

ODA3 INSTITUTE

SECTOR IMPLEMENTATION GUIDE

GAISSF™ v1.0 Telecommunications Sector Implementation Guide

Implementation guidance for the Global AI Safety and Security Framework

GAISSF-SEC-047 | Informative sector guidance | Draft for Publication
Version 1.0 | Public | External Review Open | Updated 6 October 2026

© 2026 ODA3 Pvt Ltd

Document Control

Field	Value
Document ID	GAISSF-SEC-047
Version	1.0
Status	Draft for Publication
Classification	Public / informative sector implementation guide
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
Authoritative source	GAISSF-NOR-001 v1.0 Final Publication Edition; updated 4 October 2026
Control baseline	59 controls across D1-D9
Publication channel	docs.oda3.org / ODA3 public package
Applicable-Control Baseline	52 D1-D8 controls plus applicable D9 controls
Updated	6 October 2026
Review state	External Review Open
Draft publication date	6 October 2026
Final publication date	Not yet set

Legal, Reliance and Assessment Notice

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute. This guide provides non-normative implementation guidance and does not constitute legal, regulatory, engineering, safety or certification advice. It does not guarantee security, safety, network availability, regulatory compliance or absence of harmful outcomes. Organisations must perform jurisdiction-specific legal/regulatory review and operator-specific engineering validation. GAISSF certification is not currently offered; use of this guide does not establish certification, regulatory approval, conformity, evidence sufficiency or operating effectiveness.

1. Executive Summary

Telecommunications AI operates across geographically distributed, high-availability and multi-vendor environments that combine legacy network functions, cloud-native components, edge systems, customer platforms and regulated services. AI outputs may influence planning, routing, configuration, fault management, fraud controls, subscriber identity, customer communications and security response. The defining implementation issue is therefore not model accuracy alone, but the relationship between model output, operational authority, execution controls, observability, rollback and human intervention.

This guide provides telecommunications-sector implementation guidance for GAISSF™ v1.0. GAISSF contains 59 controls across 9 domains. The Applicable-Control Baseline comprises all 52 controls in D1-D8 plus the 7 D9 controls where Physical AI or cyber-physical actuation is in scope. This guide does not create a separate telecommunications framework and does not alter GAISSF Foundational, Operational or Optimized conformance tiers. Where D9 is in scope, use GAISSF D9 alongside PAI-SF™ v1.0 as applicable; CSX-PAISF-004 is mapping only and does not establish equivalence, evidence sufficiency or automatic conformance. D7 remains the canonical GAISSF domain Human & Societal Harms and retains its phishing, deepfake, out-of-band authentication, AI social-engineering incident-response and AI-enhanced external-attack control set; sector-specific human-factors or fairness considerations do not redefine D7.

2. Scope and Sector Context

In scope: mobile and fixed operators, ISPs, satellite providers, wholesale carriers, MVNOS, tower and passive infrastructure providers, subsea and terrestrial network operators, telecom cloud and edge providers, equipment manufacturers, managed service providers, roaming and interconnect partners, OSS/BSS environments, security operations and customer-facing AI. Out of scope: replacing network engineering standards, deciding legal obligations, certifying products, or prescribing universal architecture.

Participant	Primary AI-security concern
Network operator	Availability, configuration integrity, subscriber impact
Equipment/software supplier	Embedded AI provenance, updates, supportability

Participant	Primary AI-security concern
Cloud/edge provider	Isolation, dependency resilience, telemetry and access
Roaming/interconnect partner	Data quality, trust boundaries, fraud and signalling
Regulator/lawful authority	Evidence, reporting, privacy and authorised access
Subscriber/enterprise customer	Service continuity, confidentiality, fairness and redress

