity, transaction and device data	Automated decision	High	Mandatory pre- or post-decision review
RET-UC-026	Counterfeit detection	Marketplace integrity	Images, listings, seller and provenance data	Decision support	Moderate	Risk-based review and escalation
RET-UC-027	Visual search and virtual try-on	Customer experience	Images, body or facial features and catalogue	Interactive assistance	Moderate	Risk-based review and escalation
RET-UC-028	Smart shelves and store analytics	Store operations	Sensor, shelf, video and inventory data	Edge analytics	Moderate	Risk-based review and escalation
RET-UC-029	Autonomous store systems	Store operations	Video, sensor, identity and transaction data	Autonomous system	Critical	Mandatory pre- or post-decision review
RET-UC-030	Developer copilots and code generation	Retail technology	Source code, prompts, repositories and tickets	Engineering assistance	Moderate	Risk-based review and escalation

ID	Use case	Business area	Data	Authority	Criticality	Oversight
RET-UC-031	Third-party foundation-model API	Enterprise AI	Prompts, retrieval data and generated outputs	External dependency	Moderate	Risk-based review and escalation
RET-UC-032	Synthetic retail data generation	Data science	Production distributions and schemas	Data generation	Moderate	Risk-based review and escalation

4. Retail threat and failure landscape

Analysis of public disclosures supports several demonstrated AI attack classes [T2], while retail-specific frequency and loss data remain incomplete. Academic and technical simulations support plausible attack paths [T3]. The register below separates demonstrated classes from contextual sector exposures [T2-T3].

ID	Threat or failure	Actor/source	Pathway	Evidence	Uncertainty
RET-THR-001	Training-data poisoning	Malicious supplier, insider or external attacker	Corrupts model behaviour through manipulated data	T2 demonstrated/observed class	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-002	Retrieval poisoning	Seller, advertiser or content attacker	Injects misleading catalogue or knowledge-base content	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-003	Prompt injection	Customer, attacker or compromised content source	Overrides intended chatbot or agent instructions	T2 demonstrated/observed class	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-004	Indirect prompt injection	Compromised webpage, email, review or document	Triggers hidden instructions through retrieved content	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-005	Model extraction	Competitor or cybercriminal	Steals model behaviour through systematic querying	T2 demonstrated/observed class	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-006	Membership or data inference	External attacker	Infers sensitive customer or training-set information	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-007	API credential theft	Cybercriminal or insider	Obtains privileged access to model or platform APIs	T2 demonstrated/observed class	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-008	Agent tool abuse	Customer, insider or attacker	Causes agent to invoke refunds, promotions or account actions	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-009	Inter-agent trust failure	Compromised autonomous component	Propagates untrusted instructions across agents	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-010	Uncontrolled model update	Provider or change-management failure	Changes behaviour without retailer approval or validation	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-011	Vendor outage or	Third-party provider	Removes critical AI	T3 plausible sector	Retail prevalence and

ID	Threat or failure	Actor/source	Pathway	Evidence	Uncertainty
	withdrawal		service or support	exposure	loss data are incomplete; validate against internal telemetry.
RET-THR-012	Supplier data reuse	Third-party provider	Uses retailer data for training beyond agreed purpose	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-013	Synthetic identity fraud	Fraud ring	Uses generated identities and documents to open accounts	T2 demonstrated/observed class	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-014	Loyalty-account takeover	Cybercriminal	Steals rewards, profile data or payment instruments	T2 demonstrated/observed class	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-015	Promotion and coupon abuse	Fraud ring or malicious customer	Optimises exploitation of promotion logic	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-016	Returns fraud adaptation	Fraud ring	Learns thresholds and evades returns-abuse models	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-017	Pricing manipulation	Competitor, scraper or compromised input	Influences dynamic pricing through false signals	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-018	Inventory forecast manipulation	Supplier, insider or attacker	Creates shortage, overstock or allocation distortion	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-019	Recommendation manipulation	Seller, advertiser or bot network	Improves ranking through adversarial engagement	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-020	Hallucinated product claims	Model or workflow failure	Generates false specifications, compatibility or safety information	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-021	Deceptive synthetic reviews	Seller or content generator	Creates misleading consumer endorsements	T2 demonstrated/observed class	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-022	Biometric false match	Model limitations or poor conditions	Misidentifies a customer or worker	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-023	Age-estimation error	Model limitations or demographic disparity	Incorrectly permits or denies restricted sale	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-024	Loss-prevention false positive	Model limitations or biased data	Triggers unjustified intervention	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-025	Discriminatory	Design or data bias	Produces unequal	T3 plausible sector	Retail prevalence and

ID	Threat or failure	Actor/source	Pathway	Evidence	Uncertainty
	segmentation		targeting, service or offers	exposure	loss data are incomplete; validate against internal telemetry.
RET-THR-026	Employment decision bias	Design or data bias	Unfairly affects hiring, scheduling or performance outcomes	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-027	Edge-device tampering	Physical attacker or insider	Manipulates cameras, sensors or smart shelves	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-028	Warehouse command manipulation	Cyber-physical attacker	Issues unsafe or unauthorised robotic actions	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-029	Catalogue corruption	Supplier, seller or integration failure	Propagates incorrect attributes and product information	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-030	Insufficient audit logging	Design or operational failure	Prevents reconstruction, challenge or accountability	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-031	Model drift	Changing demand or environment	Degrades performance after deployment	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-032	Seasonal distribution shift	Demand volatility	Causes forecast and fraud models to misperform	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-033	Generated phishing	Cybercriminal	Scales targeted attacks against retail workers and suppliers	T2 demonstrated/observed class	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-034	Deepfake executive or supplier fraud	Fraudster	Impersonates authorised persons to change payments or orders	T2 demonstrated/observed class	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-035	Sensitive prompt leakage	Employee or system error	Exposes customer, supplier or source-code data	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.
RET-THR-036	Open-source model compromise	Supply-chain attacker	Introduces malicious or vulnerable model artefact	T3 plausible sector exposure	Retail prevalence and loss data are incomplete; validate against internal telemetry.

5. Risk-based retail control profiles

E-commerce and customer interaction

- Recommendations, search, chatbots, product content, visual search and account services require output validation, prompt-injection controls, customer escalation and change monitoring.

Payments, fraud and loyalty

- Fraud, payment-risk, returns and loyalty decisions require low-latency controls without removing contestability, evidence retention, fraud monitoring and fallback.

Stores, computer vision and biometrics

- Store analytics, loss prevention, facial recognition and age estimation require physical-environment testing, privacy and legal review, false-match monitoring and controlled intervention.

Supply chain, warehouse and physical AI

- Forecasting, replenishment, robotics and autonomous store systems require safe state, command validation, environmental integrity, business continuity and evidence preservation.

Workforce AI

- Hiring, scheduling and productivity monitoring require documented purpose, impact assessment, human review, appeal routes, access restriction and worker transparency.

Generative and agentic AI

- Generative content, developer copilots and agents require tool-boundary controls, retrieval security, output validation, supplier governance, logging and rollback.

6. Complete GAISSE retail control interpretation

The following records preserve authoritative GAISSE identifiers and titles [T1]. Retail interpretations are practitioner guidance based on public evidence and operational analysis [T3]; they are not prevalence claims or substitutes for system-specific testing.

D1-CTL-01 - DATASET PROVENANCE & POISONING PREVENTION

Field	Retail implementation record
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative requirement	Refer to GAISSE-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Retail training, tuning and evaluation data often arrive from point-of-sale feeds, loyalty platforms, sellers, suppliers and franchise locations. Preserve source lineage, quarantine abnormal submissions and require approval before contaminated catalogue, fraud or demand data can influence a production model. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-001; RET-UC-008; RET-UC-015
Related threats	RET-THR-001; RET-THR-006; RET-THR-011
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.

