

GAISF™ Insurance Sector Implementation Guide

SEC-039 | Version 1.0 | Controlled Pre-Release Draft for Peer Review

Operational guidance for secure, resilient, fair and evidence-based use of AI across insurance

Field	Value
Document ID	SEC-039
Version	1.0
Publication date	30 June 2026
Publisher	ODA3 Institute
Category	Sector Implementation Guide
Priority / Launch Phase	High / Phase 2
Publication licence	GEL v1.0
Publication channels	Website / GitHub
Status	Controlled Pre-Release Draft for Peer Review - qualified legal/regulatory review and approval records remain open

Normative status

SEC-039 is informative. It does not amend GAISF, create independent certification requirements, or replace applicable law, regulation, actuarial judgement, contractual duties or policyholder protections.

Document control and legal notices

Control	Value
Document title	GAISSF™ Insurance Sector Implementation Guide
Document ID	SEC-039
Version	1.0
Owner	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
Classification	Informative sector guide
Authoritative framework source	GAISSF-NOR-001 Framework Standard v1.0
Control baseline	59 controls across D1-D9
Distribution	Public - Website / GitHub
Maintenance	Review at least annually and upon material GAISSF, regulatory or sector change

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute. GAISSF™ and ODA3 Institute™ are used as framework and market-facing identifiers. Use, reproduction, adaptation, certification, credential and trademark rights are governed by the applicable GAISSF publication terms and GEL v1.0.

This document does not constitute legal, regulatory, actuarial, financial, insurance, audit, certification or investment advice. It does not guarantee compliance, security, fairness, accuracy, resilience, insurability or absence of harmful outcomes. Applicable law, binding supervisory direction and contractual obligations take precedence.

Approval table

Role	Required reviewer	Status	Date	Notes
Document owner	ODA3 Institute	Approved for publication-candidate release	30 June 2026	Substantive and control-mapping review complete
Insurance practitioner	Qualified underwriting/claims leader	Open		Cross-line practitioner review required
Actuarial	Qualified actuary	Open		Validate actuarial terminology and examples
Legal/regulatory	Qualified counsel	Open		Jurisdiction-specific statements and notices
Cybersecurity / AI security	Qualified reviewer	Open		Threat and control interpretation
Standards editor	Qualified reviewer	Open		Normative language and cross-references

Revision history

Version	Date	Change	Owner
1.0	30 June 2026	Initial publication candidate: complete insurance-sector guide, verified 59-control mapping, workbook, templates, scenarios, source register and publication gates.	ODA3 Institute

Document hierarchy and precedence

- Applicable law and binding regulatory or supervisory direction.
- GAISSF-NOR-001 Framework Standard and other applicable GAISSF normative documents.
- Approved GAISSF interpretations and assessment rules.
- This informative sector guide.
- Organisational policies and procedures.

Where requirements conflict, the organisation should record the conflict, obtain qualified advice, escalate through governance, and preserve the rationale. Unresolved interpretation must not be silently converted into a control conclusion.

Normative language

SHALL and SHALL NOT appear only when quoting or accurately restating verified GAISST normative requirements. SHOULD indicates recommended sector practice; MAY indicates permission; CAN indicates capability or possibility. Conformity is determined against governing normative requirements, not this guide alone.

Executive summary

Insurance AI influences eligibility, price, coverage, claims, fraud investigation, reserving, catastrophe exposure, customer communication and operational resilience. The same model failure can therefore create policyholder harm, balance-sheet effects, conduct exposure and cyber loss. SEC-039 provides the operational layer between GAISST controls and insurance practice.

- Classify systems by decision authority, policyholder impact, financial consequence, reversibility, data sensitivity, scale and dependency concentration.
- Treat model risk, cybersecurity, actuarial validation, conduct risk, privacy and operational resilience as one evidence system.
- Retain accountability when models, data, platforms or decisions are outsourced.
- Make human oversight timely, competent, informed and authorised; ceremonial review is not effective oversight.
- Monitor outcomes, overrides, appeals, complaints, incidents, drift and vendor changes together.
- Preserve decision traceability sufficient to reconstruct material outcomes and support challenge.

1. Introduction

This guide supports insurers, reinsurers, brokers, insurtechs, third-party administrators and material service providers applying GAISST to insurance operations. It translates control objectives into sector interpretations, evidence and implementation patterns without creating new normative obligations.

1.1 How to use this guide

- Start with the system inventory and classification.
- Map applicable GAISST controls using the verified 59-control register.
- Select function-specific interpretations and evidence.
- Record legal, actuarial and jurisdiction-specific obligations separately.
- Use the workbook to assign owners, collect evidence and track remediation.
- Retain open issues and Notably Absent statements with the assessment record.

2. Scope

Included organisations: life, health, property and casualty, general, commercial and specialty insurers; reinsurers; brokers and distributors; insurtech platforms; TPAs; claims, underwriting, data and analytics providers. Included systems span predictive, generative, computer-vision, graph, optimisation, rules-plus-model and agentic systems across acquisition, development, procurement, deployment, operation, change and retirement.

Excluded: legal or actuarial opinions; product approval; rate filing decisions; insurance coverage interpretation; certification conclusions; universal numerical thresholds; and jurisdiction-specific applicability determinations.

3. Insurance operating context

Actor	Primary accountability	Typical AI dependency	Key evidence
Insurer	Policyholder outcomes, risk acceptance, claims, governance and compliance	Models, SaaS, data, decision engines	Inventory, approvals, validation, monitoring, incidents
Reinsurer	Portfolio exposure, treaty analytics and risk transfer	Catastrophe and accumulation models	Model/version records, assumptions, stress tests
Broker / agent	Advice, suitability, disclosure and submission quality	Recommendation and submission tools	Training, approved content, conversation records
TPA / claims provider	Operational claims handling within delegated authority	Triage, document, fraud and settlement tools	Authority matrix, QA, logs, escalation
Insurtech / vendor	Service security, model operation and contractual evidence	Hosted model/API/platform	Assurance, change notices, incident and subprocessor records
Data provider	Data provenance, quality, rights and update integrity	Enrichment, telematics, health, property and cyber data	Lineage, contracts, quality and correction records

Insurance decisions may have long-tail consequences. Errors can remain latent until claims emerge, portfolios mature or catastrophe events expose correlated assumptions. Legacy systems and rules engines can also materially alter model outputs; assessment scope should include the complete decision chain.

4. Sector risk landscape

Risk domain	Description	Impact pathways	GAISSF domains	Indicative evidence
Underwriting and pricing	Unstable or discriminatory risk classification, proxy effects, unapproved variables, model drift, historical-data bias and correlated portfolio errors.	Coverage denial, unaffordable pricing, adverse selection, underpricing, complaints and remediation.	D1, D6, D7, D8	Model inventory; feature approval; actuarial validation; subgroup analysis; drift reports; override logs.
Claims	Incorrect denial, suppression or prioritisation; fraud false positives; synthetic evidence; deepfakes; hallucinated summaries; automation bias.	Delayed or denied benefits, leakage, litigation, vulnerable-customer harm and operational backlog.	D1, D2, D5, D6, D7	Decision trace; evidence integrity checks; manual-review criteria; appeal records; outcome monitoring.
Policyholder and consumer harm	Unfair treatment, inadequate notice or explanation, inaccessible appeal, misleading communications and vulnerable-customer impacts.	Financial exclusion, loss of trust, remediation, supervisory action and reputational damage.	D5, D6, D7, D8	Impact assessment; notices; explanation tests; accessibility review; complaint and appeal metrics.
Data	Weak provenance, inaccurate broker data, sensitive health or financial data misuse, retention failures, proxy variables and training-data rights.	Privacy harm, unreliable decisions, legal exposure, model contamination and rework.	D1, D4, D6, D7, D8	Data register; lineage; consent/purpose basis; quality controls; access logs; deletion evidence.
Cybersecurity and adversarial	Prompt injection, poisoning, evasion, extraction, API abuse, credential compromise, insider misuse and vendor compromise.	Fraud losses, data exfiltration, service disruption, manipulated decisions and IP loss.	D1, D2, D3, D4	Threat model; red-team results; IAM evidence; runtime telemetry; incident exercises; DLP records.
Model and decision	Poor specification, uncontrolled updates, non-reproducibility, overfitting, weak thresholds, rules/model interaction and unsupported overrides.	Systematic pricing or claims errors, reserving distortion and audit failure.	D1, D6, D8	Independent validation; model cards; version control; approval record; threshold rationale; rollback test.
Third-party ecosystem	Opaque vendor models, weak audit rights, subprocessor exposure, update risk, concentration and exit limitations.	Correlated failures, service outage, lock-in, evidentiary gaps and regulatory access problems.	D4, D6, D8	Due diligence; contract clauses; audit reports; dependency map; exit test; concentration assessment.
Prudential and systemic	Common model/vendor concentration, tail-risk underestimation, catastrophe-model dependency, cyber accumulation and claims surge.	Capital, reserving, liquidity, reinsurance dispute and sector-wide operational impacts.	D4, D6, D8	Scenario analysis; accumulation map; stress test; board risk appetite; contingency and reinsurance review.

4.1 Underwriting and pricing

Unstable or discriminatory risk classification, proxy effects, unapproved variables, model drift, historical-data bias and correlated portfolio errors. Affected functions should assess business, policyholder, security, compliance and prudential consequences separately. Typical impacts include coverage denial, unaffordable pricing, adverse selection, underpricing, complaints and remediation.

Control focus: D1, D6, D7, D8. Evidence: Model inventory; feature approval; actuarial validation; subgroup analysis; drift reports; override logs.

Limitations: risk likelihood and materiality are entity-, product-, portfolio- and jurisdiction-specific; examples are not exhaustive safe harbours.