3. Telecommunications AI System Taxonomy

Category	Examples	Typical authority	Primary failure concern
Planning and engineering	Demand forecasting, radio planning, digital twins	Advisory	Stale assumptions and under-capacity
Network operations	Fault correlation, routing, remediation, slice orchestration	Advisory to bounded execution	Cascading changes and failed rollback
Cybersecurity	Detection, prioritisation, containment	Advisory to approval-gated	False containment or missed attack
Customer and commercial	Support, identity, fraud, billing	Decision support	Privacy, wrongful blocking, inaccurate advice
Regulatory and assurance	Evidence analysis, reporting support	Draft/analysis	Incorrect or unsupported compliance claims

4. Critical Asset and Risk Model

Critical assets include subscriber identity and authentication data, cryptographic material, configuration and topology data, signalling and routing data, geolocation and call-detail records, lawful-interception and emergency-routing systems, telemetry, model and dataset artefacts, vector stores, agent memory, automation credentials, audit records, supplier attestations and recovery procedures.

Risk domain	Representative risk	Required control emphasis
Availability and resilience	Incorrect automated remediation causes service outage	Bounded authority, canary, rollback, fallback
Integrity and configuration	Hallucinated or manipulated configuration	Command validation, simulation, dual approval
Signalling and protocol	AI misses or misclassifies SS7/Diameter/SIP abuse	Protocol-aware testing, drift monitoring
Subscriber harm	Wrongful fraud block or identity rejection	Impact testing, appeal, reversal monitoring
Supply chain	Compromised model or equipment update	Provenance, staged update, audit rights
Privacy and data	Unauthorised use or leakage of communications data	Purpose limitation, access, retention, output controls
Agentic automation	Excess privilege or tool invocation	Non-human identity, allowlists, transaction limits
Regulatory and contractual	Incorrect reporting or SLA breach	Legal review, evidence traceability, obligation mapping

5. Authority and Execution Control Model

Level	Description	Required controls
A0 Read-only advisory	No production change authority	Input/output logging, user validation
A1 Draft generation	Produces scripts or configurations	Syntax and semantic validation; no credentials
A2 Approval-gated	Execution only after authorised approval	Segregation of duties, signed approval, maintenance window
A3 Bounded automation	Executes predefined actions within limits	Tool allowlist, rate/transaction limits, canary, rollback
A4 Supervised agent	Chooses among bounded actions with active oversight	Continuous observation, stop control, privileged session record
A5 Autonomous execution	Material state change without per-action approval	Exceptional justification, hard boundaries, independent monitoring,

Level	Description	Required controls
		tested kill switch
A6 Emergency automation	Pre-approved action under emergency conditions	Narrow trigger, time limit, retrospective review, evidence preservation

6. Telecommunications Implementation Levels (Informative)

Implementation Level	Use	Core expectations
Level 1 - Baseline implementation	Low-impact internal or advisory AI	Inventory, ownership, basic risk assessment, access control, validation, incident route This level is an informative telecom implementation-intensity aid and is not a GAISSF conformance tier.
Level 2 - Operational implementation	Production, customer-affecting, fraud, SOC or OSS/BSS integrated systems	Automated monitoring, supplier assurance, testing, exception management, fallback This level is an informative telecom implementation-intensity aid and is not a GAISSF conformance tier.
Level 3 - Critical Telecommunications	Systems changing network state or affecting core services, identity, emergency or lawful functions	Execution separation, dual approval where material, canary, rollback, kill switch, high-integrity logs, resilience tests This level is an informative telecom implementation-intensity aid and is not a GAISSF conformance tier.