Field	Retail implementation record
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-001; RET-EVD-004
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-001; RET-MET-008
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D1-CTL-02 - MODEL EXTRACTION RESISTANCE

Field	Retail implementation record
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Recommendation, pricing and fraud APIs can expose commercially valuable decision logic through high-volume queries. Apply rate limits, behavioural detection, response minimisation and contractual controls to make systematic model replication detectable and costly. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-002; RET-UC-009; RET-UC-016; RET-UC-023
Related threats	RET-THR-002; RET-THR-007; RET-THR-012; RET-THR-017
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-002; RET-EVD-005; RET-EVD-008
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-002; RET-MET-009
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D1-CTL-03 - BEHAVIORAL DRIFT DETECTION

Field	Retail implementation record
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Retail behaviour changes sharply during promotions, holidays, product launches and fraud campaigns. Monitor performance by channel, store cohort and affected population so seasonal change is distinguished from security manipulation or silent model degradation. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-003; RET-UC-010; RET-UC-017; RET-UC-024; RET-UC-031
Related threats	RET-THR-003; RET-THR-008; RET-THR-013
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-003; RET-EVD-006; RET-EVD-009; RET-EVD-012
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-003; RET-MET-010
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D1-CTL-04 - FEDERATED LEARNING POISONING PREVENTION

Field	Retail implementation record
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Where stores, franchisees or regional entities train locally, validate and bound each submitted update before aggregation. A compromised edge node must not be able to poison group-wide fraud, forecasting or recommendation behaviour. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-004; RET-UC-011; RET-UC-018
Related threats	RET-THR-004; RET-THR-009; RET-THR-014; RET-THR-019
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and

Field	Retail implementation record
	operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-004; RET-EVD-007
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-004; RET-MET-011
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D1-CTL-05 - EMBEDDING SPACE ROBUSTNESS

Field	Retail implementation record
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Product search, visual search and retrieval systems depend on embedding similarity. Test whether adversarial images, seller text or catalogue attributes can move prohibited, counterfeit or irrelevant items into trusted result neighbourhoods. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-005; RET-UC-012; RET-UC-019; RET-UC-026
Related threats	RET-THR-005; RET-THR-010; RET-THR-015
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-005; RET-EVD-008; RET-EVD-011
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-005; RET-MET-012
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific

Field	Retail implementation record
Scope label	Foundational - canonical D1-D8 scope

D1-CTL-06 - POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING

Field	Retail implementation record
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Long-lived model artefacts, signed releases and warehouse or store-edge devices may outlive current cryptographic assumptions. Maintain crypto-agility and migration plans; do not represent post-quantum readiness as achieved unless the full signing and verification chain has been tested. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-006; RET-UC-013; RET-UC-020; RET-UC-027; RET-UC-002
Related threats	RET-THR-006; RET-THR-011; RET-THR-016; RET-THR-021
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-006; RET-EVD-009; RET-EVD-012; RET-EVD-015
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-006; RET-MET-013
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D1-CTL-07 - LORA/ADAPTER INTEGRITY VERIFICATION

Field	Retail implementation record
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Low-rank adaptation and other adapters may be used to localise models for brands, regions or franchises. Verify adapter origin, hash, approved base-model compatibility and behaviour before loading it into production. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-007; RET-UC-014; RET-UC-021
Related threats	RET-THR-007; RET-THR-012; RET-THR-017
Minimum implementation	Approved scope and owner; documented applicability; baseline

Field	Retail implementation record
	technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-007; RET-EVD-010
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-007; RET-MET-014
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D1-CTL-08 - MODEL MERGE ATTACK DETECTION

Field	Retail implementation record
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Retail teams may merge models or checkpoints to combine language, vision or fraud capabilities. Treat every merge as a new artefact requiring provenance, behavioural comparison and backdoor testing rather than inheriting trust from the source models. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-008; RET-UC-015; RET-UC-022; RET-UC-029
Related threats	RET-THR-008; RET-THR-013; RET-THR-018; RET-THR-023
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-008; RET-EVD-011; RET-EVD-014
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-008; RET-MET-015
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required

Field	Retail implementation record
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D1-CTL-09 - QUANTIZATION BACKDOOR SCREENING

Field	Retail implementation record
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Quantised models are common on cameras, kiosks and store-edge hardware. Re-test quantised builds because compression can expose or preserve behaviours that were not visible in the full-precision model. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-009; RET-UC-016; RET-UC-023; RET-UC-030; RET-UC-005
Related threats	RET-THR-009; RET-THR-014; RET-THR-019
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-009; RET-EVD-012; RET-EVD-015; RET-EVD-018
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-009; RET-MET-016
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D2-CTL-01 - DIRECT PROMPT INJECTION PREVENTION

Field	Retail implementation record
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Customer-service and shopping assistants must treat customer prompts as untrusted input. Separate instructions from customer content, constrain account actions and prevent a conversational request from bypassing refund, discount or identity controls. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-010; RET-UC-017; RET-UC-024
Related threats	RET-THR-010; RET-THR-015; RET-THR-020; RET-THR-025
Minimum implementation	Approved scope and owner; documented applicability; baseline

Field	Retail implementation record
	technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-010; RET-EVD-013
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-010; RET-MET-017
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D2-CTL-02 - INDIRECT PROMPT INJECTION PREVENTION

Field	Retail implementation record
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Retail assistants ingest product pages, reviews, supplier documents and support content. Sanitise retrieved material and isolate tool instructions so hidden text in a listing or document cannot redirect the model or exfiltrate data. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-011; RET-UC-018; RET-UC-025; RET-UC-032
Related threats	RET-THR-011; RET-THR-016; RET-THR-021
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-011; RET-EVD-014; RET-EVD-017
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-011; RET-MET-018
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required

Field	Retail implementation record
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D2-CTL-03 - JAILBREAK RESISTANCE TESTING

Field	Retail implementation record
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Test retail assistants against attempts to produce prohibited product advice, reveal policies, create fraudulent discounts or evade age and account controls. Re-test after model, prompt, retrieval or tool changes. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-012; RET-UC-019; RET-UC-026; RET-UC-001; RET-UC-008
Related threats	RET-THR-012; RET-THR-017; RET-THR-022; RET-THR-027
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-012; RET-EVD-015; RET-EVD-018; RET-EVD-021
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-012; RET-MET-019
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D2-CTL-04 - MULTI-MODAL INJECTION DEFENSE

Field	Retail implementation record
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Visual-search, receipt, shelf-image and voice systems can carry adversarial instructions outside ordinary text prompts. Validate each modality independently and at the point where modalities are fused. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-013; RET-UC-020; RET-UC-027
Related threats	RET-THR-013; RET-THR-018; RET-THR-023
Minimum implementation	Approved scope and owner; documented applicability; baseline

Field	Retail implementation record
	technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-013; RET-EVD-016
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-013; RET-MET-020
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D2-CTL-05 - FUNCTION CALL/TOOL CALL INJECTION PREVENTION

Field	Retail implementation record
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Agents connected to refunds, inventory, customer records or campaigns must validate every function call against user identity, transaction state and approved limits. Model-generated arguments are not trusted authorisation. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-014; RET-UC-021; RET-UC-028; RET-UC-003
Related threats	RET-THR-014; RET-THR-019; RET-THR-024; RET-THR-029
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-014; RET-EVD-017; RET-EVD-020
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-014; RET-MET-001
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required

Field	Retail implementation record
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D2-CTL-06 - CROSS-CONTEXT HIJACKING MITIGATION

Field	Retail implementation record
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	A retailer may reuse one model across customer, employee, seller and developer contexts. Enforce context separation so content or memory from one tenant, account or workflow cannot influence another. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-015; RET-UC-022; RET-UC-029; RET-UC-004; RET-UC-011
Related threats	RET-THR-015; RET-THR-020; RET-THR-025
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-015; RET-EVD-018; RET-EVD-021; RET-EVD-024
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-015; RET-MET-002
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D3-CTL-01 - LEAST AGENCY ENFORCEMENT

Field	Retail implementation record
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Retail agents should receive only the tools and transaction authority required for the current task. A product assistant should not obtain refund, pricing or inventory-write capability merely because those tools exist in the same platform. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-016; RET-UC-023; RET-UC-030
Related threats	RET-THR-016; RET-THR-021; RET-THR-026; RET-THR-031
Minimum implementation	Approved scope and owner; documented applicability; baseline

Field	Retail implementation record
	technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-016; RET-EVD-019
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-016; RET-MET-003
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D3-CTL-02 - INTER-AGENT COMMUNICATION SECURITY

Field	Retail implementation record
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	When merchandising, inventory, fraud and customer-service agents exchange messages, authenticate the sender, validate message schemas and record delegated authority. Do not allow one agent to create authority for another through natural-language assertions. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-017; RET-UC-024; RET-UC-031; RET-UC-006
Related threats	RET-THR-017; RET-THR-022; RET-THR-027
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-017; RET-EVD-020; RET-EVD-023
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-017; RET-MET-004
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required

Field	Retail implementation record
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D3-CTL-03 - AGENTIC PROMPT CHAINING DETECTION