4.2 Claims

Incorrect denial, suppression or prioritisation; fraud false positives; synthetic evidence; deepfakes; hallucinated summaries; automation bias. Affected functions should assess business, policyholder, security, compliance and prudential consequences separately. Typical impacts include delayed or denied benefits, leakage, litigation, vulnerable-customer harm and operational backlog.

Control focus: D1, D2, D5, D6, D7. Evidence: Decision trace; evidence integrity checks; manual-review criteria; appeal records; outcome monitoring.

Limitations: risk likelihood and materiality are entity-, product-, portfolio- and jurisdiction-specific; examples are not exhaustive safe harbours.

4.3 Policyholder and consumer harm

Unfair treatment, inadequate notice or explanation, inaccessible appeal, misleading communications and vulnerable-customer impacts. Affected functions should assess business, policyholder, security, compliance and prudential consequences separately. Typical impacts include financial exclusion, loss of trust, remediation, supervisory action and reputational damage.

Control focus: D5, D6, D7, D8. Evidence: Impact assessment; notices; explanation tests; accessibility review; complaint and appeal metrics.

Limitations: risk likelihood and materiality are entity-, product-, portfolio- and jurisdiction-specific; examples are not exhaustive safe harbours.

4.4 Data

Weak provenance, inaccurate broker data, sensitive health or financial data misuse, retention failures, proxy variables and training-data rights. Affected functions should assess business, policyholder, security, compliance and prudential consequences separately. Typical impacts include privacy harm, unreliable decisions, legal exposure, model contamination and rework.

Control focus: D1, D4, D6, D7, D8. Evidence: Data register; lineage; consent/purpose basis; quality controls; access logs; deletion evidence.

Limitations: risk likelihood and materiality are entity-, product-, portfolio- and jurisdiction-specific; examples are not exhaustive safe harbours.

4.5 Cybersecurity and adversarial

Prompt injection, poisoning, evasion, extraction, API abuse, credential compromise, insider misuse and vendor compromise. Affected functions should assess business, policyholder, security, compliance and prudential consequences separately. Typical impacts include fraud losses, data exfiltration, service disruption, manipulated decisions and ip loss.

Control focus: D1, D2, D3, D4. Evidence: Threat model; red-team results; IAM evidence; runtime telemetry; incident exercises; DLP records.

Limitations: risk likelihood and materiality are entity-, product-, portfolio- and jurisdiction-specific; examples are not exhaustive safe harbours.

4.6 Model and decision

Poor specification, uncontrolled updates, non-reproducibility, overfitting, weak thresholds, rules/model interaction and unsupported overrides. Affected functions should assess business, policyholder, security, compliance and prudential consequences separately. Typical impacts include systematic pricing or claims errors, reserving distortion and audit failure.

Control focus: D1, D6, D8. Evidence: Independent validation; model cards; version control; approval record; threshold rationale; rollback test.

Limitations: risk likelihood and materiality are entity-, product-, portfolio- and jurisdiction-specific; examples are not exhaustive safe harbours.

4.7 Third-party ecosystem

Opaque vendor models, weak audit rights, subprocessor exposure, update risk, concentration and exit limitations. Affected functions should assess business, policyholder, security, compliance and prudential consequences separately. Typical impacts include correlated failures, service outage, lock-in, evidentiary gaps and regulatory access problems.

Control focus: D4, D6, D8. Evidence: Due diligence; contract clauses; audit reports; dependency map; exit test; concentration assessment.

Limitations: risk likelihood and materiality are entity-, product-, portfolio- and jurisdiction-specific; examples are not exhaustive safe harbours.

4.8 Prudential and systemic

Common model/vendor concentration, tail-risk underestimation, catastrophe-model dependency, cyber accumulation and claims surge. Affected functions should assess business, policyholder, security, compliance and prudential consequences separately. Typical impacts include capital, reserving, liquidity, reinsurance dispute and sector-wide operational impacts.

Control focus: D4, D6, D8. Evidence: Scenario analysis; accumulation map; stress test; board risk appetite; contingency and reinsurance review.

Limitations: risk likelihood and materiality are entity-, product-, portfolio- and jurisdiction-specific; examples are not exhaustive safe harbours.

5. Insurance AI system classification

Class	Decision / impact profile	Examples	Minimum governance response
Low-impact assistive	No direct adverse decision; reversible; low sensitivity	Drafting internal text or summarising non-sensitive material	Standard access, logging, output review and acceptable-use controls.
Material operational	Supports important workflow or material volumes	Claims document classification; broker submission extraction	Formal owner, validation, monitoring, fallback and change control.
High-impact policyholder decision	Influences eligibility, price, coverage, claim or adverse action	Life underwriting score; claim denial recommendation	Independent validation, fairness testing, meaningful human review, explanation and appeal.
Prudentially significant	Can materially affect reserves, capital, accumulation or reinsurance	Catastrophe aggregation or reserving support	Actuarial and risk validation, stress testing, concentration analysis and board oversight.
Critical claims or underwriting	Failure creates immediate large-scale customer or operational harm	Automated claims triage during catastrophe event	Resilience, manual fallback, surge testing, incident playbook and executive escalation.

Classification is an implementation aid. It does not replace GAISST applicability rules or any legal definition of high-risk AI. Escalate classification where one factor is extreme even if other factors are moderate.

6. Control interpretation by insurance function

Function	AI use	Key risks	GAISST domain	Implementation	Evidence	Human oversight	Notably absent
Underwriting	Risk selection and coverage recommendation	Proxy discrimination, drift, manipulation, weak explainability	D1, D6, D7	Feature governance, actuarial validation, adverse-decision review	Model validation, feature register, override log	Mandatory for adverse or borderline outcomes	No safe-harbour assumption that model approval establishes lawfulness, actuarial adequacy or rate-filing compliance in every jurisdiction.
Pricing	Premium or discount recommendation	Unapproved variables, unfair differentiation, optimisation instability	D1, D6, D7, D8	Rate governance, subgroup and stability tests, filing alignment	Pricing test pack, approval, monitoring	Required for material exceptions and adverse outcomes	No assumption that predictive accuracy establishes actuarial fairness, filing acceptability or absence of proxy discrimination.

SEC-039 | GAISSTTM Insurance Sector Implementation Guide | v1.0

Function	AI use	Key risks	GAISST domain	Implementation	Evidence	Human oversight	Notably absent
Claims	Triage, estimation, settlement or denial support	Deepfakes, false negatives, hallucinations, automation bias	D1, D2, D5, D7	Evidence integrity, confidence thresholds, escalation and appeals	Decision trace, image checks, review record	Mandatory for denial, vulnerability and high value	No assumption that a fraud flag proves fraud, or that automated triage may deny, suppress or delay a claim without effective review and contestability.
Fraud detection	Fraud score or investigation prioritisation	False positives, evasion, bias, feedback loops	D1, D2, D7	Adaptive testing, investigator review, outcome feedback controls	Precision/recall, subgroup results, case outcomes	Investigator confirmation before adverse action	No safe-harbour assumption; legal and actuarial applicability remains separate.
Reserving	Reserve estimation support	Tail error, regime shift, opaque assumptions	D1, D6, D8	Actuarial ownership, scenario testing, reconciliation	Validation report, assumptions, back-testing	Actuarial sign-off	No assumption that model validation removes tail, accumulation, capital, accounting or reinsurance risk.
Catastrophe modelling	Exposure and loss estimation	Vendor concentration, climate shift, tail underestimation	D1, D4, D6, D8	Model plurality, version governance, stress and dependency analysis	Vendor evidence, model-change assessment, stress results	Expert review for material capital/reinsurance use	No assumption that model validation removes tail, accumulation, capital, accounting or reinsurance risk.
Policy administration	Data extraction and workflow automation	Record corruption, unauthorised changes, privacy leakage	D2, D3, D6	Transaction controls, segregation, reconciliation, rollback	Audit trail, access record, reconciliation	Approval for policy-changing actions	No safe-harbour assumption; legal and actuarial applicability remains separate.
Distribution and intermediary support	Agent recommendations and sales support	Mis-selling, unsuitable recommendations, prompt leakage	D3, D5, D7	Approved knowledge, suitability checks, constrained tools	Conversation logs, content tests, complaint data	Human agent accountability retained	No safe-harbour assumption; legal and actuarial applicability remains separate.
Customer service	Chatbot or virtual assistant	Hallucinated coverage, misleading advice, accessibility failure	D2, D5, D7	Grounding, disclaimers, escalation, transcript retention	Evaluation set, escalation metrics, transcripts	Human handoff for disputes and material decisions	No safe-harbour assumption; legal and actuarial applicability remains separate.
Reinsurance	Portfolio analytics and treaty support	Data mismatch, concentration, reporting error	D1, D4, D6, D8	Data reconciliation, dependency mapping, expert validation	Reconciliation, model inventory, approval	Specialist review for treaty/capital decisions	No safe-harbour assumption; legal and actuarial applicability remains separate.
Cyber-insurance	Security posture scoring and accumulation analysis	Gaming, stale signals, correlated vendor risk	D1, D4, D6, D8	Signal provenance, adversarial testing, accumulation scenarios	Data lineage, red-team, scenario report	Underwriter review	No safe-harbour assumption; legal and actuarial applicability remains separate.
Health and life insurance	Mortality, morbidity or care-related decision support	Sensitive data, proxy discrimination, irreversible harm	D1, D6, D7, D8	Strict data governance, clinical/actuarial input, contestability	DPIA, fairness analysis, review record	Mandatory qualified human review	No safe-harbour assumption; legal and actuarial applicability remains separate.
Telematics and IoT	Behaviour-based risk and loss prevention	Sensor spoofing, surveillance, physical safety	D1, D2, D7, D9	Device security, consent, calibration, fallback	Device inventory, security tests, consent records	Review where data materially changes price/coverage	No safe-harbour assumption; legal and actuarial applicability remains separate.