7. Required Use Cases

ID	Use case	Domain	Authority	Benefit	Principal harm
UC-01	AI-assisted radio network optimisation	RAN	Bounded automation	Capacity and coverage improvement	Unsafe parameter changes; service degradation
UC-02	Predictive maintenance for cell towers	Physical infrastructure	Recommendation	Reduced outages	Missed failure; unsafe dispatch
UC-03	AI-based fault correlation	OSS/NOC	Recommendation	Faster diagnosis	False root cause; delayed recovery
UC-04	Automated network remediation	Core/transport	Approval-gated	Reduced restoration time	Cascading outage
UC-05	5G network slice orchestration	5G core	Bounded automation	Dynamic service assurance	Resource starvation; isolation failure
UC-06	Telecom fraud detection	BSS/fraud	Decision support	Loss reduction	Wrongful blocking; discrimination
UC-07	SIM-swap detection	Identity	Decision support	Account protection	False rejection; takeover missed
UC-08	Customer-service generative AI	Customer channels	Draft generation	Faster support	Privacy leakage; misleading advice
UC-09	Security operations copilot	SOC	Recommendation	Faster triage	Fabricated incident facts
UC-10	Signalling anomaly detection	SS7/Diameter/SIP	Recommendation	Abuse detection	Evasion; false positives
UC-11	DDoS detection and mitigation	Network security	Approval-gated	Rapid containment	Blocking legitimate traffic
UC-12	Network configuration generation	Network engineering	Draft generation	Engineering efficiency	Syntactically valid unsafe command

ID	Use case	Domain	Authority	Benefit	Principal harm
UC-13	Network digital twin	Planning/assurance	Simulation	Safer planning	Model-reality divergence
UC-14	Energy optimisation	Sites/data centres	Bounded automation	Lower energy use	Thermal or availability impact
UC-15	Capacity forecasting	Planning	Recommendation	Investment optimisation	Event demand underprediction
UC-16	Roaming fraud analytics	Roaming/BSS	Decision support	Fraud reduction	Partner data quality errors
UC-17	Spam and messaging abuse detection	Messaging	Bounded enforcement	Abuse reduction	Legitimate message suppression
UC-18	Open RAN optimisation	Open RAN	Bounded automation	Performance optimisation	Multi-vendor instability
UC-19	Edge AI services	Edge	Varies	Low latency	Weak local governance; patch gaps
UC-20	Satellite-network operations	Satellite	Recommendation	Resource optimisation	Coverage or routing impact
UC-21	Regulatory reporting assistance	Compliance	Draft generation	Efficiency	Incorrect filing
UC-22	Lawful-request processing support	Legal/compliance	Triage only	Workflow support	Unauthorised disclosure
UC-23	Billing anomaly detection	BSS	Decision support	Revenue assurance	Incorrect charges
UC-24	Subscriber identity verification	Identity	Decision support	Fraud reduction	Bias; exclusion
UC-25	Autonomous network operations	Multiple	Autonomous execution	Rapid adaptation	Systemic cascading failure

8. Threat and Failure Scenarios

ID	Threat/failure	Actor	Domain	Path	Evidence status
TH-01	Prompt injection through trouble ticket	External attacker	OSS/ticketing	Malicious instructions enter agent context	Plausible
TH-02	Poisoned network telemetry	External or insider	Telemetry/AIOps	Manipulated inputs drive false diagnosis or action	Plausible
TH-03	Compromised model update	Supplier compromise	Model supply chain	Malicious or defective update changes behavior	Plausible
TH-04	Credential abuse by AI agent	Credential compromise	Automation	Agent uses excessive privileges	Plausible
TH-05	Model extraction via API	Competitor or criminal	Inference API	Systematic querying reproduces model capability	Observed technique; sector occurrence unverified
TH-06	Fraud-model evasion	Fraud group	Fraud analytics	Behavior shaped to evade detection	Plausible
TH-07	Hallucinated configuration	Non-malicious failure	Network engineering	Generated command is valid-looking but unsafe	Plausible
TH-08	Central AI dependency outage	Operational failure	AIOps platform	Loss of central service impairs distributed operations	Plausible

ID	Threat/failure	Actor	Domain	Path	Evidence status
TH-09	Subscriber data leakage	External or insider	Customer AI	Sensitive data exposed in output or logs	Plausible
TH-10	Rollback failure	Operational failure	Automation	Change cannot be reversed in required time	Plausible

9. Evidence and Assessment Model

Evidence should be attributable, time-bounded, integrity-protected and tied to a system, control, owner and assessment period. Suitable evidence includes architecture and data-flow records, model and data provenance, access and non-human identity records, test results, change and approval records, execution logs, rollback tests, drift reports, supplier attestations, incident records, privacy and legal reviews, exception decisions and training records.