Field	Retail implementation record
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Multi-step retail workflows can hide unsafe intent across individually benign prompts. Detect chains that progressively obtain customer data, alter promotions or prepare unauthorised transactions. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-018; RET-UC-025; RET-UC-032; RET-UC-007; RET-UC-014
Related threats	RET-THR-018; RET-THR-023; RET-THR-028; RET-THR-033
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-018; RET-EVD-021; RET-EVD-024; RET-EVD-002
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-018; RET-MET-005
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D3-CTL-04 - EMBODIED AI SAFETY CONTROLS

Field	Retail implementation record
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Warehouse robots, autonomous stores and AI-enabled handling equipment require bounded operating zones, tested safety interlocks and controlled behaviour when sensors, networks or models fail. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-019; RET-UC-026; RET-UC-001
Related threats	RET-THR-019; RET-THR-024; RET-THR-029
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and

Field	Retail implementation record
	operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-019; RET-EVD-022
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-019; RET-MET-006
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D3-CTL-05 - MULTI-AGENT TRUST CHAIN ATTESTATION

Field	Retail implementation record
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	For multi-agent retail operations, preserve an attested chain showing which agent, identity, model version and policy authorised each consequential action. Break the chain when any participant cannot be verified. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-020; RET-UC-027; RET-UC-002; RET-UC-009
Related threats	RET-THR-020; RET-THR-025; RET-THR-030; RET-THR-035
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-020; RET-EVD-023; RET-EVD-001
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-020; RET-MET-007
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D3-CTL-06 - PERSISTENT MEMORY EXFILTRATION PREVENTION

Field	Retail implementation record
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Persistent assistant memory may accumulate customer, employee, seller or source-code information. Prevent retrieval or export of memory outside the originating account and monitor bulk or unusual memory access. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-021; RET-UC-028; RET-UC-003; RET-UC-010; RET-UC-017
Related threats	RET-THR-021; RET-THR-026; RET-THR-031
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-021; RET-EVD-024; RET-EVD-002; RET-EVD-005
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-001; RET-MET-008
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D3-CTL-07 - SECURE MEMORY LIFECYCLE MANAGEMENT

Field	Retail implementation record
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Define retention, correction, deletion and re-indexing rules for conversational and agent memory. Account closure, employee departure and model retirement must trigger removal or controlled archival of associated memory. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-022; RET-UC-029; RET-UC-004
Related threats	RET-THR-022; RET-THR-027; RET-THR-032; RET-THR-001
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.

Field	Retail implementation record
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-022; RET-EVD-025
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-002; RET-MET-009
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D4-CTL-01 - AI BILL OF MATERIALS (AI BOM) MAINTENANCE

Field	Retail implementation record
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Maintain an AI bill of materials for each retail service covering models, adapters, datasets, retrieval stores, prompts, agents, tools, libraries, providers and edge deployments. Link changes to release and incident records. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-023; RET-UC-030; RET-UC-005; RET-UC-012
Related threats	RET-THR-023; RET-THR-028; RET-THR-033
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-023; RET-EVD-001; RET-EVD-004
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-003; RET-MET-010
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D4-CTL-02 - MODEL FILE & ARTIFACT SCANNING

Field	Retail implementation record
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Scan downloaded models, adapters and serialized artefacts before use. Retail data-science teams must treat model files from public hubs, vendors and internal experiments as executable supply-chain content. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-024; RET-UC-031; RET-UC-006; RET-UC-013; RET-UC-020
Related threats	RET-THR-024; RET-THR-029; RET-THR-034; RET-THR-003
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-024; RET-EVD-002; RET-EVD-005; RET-EVD-008
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-004; RET-MET-011
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D4-CTL-03 - MODEL HUB & REGISTRY VETTING

Field	Retail implementation record
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Approve model hubs and registries based on provenance, moderation, vulnerability response and licence controls. Prevent unreviewed models from moving directly from an analyst notebook into a customer or store workflow. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-025; RET-UC-032; RET-UC-007
Related threats	RET-THR-025; RET-THR-030; RET-THR-035
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-

Field	Retail implementation record
	channel correlation where relevant.
Illustrative evidence	RET-EVD-025; RET-EVD-003
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-005; RET-MET-012
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D4-CTL-04 - MCP SERVER BEHAVIORAL MONITORING

Field	Retail implementation record
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Model Context Protocol servers can expose inventory, customer relationship management and order systems to agents. Monitor server discovery, tool enumeration, read/write patterns and unexpected access to high-value retail data. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-026; RET-UC-001; RET-UC-008; RET-UC-015
Related threats	RET-THR-026; RET-THR-031; RET-THR-036; RET-THR-005
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-001; RET-EVD-004; RET-EVD-007
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-006; RET-MET-013
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D4-CTL-05 - THIRD-PARTY AI API SECURITY ASSESSMENT

Field	Retail implementation record
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Assess external AI application programming interfaces for authentication, tenant isolation, data retention, training use, regional processing, model-change notice, rate limits and incident support before sending customer or commercial data. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-027; RET-UC-002; RET-UC-009; RET-UC-016; RET-UC-023
Related threats	RET-THR-027; RET-THR-032; RET-THR-001
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-002; RET-EVD-005; RET-EVD-008; RET-EVD-011
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-007; RET-MET-014
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D4-CTL-06 - SHADOW AI DISCOVERY & GOVERNANCE

Field	Retail implementation record
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Shadow AI commonly appears in marketing, buying, store and franchise teams using consumer tools for copy, images or analysis. Discover unsanctioned use through procurement, network, browser and data-loss signals, then provide an approved alternative and enforce data boundaries. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-028; RET-UC-003; RET-UC-010
Related threats	RET-THR-028; RET-THR-033; RET-THR-002; RET-THR-007
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-

Field	Retail implementation record
	channel correlation where relevant.
Illustrative evidence	RET-EVD-003; RET-EVD-006
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-008; RET-MET-015
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D4-CTL-07 - AI SOFTWARE COMPOSITION ANALYSIS (SCA)

Field	Retail implementation record
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Software Composition Analysis for retail AI must include orchestration frameworks, vector databases, model loaders, plugins, computer-vision packages and agent tools, not only the conventional web application dependencies. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-029; RET-UC-004; RET-UC-011; RET-UC-018
Related threats	RET-THR-029; RET-THR-034; RET-THR-003
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-004; RET-EVD-007; RET-EVD-010
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-009; RET-MET-016
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D5-CTL-01 - HARMFUL CONTENT BLOCKING

Field	Retail implementation record
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative requirement	Refer to GAISRF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Block outputs that facilitate fraud, unsafe product use, harassment, prohibited goods or harmful employee/customer interactions. Calibrate controls to the channel and provide escalation instead of silently failing consequential requests. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-030; RET-UC-005; RET-UC-012; RET-UC-019; RET-UC-026
Related threats	RET-THR-030; RET-THR-035; RET-THR-004; RET-THR-009
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-005; RET-EVD-008; RET-EVD-011; RET-EVD-014
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-010; RET-MET-017
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D5-CTL-02 - PII LEAKAGE PREVENTION

Field	Retail implementation record
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative requirement	Refer to GAISRF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Prevent customer, payment, loyalty, employee and supplier identifiers from appearing in prompts, retrieved context or outputs beyond the approved transaction. Test redaction and access boundaries with realistic retail records. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-031; RET-UC-006; RET-UC-013
Related threats	RET-THR-031; RET-THR-036; RET-THR-005
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.

Field	Retail implementation record
Illustrative evidence	RET-EVD-006; RET-EVD-009
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-011; RET-MET-018
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D5-CTL-03 - COPYRIGHT DETECTION

Field	Retail implementation record
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Product descriptions, advertising and generated imagery may reproduce protected material. Record source rights, detect suspicious similarity and route uncertain content for review before publication. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-032; RET-UC-007; RET-UC-014; RET-UC-021
Related threats	RET-THR-032; RET-THR-001; RET-THR-006; RET-THR-011
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-007; RET-EVD-010; RET-EVD-013
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-012; RET-MET-019
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D5-CTL-04 - AI WATERMARKING ROBUSTNESS

Field	Retail implementation record
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Where watermarks or provenance markers are used for retail media, test whether resizing, cropping, recompression and marketplace reposting remove them. Do not treat watermark presence as proof that content is authentic. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-001; RET-UC-008; RET-UC-015; RET-UC-022; RET-UC-029
Related threats	RET-THR-033; RET-THR-002; RET-THR-007
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-008; RET-EVD-011; RET-EVD-014; RET-EVD-017
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-013; RET-MET-020
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D5-CTL-05 - PRIVACY-BY-DESIGN VERIFICATION

Field	Retail implementation record
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Verify privacy controls at design and release gates for loyalty profiling, retail media, biometrics, employee monitoring and conversational systems. Data minimisation and purpose boundaries must be visible in architecture and operating evidence. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-002; RET-UC-009; RET-UC-016
Related threats	RET-THR-034; RET-THR-003; RET-THR-008; RET-THR-013
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.