Function	AI use	Key risks	GAISF domain	Implementation	Evidence	Human oversight	Notably absent
Generative AI	Drafting, summarisation, retrieval and agentic workflow	Prompt injection, hallucination, leakage, unsafe tools	D2, D3, D5	RAG controls, tool allowlists, output validation, DLP	Prompt tests, retrieval logs, red-team results	Required for external or decision-relevant output	No provider assurance treated as a substitute for insurer testing, output controls, traceability and human accountability.
Internal corporate use	Productivity and analysis	Confidentiality leakage, shadow AI, inaccurate work product	D2, D4, D6	Approved tools, data classification, usage logging, training	Acceptable-use records, DLP, inventory	Reviewer accountable for work product	No safe-harbour assumption; legal and actuarial applicability remains separate.

7. Governance and accountability

Accountability remains with the insurance entity and accountable business owner. Outsourcing changes evidence sources, not accountability. Governance should integrate board risk appetite, executive ownership, actuarial and model validation, CISO controls, compliance/conduct review, privacy, procurement, resilience and internal audit.

Decision	Accountable	Consulted / responsible	Escalation
System approval	Business owner	AI governance, CISO, model risk, compliance	Board/committee for material systems
Risk classification	AI governance	Business, model risk, legal, actuarial	CRO
Data approval	Data owner	Privacy, security, actuarial/model risk	AI governance
Model validation	Independent validation / actuarial	CISO, business owner	CRO / validation committee
Security testing	CISO	Engineering, vendor, red team	AI governance
Deployment approval	Business owner	CISO, model risk, compliance, operations	Executive committee for critical systems
Monitoring	System owner	Model risk, claims/underwriting, security	CRO
Incident escalation	Incident commander	Legal, compliance, business, privacy	Executive / board by severity
Customer notification	Compliance / legal	Claims or product owner	Accountable executive
Model retirement	System owner	Records, vendor, security, business continuity	AI governance

8. Human oversight

Meaningful oversight exists only where the reviewer acts before harm becomes irreversible, has relevant competence and contextual information, can disagree without penalty, can access source evidence, and has authority and time to intervene. A nominal approval click, post-event sampling or blind reliance on a confidence score is ceremonial oversight.

Trigger	Oversight model	Reviewer	Required record
Coverage denial or material exclusion	Human-in-command	Qualified underwriter / claims decision-maker	Sources, model output, rationale, alternative considered, approval
High-value or vulnerable claimant	Mandatory manual review	Senior claims professional	Vulnerability and escalation record
Fraud flag causing adverse action	Human-in-the-loop	Trained investigator	Evidence reviewed, disposition, feedback label
Medical/health-related decision	Qualified human review	Appropriate clinical/actuarial/claims professional	Competence, sources, rationale, appeal route
Agentic action affecting policy/claim	Dual approval or constrained authority	Business owner and control function	Tool calls, authority, approvals, rollback

9. Data governance

The data register should identify source, owner, legal basis or permitted purpose, provenance, sensitivity, quality controls, known limitations, protected-characteristic or proxy risk, update frequency, retention and downstream use. Broker-submitted and third-party enrichment data require correction and challenge mechanisms.

Data ID	Source	Use	Sensitivity	Provenance / rights	Quality controls	Proxy risk	Retention	Owner
DATA-001	Policy administration system	Underwriting history	Confidential personal	Internal authoritative record	Completeness and reconciliation	Geography and occupation	Per records schedule	Data owner
DATA-002	Telematics provider	Behaviour-based pricing	Location / behavioural	Contract and device lineage	Calibration, freshness, spoofing checks	Socioeconomic and disability	Purpose-limited	Product owner

10. Security architecture

Reference architecture: identity-aware channels feed an API gateway and policy enforcement layer; input validation, malware/media integrity and prompt-injection controls precede model or decision services; retrieval is isolated by tenant, purpose and access; tools are allowlisted with least privilege and transaction limits; outputs pass confidence, policy, safety and data-loss checks; material decisions are recorded with model, prompt, data, rule, reviewer and outcome identifiers; telemetry feeds security, model-risk and business-outcome monitoring; tested manual fallback supports critical operations.

- Separate development, validation and production environments.
- Protect model registries, prompts, retrieval corpora, rules, thresholds and secrets as controlled assets.
- Use strong identity, privileged-access management, segmentation, encryption, key management, API security and immutable logging.
- Test backup, rollback, provider outage, manual fallback and catastrophe surge procedures.
- Detect unauthorised AI use and prevent sensitive data exfiltration through DLP and approved-tool controls.

11. Model validation and testing

Test family	Insurance focus	Evidence
Independent validation	Fitness for use, assumptions, data, reproducibility and limitations	Validation report and issue closure
Actuarial validation	Rate, reserve, mortality, morbidity, severity or frequency relevance	Actuarial review and sign-off
Security / adversarial	Poisoning, evasion, extraction, prompt injection, abuse and tool misuse	Threat model, test cases and remediation
Fairness / outcome	Subgroups, proxies, adverse outcomes and vulnerable customers	Defined metrics, rationale, limitations and actions
Stress / scenario	Regime shift, catastrophe surge, vendor outage and tail events	Scenario design, results and decision record
Operational acceptance	Latency, capacity, integration, rollback and manual fallback	UAT, resilience and fallback test

Universal numerical thresholds are intentionally absent. Thresholds should be justified against use, harm severity, legal requirements, portfolio characteristics, baseline performance and escalation capacity.

12. Monitoring and change management

Metric / change	Frequency	Owner	Escalation approach
Performance and calibration	Risk-based; at least per approved monitoring plan	Model owner	Deviation from approved tolerance or unexplained trend
Fairness and adverse outcomes	Aligned to decision volume and harm	Compliance / model risk	Material subgroup disparity or deterioration
Overrides, appeals and complaints	Monthly or more frequently for high-impact uses	Business owner	Concentration, reversal trend or vulnerable-customer signal
Security events and abuse	Continuous where technically feasible	CISO	Confirmed compromise, injection, exfiltration or privilege misuse
Vendor/model update	Before acceptance and after material change	Vendor owner	Unassessed change, regression or evidence gap
Data/feature change	Before production	Data/model owner	Lineage, rights, quality or proxy-risk change

13. Incident management

Severity	Policyholder / financial impact	Examples	Escalation	Evidence preservation
S1 Critical	Widespread or severe harm; material financial/prudential impact	Systemic denial/pricing error, major breach, critical claims outage	Immediate executive, legal, regulator-assessment and board escalation	Freeze versions, logs, data, rules, prompts, communications and decisions
S2 High	Material cohort or product impact	Discriminatory outcome, vendor compromise, material claim error	Incident command and senior control functions	Preserve decision and vendor evidence
S3 Moderate	Limited reversible impact	Local drift, contained data exposure, repeat hallucination	Owner and control-function remediation	Retain samples, root cause and closure
S4 Low	No material external impact	Near miss or minor control deviation	Normal issue management	Document lesson and control update

Notification timeframes are jurisdiction-specific and intentionally not stated as universal rules. The legal/regulatory assessment should identify applicable clocks and triggering facts.

14. Third-party and supply-chain management

- Assess provider security, model documentation, data rights, validation, subcontractors, incident history, resilience, geographic processing and regulatory access before contract.
- Contract for change notice, audit/access rights, incident notification, evidence retention, secure deletion, continuity, portability, exit support and material subprocessor control.
- Map fourth parties and concentration across cloud, foundation models, catastrophe models, data and claims services.
- Test exit and fallback; a contractual right without operational feasibility is weak evidence.

15. Policyholder transparency, explanation and contestability

Notices and explanations should match the decision, audience and harm. They should identify the material basis of the outcome, meaningful factors, applicable limitations, correction and appeal routes, and whether qualified human review is available. Trade-secret or security constraints may limit technical detail but do not remove the need for a meaningful, lawful explanation.

16. Assurance and evidence catalogue

Evidence	Category	Purpose	Owner	Source	Retention	Control linkage	Reliability	Common deficiency
Approved AI policy, risk appetite and committee decisions	Governance	Demonstrate design and operating effectiveness	Board / CRO	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Approver authority, approval date, challenge record and exception completeness.	Generic policy without system-level operating evidence
System classification and impact assessment	Risk	Demonstrate design and operating effectiveness	AI governance	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Prefer T1 operating evidence; corroborate with T2 independent review and T3 simulation. T4 evidence is supplementary only.	Generic policy without system-level operating evidence

SEC-039 | GAISSTTM Insurance Sector Implementation Guide | v1.0

Evidence	Category	Purpose	Owner	Source	Retention	Control linkage	Reliability	Common deficiency
Lineage, rights, quality and proxy analysis	Data	Demonstrate design and operating effectiveness	Data owner	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Source quality, rights, lineage completeness, validation status and operating period.	Generic policy without system-level operating evidence
Model card, validation, limitations and version history	Model	Demonstrate design and operating effectiveness	Model risk	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Validation independence, test coverage, version linkage and documented limitations.	Generic policy without system-level operating evidence
Threat model, tests, IAM and runtime telemetry	Security	Demonstrate design and operating effectiveness	CISO	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Testing currency, scope, independence and linkage to the production configuration.	Generic policy without system-level operating evidence
Approval, release, configuration and rollback evidence	Deployment	Demonstrate design and operating effectiveness	System owner	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Prefer T1 operating evidence; corroborate with T2 independent review and T3 simulation. T4 evidence is supplementary only.	Generic policy without system-level operating evidence
Performance, outcomes, drift, complaints and overrides	Monitoring	Demonstrate design and operating effectiveness	Business / model owner	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Prefer T1 operating evidence; corroborate with T2 independent review and T3 simulation. T4 evidence is supplementary only.	Generic policy without system-level operating evidence
Timeline, containment, impact, notification and lessons	Incident	Demonstrate design and operating effectiveness	Incident commander	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Completeness, timeliness, preserved evidence, root cause and remediation closure.	Generic policy without system-level operating evidence