Assessment method	Telecom application
Design review	Confirm trust boundaries, authority path, fallback and recovery dependencies
Configuration inspection	Inspect agent tools, credentials, allowlists, limits and environment separation
Sampling	Trace AI recommendations, approvals, executions, reversals and subscriber outcomes
Challenge testing	Use malformed, adversarial, stale and conflicting telemetry
Failure injection	Test loss of model, telemetry, cloud region, credential service or rollback
Interview/observation	Validate operator competence and actual human intervention capability

10. Metrics

Metric	Definition
AI-generated change failure rate	Failed AI-originated production changes / total AI-originated changes
AI-triggered rollback rate	AI-originated changes rolled back / total AI-originated changes
Blocked high-risk actions	Count of policy-blocked agent actions
Mean time to human intervention	Elapsed time from trigger to effective operator control
Fraud-block reversal rate	Reversed blocks / total blocks
Configuration validation failure rate	Rejected generated configurations / generated configurations
Critical systems with tested fallback	Critical AI systems with current fallback test / total critical AI systems
Rollback success rate	Successful rollback tests / rollback tests
Evidence completeness	Controls with sufficient evidence / applicable controls

Thresholds must be organisation-specific and justified. This guide provides directional indicators and escalation conditions but does not prescribe universal benchmarks. Measures must be segmented by network domain, authority, change class and service criticality. Human-intervention timing must be compared with failure-development and safe-state timing.

11. Incident Response and Resilience

AI-related incidents must integrate with network, cyber, privacy, fraud, supplier and regulatory response processes. Required capabilities include model isolation, credential revocation, automation suspension, production rollback, deterministic or manual fallback, subscriber-impact assessment, forensic preservation, supplier coordination, regulatory escalation and post-incident control reassessment. Loss of an AI service must not silently remove essential network-operating capability.

12. Supply-Chain Assurance

Supplier assurance should cover model and data provenance, software and model composition, secure development, vulnerability management, update controls, incident notification, subcontractor visibility, data-use and model-training restrictions, audit rights, evidence access, portability, termination assistance, deletion verification, continuity and change notification. Supplier statements are inputs to assurance, not substitutes for operator validation.

13. Informative Standards and Regulatory Domains

Potentially relevant references include ISO/IEC 27001, 27002, 27005, 27017, 27018, 27701, 42001 and 23894; NIST CSF, AI RMF, SP 800-53, SP 800-207 and SSDF; 3GPP security specifications; GSMA security and fraud guidance; ETSI, ENISA, ITU-T, TM Forum and Open RAN guidance; and applicable national telecom, critical-infrastructure, privacy, resilience, consumer, emergency-service and lawful-access obligations. Mapping is informative, versions must be verified, and no equivalence or automatic compliance is claimed.

14. Notably Absent

- No claim that all telecommunications AI is autonomous or safety-critical.
- No claim that every listed attack has occurred in production telecom environments.
- No universal risk score, metric threshold or retention period.
- No certification decision or guarantee of compliance, availability or security.
- No replacement for telecom engineering, legal, privacy, regulatory or safety review.
- No assumption that human approval alone is an effective safeguard.
- No assumption that rollback is technically possible in every architecture.
- No assumption that telemetry or supplier evidence is trustworthy.

14.1 Authority-to-Implementation-Level Crosswalk

A5 autonomous execution and A6 emergency automation always invoke Level 3 expectations. A4 supervised agents invoke Level 3 where they can change production state, use privileged credentials, affect regulated or critical functions, reach a material subscriber or geographic scope, act faster than effective human intervention, or influence physical infrastructure. A lower implementation level requires documented technical boundaries and approval by the designated risk authority.