Field	Retail implementation record
Illustrative evidence	RET-EVD-009; RET-EVD-012
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-014; RET-MET-001
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D5-CTL-06 - PRIVACY-PRESERVING ML VALIDATION

Field	Retail implementation record
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Where federated learning, differential privacy, synthetic data or secure computation is claimed, test the privacy parameters and residual leakage against the retail use case. A technique label alone is not evidence of effective protection. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-003; RET-UC-010; RET-UC-017; RET-UC-024
Related threats	RET-THR-035; RET-THR-004; RET-THR-009
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-010; RET-EVD-013; RET-EVD-016
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-015; RET-MET-002
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D6-CTL-01 - HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS

Field	Retail implementation record
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Require authorised human review before consequential actions such as account suspension, return denial, biometric intervention, hiring rejection, high-value refund or unsafe warehouse movement. Reviewers need the evidence and authority to reverse the model outcome. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-004; RET-UC-011; RET-UC-018; RET-UC-025; RET-UC-032
Related threats	RET-THR-036; RET-THR-005; RET-THR-010; RET-THR-015
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-011; RET-EVD-014; RET-EVD-017; RET-EVD-020
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-016; RET-MET-003
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D6-CTL-02 - AUDIT TRAIL COMPLETENESS

Field	Retail implementation record
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Logs must reconstruct the customer or operational journey: identity, input, retrieved data, model and prompt version, output, tool call, override and final action. Logging only the final response is insufficient for disputes or incidents. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-005; RET-UC-012; RET-UC-019
Related threats	RET-THR-001; RET-THR-006; RET-THR-011
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-

Field	Retail implementation record
	channel correlation where relevant.
Illustrative evidence	RET-EVD-012; RET-EVD-015
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-017; RET-MET-004
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D6-CTL-03 - AI MODEL CARD COMPLETENESS

Field	Retail implementation record
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Retail model cards should state channel, population, data origin, decision authority, known failure modes, seasonal limits, supplier dependencies and prohibited uses. Generic vendor documentation does not replace a retailer-specific deployment record. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-006; RET-UC-013; RET-UC-020; RET-UC-027
Related threats	RET-THR-002; RET-THR-007; RET-THR-012; RET-THR-017
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-013; RET-EVD-016; RET-EVD-019
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-018; RET-MET-005
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D6-CTL-04 - AI INCIDENT RESPONSE READINESS

Field	Retail implementation record
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	AI incident plans should cover misleading product content, pricing errors, fraud-control failure, biometric misidentification, agent misuse, model compromise and provider outages. Preserve model and prompt versions before rollback. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-007; RET-UC-014; RET-UC-021; RET-UC-028; RET-UC-003
Related threats	RET-THR-003; RET-THR-008; RET-THR-013
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-014; RET-EVD-017; RET-EVD-020; RET-EVD-023
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-019; RET-MET-006
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D6-CTL-05 - MODEL DEPRECATION & DECOMMISSIONING

Field	Retail implementation record
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	When retiring a model, remove endpoints, credentials, cached artefacts and dependent agent routes; archive required evidence; migrate open cases; and verify that stores or franchisees are not still using the superseded version. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-008; RET-UC-015; RET-UC-022
Related threats	RET-THR-004; RET-THR-009; RET-THR-014; RET-THR-019
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.

Field	Retail implementation record
Illustrative evidence	RET-EVD-015; RET-EVD-018
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-020; RET-MET-007
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D6-CTL-06 - THIRD-PARTY AI VENDOR GOVERNANCE

Field	Retail implementation record
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Retail contracts should secure evidence access, data-use limits, change notice, incident cooperation, subcontractor transparency, continuity and exit support. Procurement approval without enforceable operating rights leaves a control gap. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-009; RET-UC-016; RET-UC-023; RET-UC-030
Related threats	RET-THR-005; RET-THR-010; RET-THR-015
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-016; RET-EVD-019; RET-EVD-022
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-001; RET-MET-008
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D6-CTL-07 - AI RESILIENCE & BUSINESS CONTINUITY

Field	Retail implementation record
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Define degraded modes for payment risk, inventory, checkout, customer service and physical operations. Test manual or rules-based fallback under peak demand rather than assuming the provider will remain available. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-010; RET-UC-017; RET-UC-024; RET-UC-031; RET-UC-006
Related threats	RET-THR-006; RET-THR-011; RET-THR-016; RET-THR-021
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-017; RET-EVD-020; RET-EVD-023; RET-EVD-001
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-002; RET-MET-009
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P1 - Start first
Scope label	Foundational - canonical D1-D8 scope

D7-CTL-H01 - AI-GENERATED PHISHING SIMULATION

Field	Retail implementation record
Domain	D7: HUMAN & SOCIETAL HARMS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Simulate AI-generated phishing against store, finance, buying and supplier-management staff using realistic seasonal and invoice themes. Measure reporting and verification behaviour, not just click rates. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-011; RET-UC-018; RET-UC-025
Related threats	RET-THR-007; RET-THR-012; RET-THR-017
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-018; RET-EVD-021

Field	Retail implementation record
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-003; RET-MET-010
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D7-CTL-H02 - DEEFAKE DETECTION TRAINING

Field	Retail implementation record
Domain	D7: HUMAN & SOCIETAL HARMS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Train staff who approve payments, supplier changes or executive instructions to recognise deepfake voice and video indicators and to use an independent verification channel. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-012; RET-UC-019; RET-UC-026; RET-UC-001
Related threats	RET-THR-008; RET-THR-013; RET-THR-018; RET-THR-023
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-019; RET-EVD-022; RET-EVD-025
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-004; RET-MET-011
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D7-CTL-H03 - OUT-OF-BAND AUTHENTICATION

Field	Retail implementation record
Domain	D7: HUMAN & SOCIETAL HARMS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Changes to bank details, high-value refunds, privileged access and emergency supplier requests should be confirmed through a pre-registered channel independent of the initiating message or call. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-013; RET-UC-020; RET-UC-027; RET-UC-002; RET-UC-009
Related threats	RET-THR-009; RET-THR-014; RET-THR-019
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-020; RET-EVD-023; RET-EVD-001; RET-EVD-004
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-005; RET-MET-012
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D7-CTL-H04 - AI SOCIAL ENGINEERING IR

Field	Retail implementation record
Domain	D7: HUMAN & SOCIETAL HARMS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Incident procedures must recognise AI-assisted impersonation, synthetic documents and coordinated social engineering. Preserve media and communications while validating the claimed identity through trusted records. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-014; RET-UC-021; RET-UC-028
Related threats	RET-THR-010; RET-THR-015; RET-THR-020; RET-THR-025
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-021; RET-EVD-024

Field	Retail implementation record
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-006; RET-MET-013
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D7-CTL-H05 - AI-ENHANCED EXTERNAL ATTACK DEFENSE

Field	Retail implementation record
Domain	D7: HUMAN & SOCIETAL HARMS
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Tune email, identity, endpoint and fraud defences for AI-scaled reconnaissance, credential attacks and content variation. Retail peak periods require heightened monitoring because staffing and transaction volume reduce review time. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-015; RET-UC-022; RET-UC-029; RET-UC-004
Related threats	RET-THR-011; RET-THR-016; RET-THR-021
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-022; RET-EVD-025; RET-EVD-003
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-007; RET-MET-014
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D8-CTL-01 - EU AI ACT RISK TIER MAPPING

Field	Retail implementation record
Domain	D8: REGULATORY ALIGNMENT & COMPLIANCE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Map each retail AI use case to the European Union Artificial Intelligence Act role and risk analysis where the regulation applies. Do not classify an entire retailer once; assess hiring, biometrics, customer and operational systems separately. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-016; RET-UC-023; RET-UC-030; RET-UC-005; RET-UC-012
Related threats	RET-THR-012; RET-THR-017; RET-THR-022; RET-THR-027
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-023; RET-EVD-001; RET-EVD-004; RET-EVD-007
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-008; RET-MET-015
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D8-CTL-02 - ISO 42001 GAP ANALYSIS

Field	Retail implementation record
Domain	D8: REGULATORY ALIGNMENT & COMPLIANCE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Use an International Organization for Standardization/International Electrotechnical Commission 42001 gap analysis to compare management-system practices, but preserve GAISSF control-level evidence and do not claim equivalence between the instruments. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-017; RET-UC-024; RET-UC-031
Related threats	RET-THR-013; RET-THR-018; RET-THR-023
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-