Evidence	Category	Purpose	Owner	Source	Retention	Control linkage	Reliability	Common deficiency
Due diligence, contract, assurance and change records	Vendor	Demonstrate design and operating effectiveness	Third-party risk	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Prefer T1 operating evidence; corroborate with T2 independent review and T3 simulation. T4 evidence is supplementary only.	Generic policy without system-level operating evidence
Reviewer competence, intervention and override records	Oversight	Demonstrate design and operating effectiveness	Business owner	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Reviewer competence, timing, authority and record completeness.	Generic policy without system-level operating evidence
Notices, explanations, appeals and accessibility tests	Policyholder	Demonstrate design and operating effectiveness	Compliance	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Prefer T1 operating evidence; corroborate with T2 independent review and T3 simulation. T4 evidence is supplementary only.	Generic policy without system-level operating evidence
Testing, findings, remediation and limitations	Audit	Demonstrate design and operating effectiveness	Internal audit	Authoritative system or signed record	Risk-based; preserve applicable legal hold	Relevant mapped controls	Prefer T1 operating evidence; corroborate with T2 independent review and T3 simulation. T4 evidence is supplementary only.	Generic policy without system-level operating evidence

17. Insurance implementation profiles

Profile	Operating model	Priority controls	Constraints
Large composite insurer	Multiple lines, jurisdictions and legacy platforms	Portfolio inventory, federated governance, concentration and shared-service controls	Fragmented ownership and evidence
Life insurer	Long-duration products and sensitive mortality/health data	Underwriting fairness, actuarial validation, long-tail drift and contestability	Sparse outcomes and legacy assumptions
Property and casualty insurer	High-volume claims, images, catastrophe and telematics	Claims integrity, surge resilience, computer vision and accumulation	Catastrophe regime shift and vendor concentration
Health insurer	Sensitive data and high-impact benefit decisions	Purpose limitation, qualified review, fairness, explanation and appeal	Clinical context and jurisdictional complexity
Reinsurer	Portfolio aggregation, catastrophe and treaty analytics	Model plurality, concentration, assumptions and stress testing	Opaque cedant data and common-model dependency
Insurtech / digital insurer	Cloud-native, vendor-heavy and rapid change	Secure SDLC, third-party controls, monitoring and evidence automation	Resource constraints and dependency lock-in

18. Practical implementation roadmap

Phase	Indicative timeframe	Objective	Activities	Exit evidence
Phase 0	0-30 days	Mobilisation and scope	Sponsor, owner, boundaries, sources, approval gates	Charter and scoped plan
Phase 1	30-60 days	Inventory and classification	Systems, models, data, vendors, decision authority and impact	Approved inventory and tiers
Phase 2	60-100 days	Risk and control mapping	Map 59 controls, obligations, evidence and gaps	Statement of applicability and gap register
Phase 3	100-180 days	Remediation and governance	Implement priority technical, process and contractual controls	Closed critical gaps and operating evidence
Phase 4	180-240 days	Validation and assurance	Independent validation, red team, fairness, resilience and audit	Assurance report with limitations
Phase 5	Ongoing	Operational monitoring	Outcomes, drift, incidents, complaints, vendor and change monitoring	Dashboards and issue records
Phase 6	6-12 months	Continuous improvement	Thematic review, concentration, lessons and maturity	Improvement plan and readiness decision

19. Worked scenarios

19.1 AI-assisted life insurance underwriting

Element	Implementation interpretation
Context	Applicant data, medical and financial indicators support risk classification.
Threats and failure modes	Proxy discrimination; sensitive-data misuse; drift; opaque adverse decisions.
Control interpretation	Independent actuarial/model validation; restricted features; subgroup testing; meaningful underwriter review; explanation and appeal evidence.
Required evidence	System classification; data lineage; threat model; validation; approval; monitoring; oversight and incident records proportionate to risk.
Monitoring	Performance, outcomes, overrides, complaints, incidents, vendor/model changes and drift.
Incident triggers	Material decision error, security compromise, unexplained disparity, loss of traceability, vendor change or failure of manual fallback.
Residual risks	Data limitations, regime shift, human error, unknown attacks and jurisdiction-specific obligations remain.
Notably absent	No assumption that model approval establishes lawfulness or actuarial adequacy in every jurisdiction.

19.2 Automated motor claims triage

Element	Implementation interpretation
Context	Images and claim data prioritise cases and estimate complexity.
Threats and failure modes	Adversarial images; deepfakes; misclassification; catastrophe surge failure.
Control interpretation	Media integrity checks; confidence thresholds; surge testing; high-value/vulnerable escalation; manual fallback.
Required evidence	System classification; data lineage; threat model; validation; approval; monitoring; oversight and incident records proportionate to risk.
Monitoring	Performance, outcomes, overrides, complaints, incidents, vendor/model changes and drift.
Incident triggers	Material decision error, security compromise, unexplained disparity, loss of traceability, vendor change or failure of manual fallback.
Residual risks	Data limitations, regime shift, human error, unknown attacks and jurisdiction-specific obligations remain.
Notably absent	No autonomous denial based solely on triage output.

19.3 Fraud detection using network analytics

Element	Implementation interpretation
Context	Graph analytics identify suspicious claimant, provider or broker relationships.
Threats and failure modes	False positives; feedback loops; evasion; group bias.
Control interpretation	Investigator confirmation; outcome feedback; precision/recall and subgroup monitoring; feature provenance.
Required evidence	System classification; data lineage; threat model; validation; approval; monitoring; oversight and incident records proportionate to risk.
Monitoring	Performance, outcomes, overrides, complaints, incidents, vendor/model changes and drift.
Incident triggers	Material decision error, security compromise, unexplained disparity, loss of traceability, vendor change or failure of manual fallback.

Element	Implementation interpretation
Residual risks	Data limitations, regime shift, human error, unknown attacks and jurisdiction-specific obligations remain.
Notably absent	A fraud flag is not proof of fraud.

19.4 Property damage assessment using computer vision

Element	Implementation interpretation
Context	Images estimate damage severity or repair scope.
Threats and failure modes	Image manipulation; poor generalisation; geographic bias; hidden damage.
Control interpretation	Capture controls; tamper detection; uncertainty reporting; adjuster review for material settlements.
Required evidence	System classification; data lineage; threat model; validation; approval; monitoring; oversight and incident records proportionate to risk.
Monitoring	Performance, outcomes, overrides, complaints, incidents, vendor/model changes and drift.
Incident triggers	Material decision error, security compromise, unexplained disparity, loss of traceability, vendor change or failure of manual fallback.
Residual risks	Data limitations, regime shift, human error, unknown attacks and jurisdiction-specific obligations remain.
Notably absent	No claim that image-only assessment is universally sufficient.

19.5 Health insurance decision support

Element	Implementation interpretation
Context	AI supports benefit, risk or utilisation decisions.
Threats and failure modes	Sensitive health data; discrimination; clinical context loss; irreversible harm.
Control interpretation	Strict purpose limitation; qualified human review; explanation; appeal; clinical and actuarial validation.
Required evidence	System classification; data lineage; threat model; validation; approval; monitoring; oversight and incident records proportionate to risk.
Monitoring	Performance, outcomes, overrides, complaints, incidents, vendor/model changes and drift.
Incident triggers	Material decision error, security compromise, unexplained disparity, loss of traceability, vendor change or failure of manual fallback.
Residual risks	Data limitations, regime shift, human error, unknown attacks and jurisdiction-specific obligations remain.
Notably absent	No medical advice or clinical approval is provided by this guide.

19.6 Dynamic or behaviour-based pricing

Element	Implementation interpretation
Context	Telematics or behavioural signals influence premium.
Threats and failure modes	Surveillance, consent limits, sensor spoofing, unfair differentiation.
Control interpretation	Signal provenance; device security; proxy analysis; customer notice; correction process.
Required evidence	System classification; data lineage; threat model; validation; approval; monitoring; oversight and incident records proportionate to risk.
Monitoring	Performance, outcomes, overrides, complaints, incidents, vendor/model changes and drift.
Incident triggers	Material decision error, security compromise, unexplained disparity, loss of traceability, vendor change or failure of manual fallback.
Residual risks	Data limitations, regime shift, human error, unknown attacks and jurisdiction-specific obligations remain.
Notably absent	No endorsement of legality or fairness of any variable.

19.7 Generative AI claims assistant

Element	Implementation interpretation
Context	LLM summarises evidence and drafts communications.
Threats and failure modes	Hallucination; prompt injection; confidential-data leakage; misleading coverage statements.
Control interpretation	Grounded retrieval; citation to source records; prohibited-action controls; human approval; transcript logging.
Required evidence	System classification; data lineage; threat model; validation; approval; monitoring; oversight and incident records proportionate to risk.
Monitoring	Performance, outcomes, overrides, complaints, incidents, vendor/model changes and drift.
Incident triggers	Material decision error, security compromise, unexplained disparity, loss of traceability, vendor change or failure of manual fallback.
Residual risks	Data limitations, regime shift, human error, unknown attacks and jurisdiction-specific obligations remain.
Notably absent	No direct claim denial or binding coverage interpretation without qualified review.

19.8 Cyber-insurance risk scoring

Element	Implementation interpretation
Context	External security telemetry and questionnaires support underwriting.
Threats and failure modes	Gaming; stale data; concentration; weak causal assumptions.
Control interpretation	Source assurance; freshness controls; adversarial testing; underwriter override; portfolio accumulation analysis.
Required evidence	System classification; data lineage; threat model; validation; approval; monitoring; oversight and incident records proportionate to risk.
Monitoring	Performance, outcomes, overrides, complaints, incidents, vendor/model changes and drift.
Incident triggers	Material decision error, security compromise, unexplained disparity, loss of traceability, vendor change or failure of manual fallback.
Residual risks	Data limitations, regime shift, human error, unknown attacks and jurisdiction-specific obligations remain.
Notably absent	No representation that a score predicts breach with certainty.