Authority	Default treatment	Default implementation level	Level 3 trigger
A0-A1	Level 1 or Level 2	Critical decision, sensitive data, customer or regulatory impact	Validation, review, provenance and logging
A2-A3	Level 2; Level 3 for material production action	Production network, critical service, emergency/lawful function or material blast radius	Qualified approval, separation, evidence, rollback
A4	Level 2 only in bounded non-production conditions	Any production, privileged, material or physical authority	Independent constraints, canary, kill switch, forensic logging
A5-A6	Level 3	Always	Independent monitor, bounded authority, safe state, tested fallback and post-event review

14.2 Telecommunications Materiality Test

An AI-originated or AI-assisted action is material where it changes production routing, signalling, authentication, policy, charging, orchestration or security state; affects emergency communications, lawful functions or designated critical services; exceeds operator-defined subscriber, site, region, slice or enterprise thresholds; is difficult to reverse; develops faster than effective human intervention; uses cross-domain or emergency privilege; can propagate across vendors or regions; or can breach a defined service-impact threshold. Numeric thresholds remain operator-defined and must be justified by topology, service obligations, recovery capability and concentration risk.

14.3 Evidence Architecture

Evidence is a many-to-many relationship. A control may require several artefacts, and one artefact may support several controls. The evidence model therefore separates evidence artefacts, evidence-to-control mappings and control evidence requirements. Artefact count alone does not establish sufficiency. Evidence must be attributable, time-bounded, integrity-protected, relevant to the assessed scope and validated for design and operating effectiveness.

14.4 Telecom-Specific Threat Additions

TH-11 addresses plausible AI-assisted signalling evasion across SS7, Diameter, SIP and roaming contexts. It is not presented as an observed production-sector fact. TH-12 addresses multi-vendor RAN optimisation conflict, including inconsistent xApp/rApp objectives, asynchronous state, parameter oscillation and service degradation. TH-12 may arise through integration failure without malicious action.

14.5 Metrics Interpretation

Metrics include directional indicators and escalation guidance but no unsupported universal thresholds. Mean time to effective human intervention must be compared with the system's failure-development and safe-state time. Where failure develops faster than effective human intervention, human approval or monitoring cannot be the principal protective control; independent technical constraints and automated containment are required. Rollback success must be segmented by network domain, change class and rollback mechanism, and interpreted together with test frequency and realism.

14.6 Informative External References

External mappings are qualified relationships, not equivalence claims. The mapping records relationship type, overlap, material differences, applicability and confidence. D8-CTL-04 remains unchanged; its direct or contractual relevance must be assessed rather than replaced. Current 3GPP source status was rechecked on 6 October 2026: TS 28.105 (Management and orchestration; Artificial Intelligence/Machine Learning management) remains under change control; TS 33.501 (Security architecture and procedures for 5G System) remains under change control, with Release 20 version 20.3.0 uploaded on 28 September 2026; and TS 33.502 (Security-related events handling) is a Release 20 specification under change control. TS 28.404 is a Quality of Experience measurement-collection specification and is not the primary AI/ML-management specification. Exact release, version, contractual relevance and jurisdictional applicability must be reverified for each implementation.

14.7 Telecom Interpretation of Cross-Sector Physical-AI Examples

The authoritative D9 wording is retained unchanged. Telecom-specific equivalents are informative only. Safe-state examples include controlled landing or return-to-base for tower-inspection drones, independently controlled fallback setpoints for cooling systems, immediate halt for robotic fibre work, and cessation of antenna-positioning equipment in a mechanically safe alignment. Actuator-command verification may apply to antenna equipment, robotic cable tools, tower-inspection systems, cooling and power equipment, and autonomous site-security devices.

15. Control-by-Control Telecommunications Interpretations

D1-CTL-01 - DATASET PROVENANCE & POISONING PREVENTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Protect training and evaluation data integrity against poisoning and unauthorised manipulation.
Telecommunications interpretation	Protect telecom model and dataset integrity against poisoning, extraction, drift and adversarial manipulation across network, fraud, customer and security use cases. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.