Field	Retail implementation record
	channel correlation where relevant.
Illustrative evidence	RET-EVD-024; RET-EVD-002
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-009; RET-MET-016
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D8-CTL-03 - GPAI TECHNICAL DOCUMENTATION VERIFICATION

Field	Retail implementation record
Domain	D8: REGULATORY ALIGNMENT & COMPLIANCE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Where a general-purpose AI provider is in scope, verify that the technical documentation available to the retailer is sufficient for integration, risk assessment, monitoring and downstream instructions. Record unavailable evidence as a supplier limitation. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-018; RET-UC-025; RET-UC-032; RET-UC-007
Related threats	RET-THR-014; RET-THR-019; RET-THR-024; RET-THR-029
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-025; RET-EVD-003; RET-EVD-006
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-010; RET-MET-017
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D8-CTL-04 - DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)

Field	Retail implementation record
Domain	D8: REGULATORY ALIGNMENT & COMPLIANCE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Digital Operational Resilience Act incident reporting is relevant only where the retail entity or service falls within its financial-sector scope. Record the applicability decision instead of presenting the control as universally required for retail. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-019; RET-UC-026; RET-UC-001; RET-UC-008; RET-UC-015
Related threats	RET-THR-015; RET-THR-020; RET-THR-025
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-001; RET-EVD-004; RET-EVD-007; RET-EVD-010
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-011; RET-MET-018
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D8-CTL-05 - NIST SP 800-218A COMPLIANCE CHECK

Field	Retail implementation record
Domain	D8: REGULATORY ALIGNMENT & COMPLIANCE
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Apply National Institute of Standards and Technology Special Publication 800-218A practices to AI model and software development where relevant, including provenance, secure build, testing and release evidence. Document gaps for acquired services that the retailer cannot inspect. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-020; RET-UC-027; RET-UC-002
Related threats	RET-THR-016; RET-THR-021; RET-THR-026; RET-THR-031
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-

Field	Retail implementation record
	channel correlation where relevant.
Illustrative evidence	RET-EVD-002; RET-EVD-005
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-012; RET-MET-019
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Retail AI security specialist review required
Implementation priority	P2 - Risk-triggered / capability-specific
Scope label	Foundational - canonical D1-D8 scope

D9-CTL-01 - PHYSICAL HARM BOUNDARY ENFORCEMENT

Field	Retail implementation record
Domain	D9: PHYSICAL AI SAFETY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Set explicit physical limits for warehouse robots, automated handling, smart carts and autonomous store systems. Software optimisation must not permit speed, force, route or proximity beyond the approved safety boundary. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-021; RET-UC-028; RET-UC-003; RET-UC-010
Related threats	RET-THR-017; RET-THR-022; RET-THR-027
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-003; RET-EVD-006; RET-EVD-009
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-013; RET-MET-020
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Physical-AI specialist review required
Implementation priority	P3 - Conditional physical AI
Scope label	Conditional - physical AI in scope

D9-CTL-02 - SAFE STATE AND GRACEFUL DEGRADATION

Field	Retail implementation record
Domain	D9: PHYSICAL AI SAFETY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	On model, sensor, network or cloud failure, physical retail systems must enter a defined safe or controlled state without depending on continued model inference. Test degraded operation during realistic store and warehouse conditions. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-022; RET-UC-029; RET-UC-004; RET-UC-011; RET-UC-018
Related threats	RET-THR-018; RET-THR-023; RET-THR-028; RET-THR-033
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-004; RET-EVD-007; RET-EVD-010; RET-EVD-013
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-014; RET-MET-001
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Physical-AI specialist review required
Implementation priority	P3 - Conditional physical AI
Scope label	Conditional - physical AI in scope

D9-CTL-03 - HUMAN OVERRIDE AND EMERGENCY STOP

Field	Retail implementation record
Domain	D9: PHYSICAL AI SAFETY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Warehouse robotics and autonomous store systems require accessible local emergency stops and authorised human override. Remote vendor commands or software updates must not disable the emergency function. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-023; RET-UC-030; RET-UC-005
Related threats	RET-THR-019; RET-THR-024; RET-THR-029
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-005; RET-EVD-008

Field	Retail implementation record
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-015; RET-MET-002
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Physical-AI specialist review required
Implementation priority	P3 - Conditional physical AI
Scope label	Conditional - physical AI in scope

D9-CTL-04 - CYBER-PHYSICAL ATTACK DETECTION

Field	Retail implementation record
Domain	D9: PHYSICAL AI SAFETY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Correlate cyber indicators with physical anomalies such as unexpected routes, repeated sensor disagreement, command bursts or safety-zone violations. Cyber monitoring alone may miss an emerging physical incident. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-024; RET-UC-031; RET-UC-006; RET-UC-013
Related threats	RET-THR-020; RET-THR-025; RET-THR-030; RET-THR-035
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-006; RET-EVD-009; RET-EVD-012
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-016; RET-MET-003
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Physical-AI specialist review required
Implementation priority	P3 - Conditional physical AI
Scope label	Conditional - physical AI in scope

D9-CTL-05 - PHYSICAL ENVIRONMENT INTEGRITY MONITORING

Field	Retail implementation record
Domain	D9: PHYSICAL AI SAFETY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Monitor camera position, sensor obstruction, lighting, floor layout, shelf movement and other environmental changes that can invalidate a physical AI system's assumptions. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-025; RET-UC-032; RET-UC-007; RET-UC-014; RET-UC-021
Related threats	RET-THR-021; RET-THR-026; RET-THR-031
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-007; RET-EVD-010; RET-EVD-013; RET-EVD-016
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-017; RET-MET-004
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Physical-AI specialist review required
Implementation priority	P3 - Conditional physical AI
Scope label	Conditional - physical AI in scope

D9-CTL-06 - ACTUATOR COMMAND VERIFICATION

Field	Retail implementation record
Domain	D9: PHYSICAL AI SAFETY
Authoritative requirement	Refer to GAISSF-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	Validate actuator commands against identity, authorised workflow, current sensor state and physical limits before execution. Reject stale, duplicated or out-of-sequence commands. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-026; RET-UC-001; RET-UC-008
Related threats	RET-THR-022; RET-THR-027; RET-THR-032; RET-THR-001
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-008; RET-EVD-011
Test procedure	Inspect design evidence, sample operating records, test one

Field	Retail implementation record
	representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-018; RET-MET-005
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Physical-AI specialist review required
Implementation priority	P3 - Conditional physical AI
Scope label	Conditional - physical AI in scope

D9-CTL-07 - PHYSICAL INCIDENT EVIDENCE PRESERVATION

Field	Retail implementation record
Domain	D9: PHYSICAL AI SAFETY
Authoritative requirement	Refer to GAISSE-NOR-001 v1.0 for the complete normative requirement.
Retail interpretation	For physical incidents, preserve commands, sensor streams, model version, safety interlock state, operator actions and relevant video with synchronized time. Ordinary application logs are not sufficient for reconstruction. [T3]
Applicability	Determine for every in-scope system. Record Not Applicable only with approved, risk-based rationale.
Related use cases	RET-UC-027; RET-UC-002; RET-UC-009; RET-UC-016
Related threats	RET-THR-023; RET-THR-028; RET-THR-033
Minimum implementation	Approved scope and owner; documented applicability; baseline technical or procedural safeguard; retained design and operating evidence; exception and escalation route.
Enhanced implementation	Automated enforcement and telemetry; independent testing; supplier evidence rights; change-triggered reassessment; cross-channel correlation where relevant.
Illustrative evidence	RET-EVD-009; RET-EVD-012; RET-EVD-015
Test procedure	Inspect design evidence, sample operating records, test one representative failure or attack path, verify exceptions and confirm change triggers.
Illustrative metrics	RET-MET-019; RET-MET-006
Responsible roles	AI Security Lead / relevant retail system owner / independent reviewer
Common failure	Policy exists but scope, operating evidence, supplier coverage or remediation closure is missing.
Compensating control	Documented manual review, constrained functionality, segmented deployment, enhanced monitoring or service fallback pending remediation.
Maturity indicator	Current evidence for all applicable systems, measured effectiveness and no overdue high-risk exception.
Review gate	Physical-AI specialist review required
Implementation priority	P3 - Conditional physical AI
Scope label	Conditional - physical AI in scope

7. Data governance and retail information assets

- Retail data classification and purpose controls are grounded in applicable legal and standards obligations [T1], while the specific implementation examples are contextual retail guidance [T3].
- Document purpose, lawful or contractual basis where applicable, lineage, retention, access, transfers, deletion and production-data use in testing.
- Separate data required for fraud and security from data reused for marketing, model training or provider improvement.
- Treat prompts, retrieved context, model outputs, embeddings and agent action logs as governed information assets.