19.9 Catastrophe modelling dependency

Element	Implementation interpretation
Context	Vendor models inform aggregation, reinsurance and capital decisions.
Threats and failure modes	Vendor concentration; model change; tail underestimation; correlated market use.
Control interpretation	Multi-model challenge; change impact; stress/scenario testing; exit and continuity plan.
Required evidence	System classification; data lineage; threat model; validation; approval; monitoring; oversight and incident records proportionate to risk.
Monitoring	Performance, outcomes, overrides, complaints, incidents, vendor/model changes and drift.
Incident triggers	Material decision error, security compromise, unexplained disparity, loss of traceability, vendor change or failure of manual fallback.
Residual risks	Data limitations, regime shift, human error, unknown attacks and jurisdiction-specific obligations remain.
Notably absent	No assumption that vendor validation transfers accountability.

19.10 Third-party foundation model in customer service

Element	Implementation interpretation
Context	External model answers policyholder questions using approved knowledge.
Threats and failure modes	Provider update; retention; prompt injection; hallucinated coverage; outage.
Control interpretation	Contract controls; version monitoring; RAG isolation; evaluation; escalation; fallback.
Required evidence	System classification; data lineage; threat model; validation; approval; monitoring; oversight and incident records proportionate to risk.
Monitoring	Performance, outcomes, overrides, complaints, incidents, vendor/model changes and drift.
Incident triggers	Material decision error, security compromise, unexplained disparity, loss of traceability, vendor change or failure of manual fallback.
Residual risks	Data limitations, regime shift, human error, unknown attacks and jurisdiction-specific obligations remain.
Notably absent	No provider assurance treated as substitute for insurer testing.