Field	Telecommunications implementation guidance
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	dataset lineage, signed model artefacts, drift reports, adversarial test results
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D1-CTL-02 - MODEL EXTRACTION RESISTANCE

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Protect model intellectual property and sensitive model behaviour against extraction.
Telecommunications interpretation	Protect telecom model and dataset integrity against poisoning, extraction, drift and adversarial manipulation across network, fraud, customer and security use cases. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	dataset lineage, signed model artefacts, drift reports, adversarial test results
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D1-CTL-03 - BEHAVIORAL DRIFT DETECTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Prevent undetected model degradation causing business loss.
Telecommunications interpretation	Protect telecom model and dataset integrity against poisoning, extraction, drift and adversarial manipulation across network, fraud, customer and security use cases. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual

Field	Telecommunications implementation guidance
	approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	dataset lineage, signed model artefacts, drift reports, adversarial test results
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D1-CTL-04 - FEDERATED LEARNING POISONING PREVENTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Protect multi-party models from malicious clients.
Telecommunications interpretation	Protect telecom model and dataset integrity against poisoning, extraction, drift and adversarial manipulation across network, fraud, customer and security use cases. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	dataset lineage, signed model artefacts, drift reports, adversarial test results
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D1-CTL-05 - EMBEDDING SPACE ROBUSTNESS

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Ensure semantic filters work under adversarial conditions.
Telecommunications interpretation	Protect telecom model and dataset integrity against poisoning, extraction, drift and adversarial manipulation across network, fraud, customer and security use cases. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains;

Field	Telecommunications implementation guidance
	maintenance windows; human intervention capability.
Evidence examples	dataset lineage, signed model artefacts, drift reports, adversarial test results
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Future-proof model supply chain against quantum attack.
Telecommunications interpretation	Protect telecom model and dataset integrity against poisoning, extraction, drift and adversarial manipulation across network, fraud, customer and security use cases. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	dataset lineage, signed model artefacts, drift reports, adversarial test results
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D1-CTL-07 - LORA/ADAPTER INTEGRITY VERIFICATION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Protect fine-tuning and adapter integrity against malicious or unauthorised modifications.
Telecommunications interpretation	Protect telecom model and dataset integrity against poisoning, extraction, drift and adversarial manipulation across network, fraud, customer and security use cases. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	dataset lineage, signed model artefacts, drift reports,

Field	Telecommunications implementation guidance
	adversarial test results
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D1-CTL-08 - MODEL MERGE ATTACK DETECTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Prevent safety-evasive merged models from entering production.
Telecommunications interpretation	Protect telecom model and dataset integrity against poisoning, extraction, drift and adversarial manipulation across network, fraud, customer and security use cases. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	dataset lineage, signed model artefacts, drift reports, adversarial test results
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D1-CTL-09 - QUANTIZATION BACKDOOR SCREENING

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Ensure quantization doesn't activate hidden backdoors.
Telecommunications interpretation	Protect telecom model and dataset integrity against poisoning, extraction, drift and adversarial manipulation across network, fraud, customer and security use cases. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	dataset lineage, signed model artefacts, drift reports, adversarial test results
Testing	Inspect design and configuration; sample records; challenge

Field	Telecommunications implementation guidance
	inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D2-CTL-01 - DIRECT PROMPT INJECTION PREVENTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Prevent unauthorized system prompt override or instruction hijacking.
Telecommunications interpretation	Apply runtime safeguards at inference gateways, OSS/BSS integrations, network-management interfaces and edge deployments, with telemetry validation and fail-safe behavior. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	gateway policies, runtime logs, input validation records, containment tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D2-CTL-02 - INDIRECT PROMPT INJECTION PREVENTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Block malicious instructions injected via RAG, APIs, or external data sources.
Telecommunications interpretation	Apply runtime safeguards at inference gateways, OSS/BSS integrations, network-management interfaces and edge deployments, with telemetry validation and fail-safe behavior. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	gateway policies, runtime logs, input validation records, containment tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.