8. AI supply-chain and third-party risk

Supplier evidence, data-use and change-notification requirements are implementation guidance [T3] that should be reconciled with applicable contracts, laws and standards [T1].

9. Secure retail AI lifecycle

Stage	Required retail gate
Use-case approval	Document purpose, owner, affected persons, authority, legal review triggers and prohibited uses.
Procurement	Complete due diligence, data-use restrictions, evidence rights, exit and change notification.
Design and development	Threat model, data lineage, architecture review, access boundaries and human oversight.
Testing	Security, adversarial, fraud, privacy, fairness, accessibility, output, fallback and physical-environment tests as applicable.
Release	Approved evidence pack, residual risk, rollback, monitoring and incident ownership.
Operation	Monitor drift, abuse, complaints, provider changes, exceptions and business continuity.
Retirement	Revoke access, preserve required evidence, delete or archive data and manage dependent systems.

10. Testing and evaluation catalogue

ID	Test	Trigger	Method	Acceptance
RET-TST-001	Prompt-injection and tool-abuse test	On deployment and material change	Representative direct and indirect attacks	No unauthorised action or sensitive disclosure
RET-TST-002	Fraud resilience test	At least quarterly for critical fraud systems	Known fraud, adaptive evasion and false-positive sampling	Approved detection and customer-impact thresholds
RET-TST-003	Product-information accuracy test	Each release and catalogue-model change	Sample specifications, compatibility, safety and restricted claims	Critical factual errors blocked or escalated
RET-TST-004	Pricing and promotion integrity test	Before campaign or model release	Boundary, adversarial and rollback tests	No unauthorised or unexplained price/promotion outcome
RET-TST-005	Biometric and vision performance test	Before use and periodically	Representative environment and demographic slices	Approved performance, escalation and intervention limits
RET-TST-006	Seasonal drift and stress test	Before major seasonal events	Peak load and shifted distributions	Fallback and thresholds operate under peak conditions

ID	Test	Trigger	Method	Acceptance
RET-TST-007	Third-party outage and fallback test	At least annually	Provider loss, degraded mode and data recovery	Approved service continuity and manual fallback
RET-TST-008	Physical AI safe-state test	Before release and after safety-relevant change	Sensor, command, network and emergency-stop failures	System enters defined safe or controlled state

11. Human oversight and accountability

Oversight must be more than nominal [T3]. High-risk retail actions include payment or account blocking, return denial, biometric intervention, hiring rejection, high-value refunds, personalised-pricing exceptions and physical movement by autonomous equipment. The reviewer should receive the model rationale, relevant source records, confidence or uncertainty, policy limits and prior overrides; have authority to pause or reverse the action; and record the decision, evidence and escalation. Sampling after the event is not an adequate substitute where harm occurs immediately.

12. Consumer protection and transparency

- Identify when customers are interacting with AI and when generated content could affect a purchasing decision.
- Prevent unsupported product, safety, compatibility, pricing and promotional claims.
- Provide escalation and correction routes for consequential account, fraud, returns, biometric or age decisions.
- Assess dark-pattern, personalised-pricing, vulnerable-consumer, child, accessibility and synthetic-review risks by jurisdiction.

13. Monitoring metrics

ID	Metric	Definition	Data source	Frequency	Limitation	Escalation
RET-MET-001	Applicable controls with current evidence	Documented measure of applicable controls with current evidence for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-002	High-risk systems with approved human oversight	Documented measure of high-risk systems with approved human oversight for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-003	AI-related customer escalations	Documented measure of ai-related customer escalations for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-004	Prompt-injection detections	Documented measure of prompt-injection detections for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-005	Fraud false-positive rate	Documented measure of fraud false-positive rate for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may	Board- or executive-approved threshold for material deviation

ID	Metric	Definition	Data source	Frequency	Limitation	Escalation
					be invalid.	
RET-MET-006	Fraud false-negative estimate	Documented measure of fraud false-negative estimate for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-007	Pricing anomaly rate	Documented measure of pricing anomaly rate for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-008	Product-output correction rate	Documented measure of product-output correction rate for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-009	Recommendation complaint rate	Documented measure of recommendation complaint rate for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-010	Model drift alerts	Documented measure of model drift alerts for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-011	Third-party AI outages	Documented measure of third-party ai outages for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-012	Unapproved model changes	Documented measure of unapproved model changes for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-013	Privileged AI access events	Documented measure of privileged ai access events for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-014	Blocked agent actions	Documented measure of blocked agent actions for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-015	Biometric false-match rate	Documented measure of biometric false-match rate for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-016	Loss-prevention intervention precision	Documented measure of loss-prevention intervention precision for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-017	Rollback frequency	Documented measure of rollback	Security, model, fraud, customer-service, IAM,	Monthly for critical systems; quarterly	Thresholds require internal baseline; cross-	Board- or executive-approved

ID	Metric	Definition	Data source	Frequency	Limitation	Escalation
		frequency for the approved retail AI scope.	change or incident telemetry	otherwise	retailer comparisons may be invalid.	threshold for material deviation
RET-MET-018	Overdue high-risk exceptions	Documented measure of overdue high-risk exceptions for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-019	Mean time to detect AI incidents	Documented measure of mean time to detect ai incidents for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation
RET-MET-020	Mean time to contain AI incidents	Documented measure of mean time to contain ai incidents for the approved retail AI scope.	Security, model, fraud, customer-service, IAM, change or incident telemetry	Monthly for critical systems; quarterly otherwise	Thresholds require internal baseline; cross-retailer comparisons may be invalid.	Board- or executive-approved threshold for material deviation

14. AI incident management and resilience

AI incidents should be triaged by customer, worker, financial, operational, legal, privacy, safety and evidence impact. Response plans should preserve model versions, prompts, retrieved context, outputs, decisions, agent actions, access records and supplier communications. Retail fallback may include manual review, static rules, disabling personalisation, suspending biometric matching or operating warehouse systems in constrained mode.

15. Roles and responsibilities

Role	Governance	Implementation	Testing	Operation	Assurance
Board/risk committee	A	I	I	I	I
Executive sponsor	A	R	I	I	I
CISO / AI Security Lead	C	R	R	R	C
AI Governance Lead	R	R	C	C	R
Privacy / Legal / Compliance	C	C	C	C	R
Retail system owner	I	R	R	R	R
Fraud / Loss Prevention	I	C	R	R	R
Procurement / Supplier Assurance	I	C	R	C	R
Internal Audit / Independent Assessor	I	C	C	C	R

16. Implementation roadmap

Phase	Indicative window	Outputs
1 - Discovery and inventory	Days 0-30	Scope, owners, inventory, suppliers, data flows and criticality.

Phase	Indicative window	Outputs
2 - Risk and gap assessment	Days 31-60	Statement of Applicability, risk profiles, threat models and remediation plan.
3 - Control implementation	Days 61-120	Technical and procedural controls, supplier clauses, testing and monitoring.
4 - Assurance	Days 121-180	Evidence pack, internal assessment, issue closure and management review.
5 - Continuous improvement	Ongoing	Change monitoring, incidents, drift, regulatory review and reassessment.

Planning estimates are informative. Small retailers may use simpler governance and tooling, but should not omit applicable outcomes without documented rationale.

17. Evidence catalogue

ID	Evidence	Owner	Minimum contents	Frequency	Common deficiency
RET-EVD-001	AI system inventory	AI Security Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-002	Statement of Applicability	Data Governance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-003	Retail AI risk assessment	Supplier Assurance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-004	Threat model	Retail Operations Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-005	Data-flow diagram	Privacy Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-006	Data provenance and lineage record	Fraud Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-007	Model or system card	AI Governance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-008	Supplier due-diligence record	AI Security Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-009	AI bill of materials	Data Governance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence

ID	Evidence	Owner	Minimum contents	Frequency	Common deficiency
RET-EVD-010	Security architecture review	Supplier Assurance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-011	Adversarial test report	Retail Operations Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-012	Fraud-resilience test report	Privacy Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-013	Privacy impact assessment	Fraud Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-014	Fairness and impact assessment	AI Governance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-015	Human-oversight procedure	AI Security Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-016	Access-control review	Data Governance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-017	Change and release approval	Supplier Assurance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-018	Model monitoring report	Retail Operations Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-019	Incident record	Privacy Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-020	Business continuity and fallback test	Fraud Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-021	Customer disclosure and escalation record	AI Governance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-022	Biometric or computer-vision approval record	AI Security Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-023	Training and competency record	Data Governance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence

ID	Evidence	Owner	Minimum contents	Frequency	Common deficiency
RET-EVD-024	Exception register	Supplier Assurance Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence
RET-EVD-025	Management review minutes	Retail Operations Lead	Scope, owner, date, method, result, exceptions, approvals and referenced systems	At least annually and on material change	Missing scope, stale approval, unsupported assertion or absent operating evidence

18. Maturity model

Level	Description
1 - Initial	AI systems and controls are incomplete, reactive or undocumented.
2 - Repeatable	Priority systems have owners and recurring control activity, but coverage is inconsistent.
3 - Defined	Common governance, lifecycle, supplier and evidence methods are implemented across scope.
4 - Measured	Effectiveness, drift, incidents, exceptions and customer impacts are measured and reviewed.
5 - Adaptive	Controls are adjusted from telemetry, incidents, threat change and independent assurance.