20. Verified GAISSE control mapping

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	Protect insurance data, models, features and validation against poisoning, extraction, drift and adversarial manipulation.	Underwriting; pricing; claims; fraud; reserving; catastrophe modelling	Apply dataset provenance & poisoning prevention to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Data lineage, source contracts, feature approvals and poisoning controls; [T2] independent actuarial/ MRM validation; [T3] contaminated-data and proxy-variable tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D1-CTL-02	MODEL EXTRACTION RESISTANCE	Protect insurance data, models, features and validation against poisoning, extraction, drift and adversarial manipulation.	Underwriting; pricing; claims; fraud; reserving; catastrophe modelling	Apply model extraction resistance to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] API telemetry, rate limits and access logs; [T2] penetration-test report; [T3] model-extraction simulation.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D1-CTL-03	BEHAVIORAL DRIFT DETECTION	Protect insurance data, models, features and validation against poisoning, extraction, drift and adversarial manipulation.	Underwriting; pricing; claims; fraud; reserving; catastrophe modelling	Apply behavioral drift detection to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Automated drift/outcome logs and alerts; [T2] MRM or actuarial review; [T3] out-of-distribution and catastrophe-regime stress tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION	Protect insurance data, models, features and validation against poisoning, extraction, drift and adversarial manipulation.	Underwriting; pricing; claims; fraud; reserving; catastrophe modelling	Apply federated learning poisoning prevention to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D1-CTL-05	EMBEDDING SPACE ROBUSTNESS	Protect insurance data, models, features and validation against poisoning, extraction, drift and adversarial manipulation.	Underwriting; pricing; claims; fraud; reserving; catastrophe modelling	Apply embedding space robustness to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D1-CTL-06	POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING	Protect insurance data, models, features and validation against poisoning, extraction, drift and adversarial manipulation.	Underwriting; pricing; claims; fraud; reserving; catastrophe modelling	Apply post-quantum model signing & crypto hardening to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION	Protect insurance data, models, features and validation against poisoning, extraction, drift and adversarial manipulation.	Underwriting; pricing; claims; fraud; reserving; catastrophe modelling	Apply lora/adapter integrity verification to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D1-CTL-08	MODEL MERGE ATTACK DETECTION	Protect insurance data, models, features and validation against poisoning, extraction, drift and adversarial manipulation.	Underwriting; pricing; claims; fraud; reserving; catastrophe modelling	Apply model merge attack detection to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D1-CTL-09	QUANTIZATION BACKDOOR SCREENING	Protect insurance data, models, features and validation against poisoning, extraction, drift and adversarial manipulation.	Underwriting; pricing; claims; fraud; reserving; catastrophe modelling	Apply quantization backdoor screening to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D2-CTL-01	DIRECT PROMPT INJECTION PREVENTION	Secure production inference, APIs, prompts, retrieval, identities, logging, monitoring and runtime containment.	Claims platforms; customer portals; APIs; GenAI assistants; decision engines	Apply direct prompt injection prevention to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Input/output policy logs, tool-call traces and blocked-attempt telemetry; [T2] security review; [T3] direct, indirect and cross-agent injection tests.	CISO / Security Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D2-CTL-02	INDIRECT PROMPT INJECTION PREVENTION	Secure production inference, APIs, prompts, retrieval, identities, logging, monitoring and runtime containment.	Claims platforms; customer portals; APIs; GenAI assistants; decision engines	Apply indirect prompt injection prevention to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Input/output policy logs, tool-call traces and blocked-attempt telemetry; [T2] security review; [T3] direct, indirect and cross-agent injection tests.	CISO / Security Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D2-CTL-03	JAILBREAK RESISTANCE TESTING	Secure production inference, APIs, prompts, retrieval, identities, logging, monitoring and runtime containment.	Claims platforms; customer portals; APIs; GenAI assistants; decision engines	Apply jailbreak resistance testing to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] IAM, runtime, API and security telemetry; [T2] control-effectiveness review; [T3] attack, abuse and failover exercises.	CISO / Security Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D2-CTL-04	MULTI-MODAL INJECTION DEFENSE	Secure production inference, APIs, prompts, retrieval, identities, logging, monitoring and runtime containment.	Claims platforms; customer portals; APIs; GenAI assistants; decision engines	Apply multi-modal injection defense to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] IAM, runtime, API and security telemetry; [T2] control-effectiveness review; [T3] attack, abuse and failover exercises.	CISO / Security Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D2-CTL-05	FUNCTION CALL/TOOL CALL INJECTION PREVENTION	Secure production inference, APIs, prompts, retrieval, identities, logging, monitoring and runtime containment.	Claims platforms; customer portals; APIs; GenAI assistants; decision engines	Apply function call/tool call injection prevention to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Agent identity, delegation, tool-call and transaction logs; [T2] accountable-owner approval; [T3] loop, privilege and agent-to-agent authentication tests.	CISO / Security Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D2-CTL-06	CROSS-CONTEXT HIJACKING MITIGATION	Secure production inference, APIs, prompts, retrieval, identities, logging, monitoring and runtime containment.	Claims platforms; customer portals; APIs; GenAI assistants; decision engines	Apply cross-context hijacking mitigation to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] IAM, runtime, API and security telemetry; [T2] control-effectiveness review; [T3] attack, abuse and failover exercises.	CISO / Security Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D3-CTL-01	LEAST AGENCY ENFORCEMENT	Constrain delegated authority, tools, transactions and autonomous actions in claims, underwriting and customer operations.	Agentic claims; workflow automation; broker support; autonomous triage	Apply least agency enforcement to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	AI Governance / Business Owner	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D3-CTL-02	INTER-AGENT COMMUNICATION SECURITY	Constrain delegated authority, tools, transactions and autonomous actions in claims, underwriting and customer operations.	Agentic claims; workflow automation; broker support; autonomous triage	Apply inter-agent communication security to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Agent identity, delegation, tool-call and transaction logs; [T2] accountable-owner approval; [T3] loop, privilege and agent-to-agent authentication tests.	AI Governance / Business Owner	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D3-CTL-03	AGENTIC PROMPT CHAINING DETECTION	Constrain delegated authority, tools, transactions and autonomous actions in claims, underwriting and customer operations.	Agentic claims; workflow automation; broker support; autonomous triage	Apply agentic prompt chaining detection to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Agent identity, delegation, tool-call and transaction logs; [T2] accountable-owner approval; [T3] loop, privilege and agent-to-agent authentication tests.	AI Governance / Business Owner	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D3-CTL-04	EMBODIED AI SAFETY CONTROLS	Constrain delegated authority, tools, transactions and autonomous actions in claims, underwriting and customer operations.	Agentic claims; workflow automation; broker support; autonomous triage	Apply embodied ai safety controls to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	AI Governance / Business Owner	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D3-CTL-05	MULTI-AGENT TRUST CHAIN ATTESTATION	Constrain delegated authority, tools, transactions and autonomous actions in claims, underwriting and customer operations.	Agentic claims; workflow automation; broker support; autonomous triage	Apply multi-agent trust chain attestation to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Agent identity, delegation, tool-call and transaction logs; [T2] accountable-owner approval; [T3] loop, privilege and agent-to-agent authentication tests.	AI Governance / Business Owner	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION	Constrain delegated authority, tools, transactions and autonomous actions in claims, underwriting and customer operations.	Agentic claims; workflow automation; broker support; autonomous triage	Apply persistent memory exfiltration prevention to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	AI Governance / Business Owner	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D3-CTL-07	SECURE MEMORY LIFECYCLE MANAGEMENT	Constrain delegated authority, tools, transactions and autonomous actions in claims, underwriting and customer operations.	Agentic claims; workflow automation; broker support; autonomous triage	Apply secure memory lifecycle management to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	AI Governance / Business Owner	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSTTM Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D4-CTL-01	AI BILL OF MATERIALS (AI BOM) MAINTENANCE	Govern insurtech, cloud, data-broker, catastrophe-model, foundation-model and fourth-party dependencies.	All outsourced models, data, SaaS, cloud, TPA and reinsurer analytics	Apply ai bill of materials (ai bom) maintenance to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Due diligence, AI/SBOM, dependency map, contracts and incident/change notices; [T2] independent vendor assurance; [T3] exit, outage and concentration tests.	Head of Third-Party Risk / Procurement	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D4-CTL-02	MODEL FILE & ARTIFACT SCANNING	Govern insurtech, cloud, data-broker, catastrophe-model, foundation-model and fourth-party dependencies.	All outsourced models, data, SaaS, cloud, TPA and reinsurer analytics	Apply model file & artifact scanning to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals; [T2] independent review; [T3] controlled simulation/red-team evidence; [T4] vendor or industry claims only as supplementary context.	Head of Third-Party Risk / Procurement	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D4-CTL-03	MODEL HUB & REGISTRY VETTING	Govern insurtech, cloud, data-broker, catastrophe-model, foundation-model and fourth-party dependencies.	All outsourced models, data, SaaS, cloud, TPA and reinsurer analytics	Apply model hub & registry vetting to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	Head of Third-Party Risk / Procurement	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING	Govern insurtech, cloud, data-broker, catastrophe-model, foundation-model and fourth-party dependencies.	All outsourced models, data, SaaS, cloud, TPA and reinsurer analytics	Apply mcp server behavioral monitoring to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	Head of Third-Party Risk / Procurement	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT	Govern insurtech, cloud, data-broker, catastrophe-model, foundation-model and fourth-party dependencies.	All outsourced models, data, SaaS, cloud, TPA and reinsurer analytics	Apply third-party ai api security assessment to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Due diligence, AI/SBOM, dependency map, contracts and incident/change notices; [T2] independent vendor assurance; [T3] exit, outage and concentration tests.	Head of Third-Party Risk / Procurement	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	Govern insurtech, cloud, data-broker, catastrophe-model, foundation-model and fourth-party dependencies.	All outsourced models, data, SaaS, cloud, TPA and reinsurer analytics	Apply shadow ai discovery & governance to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	Head of Third-Party Risk / Procurement	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D4-CTL-07	AI SOFTWARE COMPOSITION ANALYSIS (SCA)	Govern insurtech, cloud, data-broker, catastrophe-model, foundation-model and fourth-party dependencies.	All outsourced models, data, SaaS, cloud, TPA and reinsurer analytics	Apply ai software composition analysis (sca) to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Due diligence, AI/SBOM, dependency map, contracts and incident/change notices; [T2] independent vendor assurance; [T3] exit, outage and concentration tests.	Head of Third-Party Risk / Procurement	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D5-CTL-01	HARMFUL CONTENT BLOCKING	Block, constrain and escalate hallucinated, misleading, unsafe or unauthorised outputs in policyholder communications, claims summaries, underwriting support and agent-facing content.	Customer communications; claim summaries; policy documents; recommendations	Apply harmful content blocking to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Output-policy configuration, blocked-output logs and complaint/correction records; [T2] conduct review; [T3] hallucination and harmful-content tests.	Conduct / Privacy / Legal / CISO, according to control	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D5-CTL-02	PII LEAKAGE PREVENTION	Prevent leakage of medical records, government identifiers, financial identifiers, claims data and telemetry through prompts, retrieval, generated outputs, logs and model-provider interfaces ; apply redaction and output inspection before disclosure .	Customer communications; claim summaries; policy documents; recommendations	Apply pii leakage prevention to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] DLP/redaction configuration, leakage alerts and disclosure logs; [T2] DPIA/privacy review; [T3] prompt, retrieval and output exfiltration tests.	Conduct / Privacy / Legal / CISO, according to control	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D5-CTL-03	COPYRIGHT DETECTION	Verify training, retrieval and reference-content provenance for generative underwriting and claims assistants ; detect unauthorised use of proprietary actuarial models, policy wordings, manuals and third-party copyrighted material.	Customer communications; claim summaries; policy documents; recommendations	Apply copyright detection to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Training/retrieval provenance, licences and content-match alerts; [T2] legal/IP review; [T3] proprietary-content ingestion tests.	Conduct / Privacy / Legal / CISO, according to control	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D5-CTL-04	AI WATERMARKING ROBUSTNESS	Apply provenance marking or watermarking where appropriate to insurer-generated synthetic media and communications, and operate detection and escalation pipelines for inbound deepfake or synthetically altered claims evidence.	Customer communications; claim summaries; policy documents; recommendations	Apply ai watermarking robustness to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Synthetic-media provenance, watermark configuration and detection alerts; [T2] communications/security review; [T3] watermark-removal and deepfake tests.	Conduct / Privacy / Legal / CISO, according to control	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION	Embed privacy requirements in insurance AI design, including purpose limitation, data minimisation, role-based access, retention, privacy testing and review of sensitive health, biometric, financial and telematics data.	Customer communications; claim summaries; policy documents; recommendations	Apply privacy-by-design verification to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Privacy requirements, data-flow map, minimisation/retention controls and technique parameters; [T2] DPIA or independent privacy validation; [T3] re-identification, inference and utility tests.	Conduct / Privacy / Legal / CISO, according to control	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION	Validate privacy-preserving techniques used in distributed or sensitive insurance analytics, including re-identification, inference and utility testing; do not assume anonymisation, federation or synthetic data eliminates privacy risk.	Customer communications; claim summaries; policy documents; recommendations	Apply privacy-preserving ml validation to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Privacy requirements, data-flow map, minimisation/retention controls and technique parameters; [T2] DPIA or independent privacy validation; [T3] re-identification, inference and utility tests.	Conduct / Privacy / Legal / CISO, according to control	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	Establish accountable governance, classification, documentation, oversight, assurance and lifecycle decisions.	Enterprise governance; model risk; actuarial; security; audit	Apply human-in-the-loop for high-risk actions to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Governance approvals, accountable-owner register and exceptions; [T2] second-line challenge; [T3] governance tabletop and decision reconstruction.	Board / CRO / AI Governance	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D6-CTL-02	AUDIT TRAIL COMPLETENESS	Establish accountable governance, classification, documentation, oversight, assurance and lifecycle decisions.	Enterprise governance; model risk; actuarial; security; audit	Apply audit trail completeness to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Governance approvals, accountable-owner register and exceptions; [T2] second-line challenge; [T3] governance tabletop and decision reconstruction.	Board / CRO / AI Governance	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D6-CTL-03	AI MODEL CARD COMPLETENESS	Establish accountable governance, classification, documentation, oversight, assurance and lifecycle decisions.	Enterprise governance; model risk; actuarial; security; audit	Apply ai model card completeness to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Governance approvals, accountable-owner register and exceptions; [T2] second-line challenge; [T3] governance tabletop and decision reconstruction.	Board / CRO / AI Governance	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D6-CTL-04	AI INCIDENT RESPONSE READINESS	Establish accountable governance, classification, documentation, oversight, assurance and lifecycle decisions.	Enterprise governance; model risk; actuarial; security; audit	Apply ai incident response readiness to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Governance approvals, accountable-owner register and exceptions; [T2] second-line challenge; [T3] governance tabletop and decision reconstruction.	Board / CRO / AI Governance	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D6-CTL-05	MODEL DEPRECIATION & DECOMMISSIONING	Establish accountable governance, classification, documentation, oversight, assurance and lifecycle decisions.	Enterprise governance; model risk; actuarial; security; audit	Apply model depreciation & decommissioning to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Governance approvals, accountable-owner register and exceptions; [T2] second-line challenge; [T3] governance tabletop and decision reconstruction.	Board / CRO / AI Governance	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	Establish accountable governance, classification, documentation, oversight, assurance and lifecycle decisions.	Enterprise governance; model risk; actuarial; security; audit	Apply third-party ai vendor governance to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Due diligence, AI/SBOM, dependency map, contracts and incident/change notices; [T2] independent vendor assurance; [T3] exit, outage and concentration tests.	Board / CRO / AI Governance	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY	Establish accountable governance, classification, documentation, oversight, assurance and lifecycle decisions.	Enterprise governance; model risk; actuarial; security; audit	Apply ai resilience & business continuity to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Recovery plans, fallback evidence and availability telemetry; [T2] resilience review; [T3] catastrophe-surge, outage and manual-fallback exercise.	Board / CRO / AI Governance	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D7-CTL-H01	AI-GENERATED PHISHING SIMULATION	Prevent discriminatory, privacy-invasive, deceptive or otherwise harmful policyholder and workforce outcomes.	Underwriting; pricing; claims; marketing; health and life decisions	Apply ai-generated phishing simulation to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Training, outcome and incident records; [T2] conduct/human-risk review; [T3] deepfake, phishing or harm simulation .	Compliance / Conduct / Privacy	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D7-CTL-H02	DEEFAKE DETECTION TRAINING	Prevent discriminatory, privacy-invasive, deceptive or otherwise harmful policyholder and workforce outcomes.	Underwriting; pricing; claims; marketing; health and life decisions	Apply deepfake detection training to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Training, outcome and incident records; [T2] conduct/human-risk review; [T3] deepfake, phishing or harm simulation .	Compliance / Conduct / Privacy	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D7-CTL-H03	OUT-OF-BAND AUTHENTICATION	Prevent discriminatory, privacy-invasive, deceptive or otherwise harmful policyholder and workforce outcomes.	Underwriting; pricing; claims; marketing; health and life decisions	Apply out-of-band authentication to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Training, outcome and incident records; [T2] conduct/human-risk review; [T3] deepfake, phishing or harm simulation	Compliance / Conduct / Privacy	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D7-CTL-H04	AI SOCIAL ENGINEERING IR	Prevent discriminatory, privacy-invasive, deceptive or otherwise harmful policyholder and workforce outcomes.	Underwriting; pricing; claims; marketing; health and life decisions	Apply ai social engineering ir to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Training, outcome and incident records; [T2] conduct/human-risk review; [T3] deepfake, phishing or harm simulation	Compliance / Conduct / Privacy	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D7-CTL-H05	AI-ENHANCED EXTERNAL ATTACK DEFENSE	Prevent discriminatory, privacy-invasive, deceptive or otherwise harmful policyholder and workforce outcomes.	Underwriting; pricing; claims; marketing; health and life decisions	Apply ai-enhanced external attack defense to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Training, outcome and incident records; [T2] conduct/human-risk review; [T3] deepfake, phishing or harm simulation	Compliance / Conduct / Privacy	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D8-CTL-01	EU AI ACT RISK TIER MAPPING	Maintain legal, regulatory, records, incident, resilience and jurisdiction-specific obligation management.	Compliance; records; operational resilience; incident reporting; privacy	Apply eu ai act risk tier mapping to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D8-CTL-02	ISO 42001 GAP ANALYSIS	Maintain legal, regulatory, records, incident, resilience and jurisdiction-specific obligation management.	Compliance; records; operational resilience; incident reporting; privacy	Apply iso 42001 gap analysis to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D8-CTL-03	GPAI TECHNICAL DOCUMENTATION VERIFICATION	Maintain legal, regulatory, records, incident, resilience and jurisdiction-specific obligation management.	Compliance; records; operational resilience; incident reporting; privacy	Apply gpai technical documentation verification to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	Maintain legal, regulatory, records, incident, resilience and jurisdiction-specific obligation management.	Compliance; records; operational resilience; incident reporting; privacy	Apply dora ict incident reporting (financial sector) to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D8-CTL-05	NIST SP 800-218A COMPLIANCE CHECK	Maintain legal, regulatory, records, incident, resilience and jurisdiction-specific obligation management.	Compliance; records; operational resilience; incident reporting; privacy	Apply nist sp 800-218a compliance check to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Versioned model/data records and monitoring logs; [T2] independent MRM/Appointed Actuary validation; [T3] adversarial, stress and challenge r-model tests.	Chief Actuary / Head of Model Risk	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D9-CTL-01	PHYSICAL HARM BOUNDARY ENFORCEMENT	Apply physical-AI safeguards where telematics, IoT, drones, vehicles, sensors or robotic inspection affect insured risks.	Telematics; IoT; drones; image inspection; connected devices	Apply physical harm boundary enforcement to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	Engineering / Safety / Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D9-CTL-02	SAFE STATE AND GRACEFUL DEGRADATION	Apply physical-AI safeguards where telematics, IoT, drones, vehicles, sensors or robotic inspection affect insured risks.	Telematics; IoT; drones; image inspection; connected devices	Apply safe state and graceful degradation to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	Engineering / Safety / Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP	Apply physical-AI safeguards where telematics, IoT, drones, vehicles, sensors or robotic inspection affect insured risks.	Telematics; IoT; drones; image inspection; connected devices	Apply human override and emergency stop to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	Engineering / Safety / Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