Field	Telecommunications implementation guidance
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D2-CTL-03 - JAILBREAK RESISTANCE TESTING

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Validate safety guardrails against evolving adversarial prompt techniques.
Telecommunications interpretation	Apply runtime safeguards at inference gateways, OSS/BSS integrations, network-management interfaces and edge deployments, with telemetry validation and fail-safe behavior. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	gateway policies, runtime logs, input validation records, containment tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D2-CTL-04 - MULTI-MODAL INJECTION DEFENSE

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Prevent hidden commands embedded in images, audio, or video from executing.
Telecommunications interpretation	Apply runtime safeguards at inference gateways, OSS/BSS integrations, network-management interfaces and edge deployments, with telemetry validation and fail-safe behavior. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	gateway policies, runtime logs, input validation records, containment tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner;

Field	Telecommunications implementation guidance
	untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Secure structured tool/function parameters from adversarial manipulation.
Telecommunications interpretation	Apply runtime safeguards at inference gateways, OSS/BSS integrations, network-management interfaces and edge deployments, with telemetry validation and fail-safe behavior. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	gateway policies, runtime logs, input validation records, containment tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D2-CTL-06 - CROSS-CONTEXT HIJACKING MITIGATION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Prevent system prompt dilution or override in long-context windows.
Telecommunications interpretation	Apply runtime safeguards at inference gateways, OSS/BSS integrations, network-management interfaces and edge deployments, with telemetry validation and fail-safe behavior. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	gateway policies, runtime logs, input validation records, containment tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without

Field	Telecommunications implementation guidance
	validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D3-CTL-01 - LEAST AGENCY ENFORCEMENT

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Limit agent tool access and action scopes to prevent catastrophic autonomous actions.
Telecommunications interpretation	Constrain AI agents and automation through explicit authority levels, tool allowlists, non-human identity controls, approval gates, transaction limits and tested rollback. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	agent permission matrix, approval records, signed action logs, rollback tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D3-CTL-02 - INTER-AGENT COMMUNICATION SECURITY

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Authenticate and encrypt all agent-to-agent messaging to prevent internal compromise.
Telecommunications interpretation	Constrain AI agents and automation through explicit authority levels, tool allowlists, non-human identity controls, approval gates, transaction limits and tested rollback. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	agent permission matrix, approval records, signed action logs, rollback tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.

Field	Telecommunications implementation guidance
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D3-CTL-03 - AGENTIC PROMPT CHAINING DETECTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Detect distributed attacks leveraging multiple agents/turns to bypass controls.
Telecommunications interpretation	Constrain AI agents and automation through explicit authority levels, tool allowlists, non-human identity controls, approval gates, transaction limits and tested rollback. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	agent permission matrix, approval records, signed action logs, rollback tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D3-CTL-04 - EMBODIED AI SAFETY CONTROLS

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Secure physical-world AI interfaces (robots, drones, IoT) from sensor spoofing and unsafe commands.
Telecommunications interpretation	Constrain AI agents and automation through explicit authority levels, tool allowlists, non-human identity controls, approval gates, transaction limits and tested rollback. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	agent permission matrix, approval records, signed action logs, rollback tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-

Field	Telecommunications implementation guidance
	critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Cryptographically verify agent identity, permissions, and trust relationships.
Telecommunications interpretation	Constrain AI agents and automation through explicit authority levels, tool allowlists, non-human identity controls, approval gates, transaction limits and tested rollback. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	agent permission matrix, approval records, signed action logs, rollback tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D3-CTL-06 - PERSISTENT MEMORY EXFILTRATION PREVENTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Protect cross-session user data stored in vector stores or agent memory.
Telecommunications interpretation	Constrain AI agents and automation through explicit authority levels, tool allowlists, non-human identity controls, approval gates, transaction limits and tested rollback. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	agent permission matrix, approval records, signed action logs, rollback tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber

Field	Telecommunications implementation guidance
	threats.