19. Common implementation failures

Failure	Consequence	Corrective action
Treating AI as ordinary software	Model behaviour, data and provider change are not separately governed	Inventory model and data dependencies; add change triggers and monitoring.
Incomplete inventory	Embedded, franchise or SaaS AI remains outside assurance	Reconcile procurement, architecture, data and supplier records.
Reliance on vendor assurances	No retailer-specific operating evidence	Contract for evidence and test representative controls.
No tested fallback	Outage or model failure stops retail operations	Define and exercise manual or degraded modes.
Policy without evidence	Assessment cannot establish effectiveness	Collect sampled operating records, logs and approvals.
Uncontrolled generative AI	Data leakage and misleading content	Apply approved tools, retrieval controls, output checks and logging.

20. Worked scenarios

RET-SCN-001 - E-commerce recommendation manipulation

Field	Scenario record
Use case	RET-UC-001
Threat/failure	RET-THR-019
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-001 and RET-THR-019 were absent, ineffective or not evidenced in operation.
Detection	Detect abnormal seller/bot engagement, ranking shifts

Field	Scenario record
	and conversion patterns; compare against clean holdout queries.
Containment	Freeze suspicious ranking signals, remove manipulated inputs, revert the ranking model and review affected seller decisions.
Lesson	Ranking integrity requires adversarial engagement monitoring, not only offline relevance testing.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Freeze suspicious ranking signals, remove manipulated inputs, revert the ranking model and review affected seller decisions.

RET-SCN-002 - Loyalty takeover with AI-assisted fraud

Field	Scenario record
Use case	RET-UC-018
Threat/failure	RET-THR-014
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-018 and RET-THR-014 were absent, ineffective or not evidenced in operation.
Detection	Correlate impossible travel, device change, reward redemption and AI-generated support interactions.
Containment	Lock redemption, preserve account/session evidence, step up identity verification and reverse unauthorised reward transfers.
Lesson	Loyalty value should be protected with payment-grade identity and recovery controls.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Lock redemption, preserve account/session evidence, step up identity verification and reverse unauthorised reward transfers.

RET-SCN-003 - Hallucinated product information

Field	Scenario record
Use case	RET-UC-015
Threat/failure	RET-THR-020
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-015 and RET-THR-020 were absent, ineffective or not evidenced in operation.
Detection	Sample generated specifications against authoritative supplier data and monitor corrections, returns and complaints.
Containment	Unpublish affected content, revert to approved catalogue text, notify owners and correct customers where reliance may have occurred.
Lesson	Generated retail content needs authoritative attribute validation before publication.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Unpublish affected content, revert to approved catalogue text, notify owners and correct customers where reliance may have occurred.

RET-SCN-004 - Promotion-engine abuse

Field	Scenario record
Use case	RET-UC-004
Threat/failure	RET-THR-015
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-004 and RET-THR-015 were absent, ineffective or not evidenced in operation.
Detection	Detect unusual coupon combinations, account clusters, rapid redemptions and margin anomalies.
Containment	Disable the promotion rule, block abusive sessions, preserve transaction evidence and reissue corrected terms where needed.
Lesson	Promotion optimisation and promotion enforcement must be separated and independently tested.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Disable the promotion rule, block abusive sessions, preserve transaction evidence and reissue corrected terms where needed.

RET-SCN-005 - Self-checkout vision failure

Field	Scenario record
Use case	RET-UC-010
Threat/failure	RET-THR-024
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-010 and RET-THR-024 were absent, ineffective or not evidenced in operation.
Detection	Monitor mismatch between vision events, scanned items, weight sensors, payment events and staff overrides.
Containment	Place lanes in assisted mode, isolate the failing model/device and preserve video and sensor logs before recalibration.
Lesson	Store vision controls need tested human fallback during peak operations.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Place lanes in assisted mode, isolate the failing model/device and preserve video and sensor logs before recalibration.

RET-SCN-006 - Facial-recognition false match

Field	Scenario record
Use case	RET-UC-020
Threat/failure	RET-THR-022
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-020 and RET-THR-022 were absent, ineffective or not evidenced in operation.
Detection	Track match confidence, demographic/environmental performance and intervention outcomes; investigate complaints immediately.
Containment	Stop automated matching, prevent enforcement action,

Field	Scenario record
	preserve evidence and route the event to authorised manual review.
Lesson	A biometric alert is an investigative signal, not proof of identity.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Stop automated matching, prevent enforcement action, preserve evidence and route the event to authorised manual review.

RET-SCN-007 - Returns model false positive

Field	Scenario record
Use case	RET-UC-025
Threat/failure	RET-THR-016
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-025 and RET-THR-016 were absent, ineffective or not evidenced in operation.
Detection	Analyse appeal reversals, customer complaints, cohort disparities and sudden threshold changes.
Containment	Pause automated denial, permit manual returns review, restore wrongly affected accounts and recalibrate only after impact analysis.
Lesson	Fraud loss reduction does not justify unreviewable customer decisions.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Pause automated denial, permit manual returns review, restore wrongly affected accounts and recalibrate only after impact analysis.

RET-SCN-008 - Inventory forecast poisoning

Field	Scenario record
Use case	RET-UC-005
Threat/failure	RET-THR-001
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-005 and RET-THR-001 were absent, ineffective or not evidenced in operation.
Detection	Compare supplier/store submissions, forecast residuals and peer-location updates for abnormal influence.
Containment	Quarantine suspect data or model updates, rerun the forecast from a trusted baseline and review resulting orders.
Lesson	Forecast provenance must cover local and supplier-originated updates.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Quarantine suspect data or model updates, rerun the forecast from a trusted baseline and review resulting orders.

RET-SCN-009 - Third-party chatbot data leakage

Field	Scenario record
Use case	RET-UC-014
Threat/failure	RET-THR-035
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-014 and RET-THR-035 were absent, ineffective or not evidenced in operation.
Detection	Use data-loss alerts, prompt/output sampling and provider logs to identify sensitive fields leaving the approved boundary.
Containment	Disable the integration, revoke credentials, request provider preservation/deletion evidence and assess affected customers.
Lesson	Chatbot privacy depends on upstream retrieval and provider data-use controls.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Disable the integration, revoke credentials, request provider preservation/deletion evidence and assess affected customers.

RET-SCN-010 - AI-generated phishing against staff

Field	Scenario record
Use case	RET-UC-030
Threat/failure	RET-THR-033
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-030 and RET-THR-033 were absent, ineffective or not evidenced in operation.
Detection	Correlate email telemetry, identity anomalies, supplier-change requests and employee reporting.
Containment	Block the campaign, reset affected credentials, suspend requested payment changes and verify identities out of band.
Lesson	AI-scaled variation makes process verification more durable than content-only detection.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Block the campaign, reset affected credentials, suspend requested payment changes and verify identities out of band.

RET-SCN-011 - Warehouse-agent malfunction

Field	Scenario record
Use case	RET-UC-008
Threat/failure	RET-THR-028
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-008 and RET-THR-028 were absent, ineffective or not evidenced in operation.
Detection	Detect route deviation, command anomalies, sensor disagreement and safety-zone violations.
Containment	Trigger the local emergency stop, isolate the robotic cell, prevent remote restart and verify the physical area before recovery.

Field	Scenario record
Lesson	Physical containment must remain available when cloud control and inference are unavailable.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Trigger the local emergency stop, isolate the robotic cell, prevent remote restart and verify the physical area before recovery.