SEC-039 | GAISSF™ Insurance Sector Implementation Guide | v1.0

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION	Apply physical-AI safeguards where telematics, IoT, drones, vehicles, sensors or robotic inspection affect insured risks.	Telematics; IoT; drones; image inspection; connected devices	Apply cyber-physical attack detection to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	Engineering / Safety / Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	Apply physical-AI safeguards where telematics, IoT, drones, vehicles, sensors or robotic inspection affect insured risks.	Telematics; IoT; drones; image inspection; connected devices	Apply physical environment integrity monitoring to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	Engineering / Safety / Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

Control ID	Control title	Insurance interpretation	Functions	Example implementation	Evidence	Owner	Assessment	Caveat	Notably absent
D9-CTL-06	ACTUATOR COMMAND VERIFICATION	Apply physical-AI safeguards where telematics, IoT, drones, vehicles, sensors or robotic inspection affect insured risks.	Telematics; IoT; drones; image inspection; connected devices	Apply actuator command verification to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	Engineering / Safety / Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.
D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	Apply physical-AI safeguards where telematics, IoT, drones, vehicles, sensors or robotic inspection affect insured risks.	Telematics; IoT; drones; image inspection; connected devices	Apply physical incident evidence preservation to the complete insurance decision chain and document sector-specific threats, limits and fallbacks.	[T1] Control configuration, operating logs and approvals ; [T2] independent review; [T3] controlled simulation /red-team evidence; [T4] vendor or industry claims only as supplementary context.	Engineering / Safety / Operations	Test design and operating effectiveness; sample material decisions; verify scope	Interpretation is informative; applicability and sufficiency remain entity-specific.	No claim of regulatory equivalence or automatic certification.

21. Regulatory and standards landscape

External sources provide context, not automatic obligations or equivalence. Implementing organisations should verify current status, jurisdiction, adoption, effective dates, amendments and supervisory interpretation before reliance.

Source ID	Instrument	Issuer / jurisdiction	Relevance	Status / limitation
SRC-02	Application Paper on the Supervision of Artificial Intelligence	International Association of Insurance Supervisors / International supervisory guidance	Insurance supervision, governance and conduct context	Application paper; not binding law and jurisdictional implementation varies.
SRC-03	Opinion on Artificial Intelligence Governance and Risk Management	EIOPA / European Union / EEA supervisory context	Insurance-sector governance and risk management principles	Addressed to national supervisors; applicability must be assessed.
SRC-04	Model Bulletin: Use of Artificial Intelligence Systems by Insurers	NAIC / United States state insurance regulation model	Written AIS program, governance, consumer outcomes and regulator examination expectations	Model bulletin; adoption and wording vary by state.

Source ID	Instrument	Issuer / jurisdiction	Relevance	Status / limitation
SRC-05	Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1	NIST / United States / cross-sector voluntary framework	Cross-sector lifecycle risk management	Voluntary framework; not insurance-specific or a legal compliance standard.
SRC-06	Artificial Intelligence Risk Management Framework: Generative AI Profile, NIST AI 600-1	NIST / United States / cross-sector voluntary profile	Generative-AI risks and controls	Profile requires tailoring to insurance use cases and law.
SRC-07	Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy AI in the European Insurance Sector	EIOPA Consultative Expert Group / European insurance sector	Fairness, explainability, governance, data and resilience context	Expert-group report, not binding law.

22. Financial impact vectors

Vector	Impact pathway
Claims leakage	Incorrect estimation, weak fraud detection or uncontrolled settlement recommendations.
Incorrect claims denial	False negatives or automation bias create remediation and litigation exposure.
Underpricing / overpricing	Model or data errors distort premium adequacy or customer outcomes.
Adverse selection	Poor segmentation or drift changes portfolio risk mix.
Reserving error	Model assumptions or regime shifts distort liabilities and management information.
Capital and reinsurance impacts	Accumulation or catastrophe-model error affects risk transfer and solvency decisions.
Regulatory and legal cost	Examination, remediation, penalties, disputes and record reconstruction.
Operational disruption	Vendor outage, model compromise or claims surge impairs critical services.
Fraud losses	Adversarial evasion, synthetic evidence or compromised scoring increases leakage.
Reputation and attrition	Unfair, opaque or inaccurate outcomes damage trust and distribution relationships.

These are pathways, not guaranteed outcomes. Quantification should use entity-specific exposure, decision volume, remediation cost, claims severity, capital and reinsurance assumptions.

23. Metrics and reporting

Metric	Definition	Owner	Frequency	Interpretation / gaming caveat
Inventory coverage	Material systems recorded / systems identified	AI governance	Monthly	Unknown shadow AI or stale records can distort metric
High-impact validation currency	High-impact systems with current validation	Model risk	Quarterly	A current report may still contain unresolved limitations
Adverse outcome rate	Adverse decisions by product and subgroup	Compliance / business	Monthly	Small samples and confounding require careful interpretation
Appeal reversal rate	Decisions reversed after challenge	Claims / underwriting	Monthly	Low appeal access can artificially lower the rate
Override rate and reason	Human overrides by system and outcome	Business owner	Monthly	Targeting low override rates can suppress appropriate challenge
Drift exceptions	Open performance/data drift breaches	Model owner	Risk-based	Threshold choice can conceal slow deterioration
Security abuse events	Injection, extraction, evasion or unauthorised-use events	CISO	Continuous / monthly report	Detection coverage varies
Vendor concentration	Critical services sharing provider/model/cloud	Third-party risk	Quarterly	Contract-level count may miss common fourth parties
Manual fallback readiness	Critical systems with tested fallback	Operations	Quarterly	Documented procedure is not proof of usable capacity

24. Notably Absent

- No legal, regulatory, actuarial, financial, insurance or investment advice.

- No regulator, actuarial or certification approval.
- No guaranteed compliance, fairness, accuracy, security, resilience or insurability.
- No universal risk, performance, fairness, confidence or notification threshold.
- No substitute for independent validation, policyholder-impact assessment or jurisdiction-specific review.
- No complete list of insurance threats, regulations, standards, vendors or use cases.
- No endorsement of any model, vendor, technology, data source or methodology.
- No determination that a particular insurance decision, variable, rate, claim outcome or coverage interpretation is lawful.
- No universal definition of high-risk AI.
- No presumption that human review, explainability or provider assurance is effective without operating evidence.

Appendix A - Terms and definitions

Term	Working definition
Adverse consumer outcome	A decision or process outcome that may unlawfully or unfairly disadvantage a policyholder, applicant, claimant or beneficiary.
Decision authority	The degree to which an AI system recommends, determines, executes or constrains an insurance action.
Meaningful human oversight	Timely review by a competent and authorised person with sufficient information and ability to intervene.
Insurance AI system	An AI-enabled component or decision chain used in insurance operations, including models, rules, prompts, retrieval, tools and integrations.
Policyholder impact	Actual or reasonably foreseeable effect on eligibility, price, coverage, claim, service, privacy, dignity or ability to challenge.