RET-SCN-012 - Retail-media targeting misuse

Field	Scenario record
Use case	RET-UC-019
Threat/failure	RET-THR-025
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-019 and RET-THR-025 were absent, ineffective or not evidenced in operation.
Detection	Audit audience construction, sensitive proxies, advertiser queries and complaint patterns.
Containment	Suspend the audience/campaign, prevent further data export, preserve targeting logic and conduct privacy and consumer-impact review.
Lesson	Retail media governance must cover inference and advertiser use, not only raw data access.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Suspend the audience/campaign, prevent further data export, preserve targeting logic and conduct privacy and consumer-impact review.

RET-SCN-013 - Franchise deployment without approval

Field	Scenario record
Use case	RET-UC-031
Threat/failure	RET-THR-010
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-031 and RET-THR-010 were absent, ineffective or not evidenced in operation.
Detection	Reconcile network, expense, browser and data-access signals against the approved AI inventory across franchise locations.
Containment	Block data access to the unapproved service, preserve usage records and require franchise remediation through contractual governance.
Lesson	Corporate policy alone does not control independent franchise technology without enforceable operational levers.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Block data access to the unapproved service, preserve usage records and require franchise remediation through contractual governance.

RET-SCN-014 - Dynamic-pricing governance failure

Field	Scenario record
Use case	RET-UC-003
Threat/failure	RET-THR-017
Context	Illustrative, non-vendor-specific retail scenario.
Likely control failures	Controls linked to RET-UC-003 and RET-THR-017 were absent, ineffective or not evidenced in operation.
Detection	Monitor unexplained price dispersion, rapid changes, protected/proxy cohorts, complaints and competitor-input anomalies.
Containment	Freeze automated repricing, restore the last approved price rules, preserve inputs and provide correction/escalation for affected customers.
Lesson	Pricing systems require explicit authority, explainability and rollback limits.
Notably Absent	This is not represented as a confirmed incident or prevalence estimate.
Recommended immediate action	Freeze automated repricing, restore the last approved price rules, preserve inputs and provide correction/escalation for affected customers.

21. External standards and regulatory crosswalk

The crosswalk identifies relationship types, not equivalence. Applicability and clause-level obligations must be verified by jurisdiction and system role.

ID	Source	Issuer	Relationship	Jurisdiction	Verification date
EXT-001	NIST AI RMF 1.0	NIST	Supporting control	United States / international use	2026-07-01
EXT-002	Regulation (EU) 2024/1689 (AI Act)	European Union	Contextual and partial alignment	European Union	2026-07-01
EXT-003	PCI DSS v4.0.1	PCI Security Standards Council	Supporting control	Contractual payment ecosystem	2026-07-01
EXT-004	ISO/IEC 42001:2023	ISO/IEC	Contextual and partial alignment	International	2026-07-01
EXT-005	ISO/IEC 27001:2022	ISO/IEC	Supporting control	International	2026-07-01
EXT-006	NIST Cybersecurity Framework 2.0	NIST	Supporting control	United States / international use	2026-07-01
EXT-007	FTC Consumer Review Rule	U.S. Federal Trade Commission	Contextual relevance	United States	2026-07-01
EXT-008	Web Content Accessibility Guidelines 2.2	W3C	Supporting control	International	2026-07-01
EXT-009	GDPR Regulation (EU) 2016/679	European Union	Contextual and partial alignment	European Union / EEA	2026-07-01
EXT-010	NIST Privacy Framework 1.0	NIST	Supporting control	United States / international use	2026-07-01

22. Notably Absent

- No proprietary retailer telemetry, confirmed field-exploitation corpus or sector-wide incident denominator was available.
- No claim is made that the listed threats have equal probability or that public reporting reflects actual prevalence.

- No automatic legal, privacy, employment, consumer-protection, accessibility, payment-card, biometric or certification conclusion is provided.
- No independent validation of retailer-specific performance, loss, false-positive or false-negative rates was performed.
- Jurisdiction-specific biometric, employment, pharmacy, age-restricted sales and personalised-pricing obligations require separate legal review.
- The guide does not establish that all retail AI systems are high risk; classification depends on function, authority, affected persons, jurisdiction and deployment.

23. Limitations

The guide depends on public evidence and the authoritative GAISSF baseline. Retail architectures, contracts, jurisdictions and operating data differ materially. Public incident data is incomplete, vendors may not disclose relevant model changes, and rapidly changing technology can make implementation examples stale. Specialist review is required before publication or use as an assessment basis.

Appendix A - Retail AI inventory template

System ID	Name	Use case	Owner	Supplier	Deployment	Data	Criticality	Oversight	Status	Last review
RET-SYS-__										

Appendix B - Risk assessment template

Risk ID	System	Threat	Impact	Likelihood basis	Controls	Residual risk	Owner	Decision
RET-RSK-__								

Appendix C - Supplier due-diligence questions

- What data is collected, retained, transferred, used for provider training or disclosed to subprocessors?
- How are model versions, material behavioural changes, vulnerabilities and incidents notified?
- What evidence, testing results, logs, model documentation and audit rights are available?
- How are access, tenant isolation, deletion, portability, continuity and termination handled?
- Which safety, security, privacy, accessibility and human-oversight limitations remain unverified?

Appendix D - Deployment readiness checklist

Readiness item	Status
Scope and accountable owner approved	Open
Use case and criticality classified	Open
Data flows and suppliers documented	Open
Applicable controls and exceptions approved	Open
Security and misuse testing passed	Open
Human oversight tested	Open
Monitoring and thresholds configured	Open

Readiness item	Status
Incident and fallback procedures exercised	Open
Legal/privacy/consumer review completed where triggered	Open
Residual risk accepted by authorised role	Open

Appendix E - Source and evidence register

Source ID	Title	Issuer	Class	URL	Verified
EXT-001	NIST AI RMF 1.0	NIST	Voluntary AI risk management framework	https://www.nist.gov/itl/ai-risk-management-framework	2026-07-01
EXT-002	Regulation (EU) 2024/1689 (AI Act)	European Union	Risk-based AI regulation	https://eur-lex.europa.eu/eli/reg/2024/1689/oj	2026-07-01
EXT-003	PCI DSS v4.0.1	PCI Security Standards Council	Payment-card data security standard	https://www.pcisecuritystandards.org/document_library/	2026-07-01
EXT-004	ISO/IEC 42001:2023	ISO/IEC	AI management system standard	https://www.iso.org/standard/81230.html	2026-07-01
EXT-005	ISO/IEC 27001:2022	ISO/IEC	Information security management system	https://www.iso.org/standard/27001	2026-07-01
EXT-006	NIST Cybersecurity Framework 2.0	NIST	Cybersecurity risk management framework	https://www.nist.gov/cyberframework	2026-07-01
EXT-007	FTC Consumer Review Rule	U.S. Federal Trade Commission	Prohibitions concerning fake reviews and testimonials	https://www.ftc.gov/business-guidance/resources/consumer-reviews-testimonials-rule-questions-answers	2026-07-01
EXT-008	Web Content Accessibility Guidelines 2.2	W3C	Accessibility guidance	https://www.w3.org/TR/WCAG22/	2026-07-01
EXT-009	GDPR Regulation (EU) 2016/679	European Union	Personal-data protection regulation	https://eur-lex.europa.eu/eli/reg/2016/679/oj	2026-07-01
EXT-010	NIST Privacy Framework 1.0	NIST	Privacy risk management framework	https://www.nist.gov/privacy-framework	2026-07-01

Appendix F - Open review gates

Gate	Reviewer	Status	Closure requirement
RG-01	Retail cybersecurity specialist	Open	Validate sector threat and control interpretation.
RG-02	Payments / PCI specialist	Open	Validate payment-system scope and PCI references.
RG-03	Privacy and data protection	Open	Validate personal-data, profiling and transfer guidance.
RG-04	Biometric and computer vision	Open	Validate biometric, age-estimation and intervention guidance.
RG-05	Employment and workforce AI	Open	Validate hiring, scheduling and monitoring guidance.
RG-06	Consumer protection	Open	Validate pricing, reviews, claims, transparency and

Gate	Reviewer	Status	Closure requirement
			contestability.
RG-07	Accessibility	Open	Validate accessibility testing and customer interaction guidance.
RG-08	Retail fraud and loss prevention	Open	Validate fraud scenarios, metrics and evidence.
RG-09	Supply chain and warehouse operations	Open	Validate robotics, fulfilment and continuity guidance.
RG-10	Franchise and marketplace operations	Open	Validate decentralised governance and seller impacts.
RG-11	Legal/editorial citation review	Open	Verify jurisdictional claims and source register.
RG-12	Final publication QA	Open	Close all material defects and approve release.