Appendix B - Insurance AI System Inventory

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

System ID	Name	Business owner	Function	Decision authority	Classification	Data sensitivity	Vendor	GAISST scope	Status
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix C - Insurance AI Risk Assessment

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Risk ID	System ID	Scenario	Threat/failure	Policyholder impact	Financial impact	Likelihood rationale	Controls	Residual risk	Owner	Action
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix D - Control Interpretation Matrix

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Control ID	Control title	Applicable?	Insurance interpretation	Implementation	Evidence	Owner	Test	Gap	Status
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix E - Evidence Catalogue

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Evidence ID	Category	Title	Control links	Owner	Source	Period	Retention	Reliability	Location
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix F - Human Oversight Matrix

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Decision	Trigger	Oversight model	Reviewer competence	Information required	Authority	Time limit	Override record	Escalation
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix G - Vendor Due Diligence Questionnaire

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Question ID	Domain	Question	Evidence requested	Response	Risk rating	Reviewer	Action
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix H - Incident Classification Matrix

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Incident ID	System	Description	Severity	Policyholder impact	Financial impact	Security impact	Regulatory assessment	Owner	Status
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix I - Implementation Roadmap Tracker

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Task ID	Phase	Task	Owner	Start	Due	Dependency	Evidence	Status	Completion %
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix J - Worked Scenario Record

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Scenario ID	Context	Data	Decision authority	Threats	Controls	Evidence	Oversight	Monitoring	Residual risk
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix K - Source Register

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Source ID	Title	Issuer	Jurisdiction	Date	Tier	URL	Supported sections	Limitations	Status
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix L - Notably Absent Register

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Item ID	Excluded claim/assumption	Reason	Affected section	Owner	Review date
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix M - Document Review Checklist

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Check ID	Category	Check	Owner	Status	Evidence / note
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed

Appendix N - Open Issues and Deferred Decisions

Purpose: provide a controlled record supporting implementation, assessment and review. Instructions: complete all material fields, retain source evidence, identify assumptions and do not treat example entries as mandatory thresholds. Record owner and review frequency should be assigned according to risk and applicable retention requirements.

Issue ID	Description	Reason unresolved	Owner	Dependency	Risk	Required decision	Target stage	Publication impact	Status
EXAMPLE - illustrative	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed	To be completed

Open issues register

ID	Issue	Reason	Owner	Dependency	Risk	Decision	Target	Impact	Status
OI-001	Jurisdiction-specific legal and regulatory review	Applicability varies	Qualified counsel	Target markets	Unsupported publication claim	Approve or qualify references	Before final public release	High	Open - legal review required
OI-002	Actuarial terminology and examples	Requires professional review	Qualified actuary	Insurance lines	Misinterpretation	Approve or revise	Before final public release	High	Open - actuarial review required
OI-003	Formal approval identities	Named approvers not provided	Document owner	Approval process	Incomplete governance record	Record approvals	Before final public release	Medium	Open
OI-004	Final website and repository URLs	Publication destinations not provided	Publication owner	Website/ GitHub	Broken access or placeholder	Insert verified URLs	Before final public release	Medium	Open
OI-005	Trademark-status wording	Final status should be confirmed at release	Legal owner	Trademark register	Incorrect notice	Confirm wording	Before final public release	Medium	Open - trademark confirmation required

Source register

ID	Title	Issuer	Jurisdiction	Publication date	Tier	URL	Supports	Limitations	Status
SRC-IAIS-01	Application Paper on the Supervision of Artificial Intelligence	IAIS	Global	July 2025	T1	https://www.iais.org/2025/07/the-iais-publishes-application-paper-on-the-supervision-of-artificial-intelligence/	Governance; conduct; supervision	Non-binding application paper; jurisdictional applicability review required	Source verified; applicability open
SRC-NAIC-01	Model Bulletin: Use of Artificial Intelligence Systems by Insurers	NAIC	United States / adopting jurisdictions	4 December 2023	T1	https://content.naic.org/sites/default/files/inline-files/2023-12-4%20Model%20Bulletin_Adopted_0.pdf	AIS programme; governance; consumer outcomes; third parties	Adoption and interpretation vary by jurisdiction	Source verified; applicability open

ID	Title	Issuer	Jurisdiction	Publication date	Tier	URL	Supports	Limitations	Status
SRC-EIOPA-01	Opinion on Artificial Intelligence Governance and Risk Management	EIOPA	European Union	2025	T1	https://www.eiopa.europa.eu/publications/opinion-artificial-intelligence-governance-and-risk-management_en	Insurance-sector AI governance and risk management	Apply with EU and national law	Source verified; applicability open
SRC-EIOPA-02	Artificial Intelligence Governance Principles : Towards Ethical and Trustworthy AI in the European Insurance Sector	EIOPA Consultative Expert Group	European Union	June 2021	T2	https://www.eiopa.europa.eu/publications/artificial-intelligence-governance-principles-towards-ethical-and-trustworthy-artificial_en	Fairness; explainability; oversight	Expert-group report; not binding law	Verified contextual source
SRC-SII-01	Solvency II framework	European Commission / EIOPA	European Union	Current framework	T1	https://www.eiopa.europa.eu/browse/regulation-and-policy/solvency-ii_en	Prudential and capital context	No direct GAISSF equivalence; legal review required	Source verified; applicability open
SRC-IFRS17-01	IFRS 17 Insurance Contracts	IASB / IFRS Foundation	IFRS jurisdictions	Effective 1 January 2023 subject to adoption	T1	https://www.ifrs.org/issued-standards/list-of-standards/ifrs-17-insurance-contracts/	Financial reporting context	Accounting linkage to AI failures requires qualified review	Source verified; applicability open

Final quality-control report

Review	Result	Finding
Structural review	Pass	All required sections, appendices, scenarios and registers included.
Normative-language review	Pass	No new mandatory sector requirements; verified GAISSF IDs used.

Review	Result	Finding
Cross-reference review	Pass with approval caveat	Control IDs verified to GAISST-NOR-001; named approval records remain open.
Citation/source review	Pass with applicability caveat	Authoritative sources listed; jurisdictional applicability requires qualified review.
Legal/regulatory review	Open	Qualified review required before public reliance in target jurisdictions.
Sector review	Open	Qualified insurance and actuarial review required.
Publication review	Pass with open release metadata	Final URLs and approval identities remain open.

Reader guide

Reader	Priority sections	Key appendices / artifacts
Board, CFO, CRO and Appointed Actuary	Executive summary; prudential and actuarial impact vectors; governance; Notably Absent	Open issues; workbook dashboard and risk register
CISO and security architecture	Risk landscape; security architecture; agentic AI; control mapping	Control Mapping and Incident Register
Claims and underwriting leaders	Function interpretations; human oversight; worked scenarios	Human Oversight and Scenarios sheets
Compliance, conduct and privacy	Transparency and contestability; data governance; incident management	Source Register and Evidence Register
Procurement and vendor risk	Third-party management and concentration	Vendor Assessment and AI/SBOM evidence

Prudential and actuarial impact vectors

The following table translates security and AI-control failures into potential balance-sheet, actuarial and prudential pathways. It does not assert that a control failure automatically creates an accounting, capital or regulatory breach.

GAISST domain	Insurance failure pathway	Potential prudential / actuarial consequence
D1 - Model integrity	Pricing or underwriting instability, poisoning or drift	Adverse selection, margin erosion, reserve assumption distortion and rate-filing challenge.
D4 - Third-party AI security	Common catastrophe, cloud, data or foundation-model dependency failure	Correlated portfolio error, accumulation underestimation, service interruption and reinsurance treaty dispute.
D5 - Output integrity	Misleading claims, policy or financial-reporting content	Claims leakage, customer remediation, reporting control failure and audit qualification risk.
D6 - Governance	Weak accountability, oversight or continuity	Operational resilience failure, delayed catastrophe response and governance or supervisory findings.
D8 - Model risk	Invalid reserving, capital or catastrophe-model assumptions	Potential IFRS 17 reporting misstatement, solvency-capital distortion and board risk-appetite breach; applicability requires qualified review.

Evidence quality tiers

- T1: Primary verified operating evidence: automated logs, immutable decision/claims trails, access records, telemetry and approved source records.
- T2: Independent or second-line verified evidence: MRM validation, Appointed Actuary sign-off, internal audit, privacy, legal or security review.
- T3: Controlled simulation evidence: adversarial testing, deepfake-claim injection, stress testing, catastrophe surge, failover and out-of-distribution exercises.
- T4: Anecdotal or unverified context: vendor benchmarks, surveys and generic white papers; insufficient alone for high-impact underwriting, pricing or claims conclusions.

Agentic AI in insurance workflows

Multi-agent insurance workflows can connect broker, insurer, reinsurer, claims, data and payment services. The decision boundary must include the full delegation chain rather than assessing each agent in isolation.

- Agent-to-agent authentication failure between broker, insurer, reinsurer and service-provider agents
- Compounding error in autonomous underwriting, claims adjustment or reinsurance placement
- Orphaned execution loops that repeatedly request evidence, change reserves, issue communications or invoke payment tools
- Delegation-chain ambiguity, excessive tool authority and inability to reconstruct which agent made or executed a decision

Minimum implementation controls:

- Unique workload identity and mutual authentication for each agent
- Explicit delegation scope, transaction limits, segregation of duties and expiry
- Loop, cost, time and action-count circuit breakers
- Human approval before binding coverage, denying claims, changing reserves, placing reinsurance or initiating payment
- Complete agent-to-agent message, tool-call, model-version and approval trace

Maintenance plan

Review SEC-039 at least annually and after a material GAISSF revision, insurance supervisory development, significant sector incident, material technology change or substantiated practitioner feedback. Use minor versions for corrections and clarifications and major versions for substantive architecture or control-interpretation changes. Publish change notices through the official ODA3 Institute website and repository.

Publication-readiness declaration

CONTROLLED PRE-RELEASE DRAFT FOR PEER REVIEW. The substantive implementation package and verified GAISSF control mapping are complete. Final public release is not authorised until qualified insurance/actuarial and jurisdiction-specific legal/regulatory applicability reviews, named approvals, trademark/legal-entity verification and final publication URLs are closed.

End of SEC-039 v1.0