D3-CTL-07 - SECURE MEMORY LIFECYCLE MANAGEMENT

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Ensure secure creation, rotation, and cryptographic deletion of AI memory stores.
Telecommunications interpretation	Constrain AI agents and automation through explicit authority levels, tool allowlists, non-human identity controls, approval gates, transaction limits and tested rollback. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	agent permission matrix, approval records, signed action logs, rollback tests
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Maintain complete inventory of all AI models, datasets, dependencies, and third-party components.
Telecommunications interpretation	Assure network-equipment, cloud, model, data, managed-service and software suppliers through provenance, update control, incident notice, audit rights and exit planning. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	supplier due diligence, SBOM/MBOM, update attestations, contract clauses
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D4-CTL-02 - MODEL FILE & ARTIFACT SCANNING

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Detect malware, backdoors, and unsafe serialization in model files before deployment.
Telecommunications interpretation	Assure network-equipment, cloud, model, data, managed-service and software suppliers through provenance, update control, incident notice, audit rights and exit planning. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	supplier due diligence, SBOM/MBOM, update attestations, contract clauses
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D4-CTL-03 - MODEL HUB & REGISTRY VETTING

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Assess and approve models from public/private hubs before production use.
Telecommunications interpretation	Assure network-equipment, cloud, model, data, managed-service and software suppliers through provenance, update control, incident notice, audit rights and exit planning. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	supplier due diligence, SBOM/MBOM, update attestations, contract clauses
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D4-CTL-04 - MCP SERVER BEHAVIORAL MONITORING

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Monitor Model Context Protocol (MCP) servers for unauthorized tool access or anomalous behaviour.
Telecommunications interpretation	Assure network-equipment, cloud, model, data, managed-service and software suppliers through provenance, update control, incident notice, audit rights and exit planning. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	supplier due diligence, SBOM/MBOM, update attestations, contract clauses
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Evaluate third-party AI APIs for security, privacy, governance, contractual and operational risk posture.
Telecommunications interpretation	Assure network-equipment, cloud, model, data, managed-service and software suppliers through provenance, update control, incident notice, audit rights and exit planning. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	supplier due diligence, SBOM/MBOM, update attestations, contract clauses
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D4-CTL-06 - SHADOW AI DISCOVERY & GOVERNANCE

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Detect and govern unauthorized AI tools and deployments bypassing IT controls.
Telecommunications interpretation	Assure network-equipment, cloud, model, data, managed-service and software suppliers through provenance, update control, incident notice, audit rights and exit planning. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	supplier due diligence, SBOM/MBOM, update attestations, contract clauses
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Identify and remediate vulnerabilities in AI framework dependencies and libraries.
Telecommunications interpretation	Assure network-equipment, cloud, model, data, managed-service and software suppliers through provenance, update control, incident notice, audit rights and exit planning. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	supplier due diligence, SBOM/MBOM, update attestations, contract clauses
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D5-CTL-01 - HARMFUL CONTENT BLOCKING

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Reduce exposure to harmful or prohibited content through defined policy, filtering, escalation and evidence controls without relying on unsupported financial-impact claims.
Telecommunications interpretation	Validate AI outputs before customer communication, regulatory reporting, incident action or network execution; preserve provenance and prevent misleading or unsafe content. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	output validation rules, sampling records, provenance labels, escalation logs
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D5-CTL-02 - PII LEAKAGE PREVENTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Prevent unauthorised disclosure of personal or sensitive information across AI inputs, outputs, logs, memory and retrieval paths.
Telecommunications interpretation	Validate AI outputs before customer communication, regulatory reporting, incident action or network execution; preserve provenance and prevent misleading or unsafe content. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	output validation rules, sampling records, provenance labels, escalation logs
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D5-CTL-03 - COPYRIGHT DETECTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Detect and manage copyright and licensing risk in AI-generated or retrieved content.
Telecommunications interpretation	Validate AI outputs before customer communication, regulatory reporting, incident action or network execution; preserve provenance and prevent misleading or unsafe content. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	output validation rules, sampling records, provenance labels, escalation logs
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D5-CTL-04 - AI WATERMARKING ROBUSTNESS

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Enable deepfake attribution + brand protection.
Telecommunications interpretation	Validate AI outputs before customer communication, regulatory reporting, incident action or network execution; preserve provenance and prevent misleading or unsafe content. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	output validation rules, sampling records, provenance labels, escalation logs
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004

Field	Telecommunications implementation guidance
	where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Verify that privacy requirements and controls are incorporated into design and operation for the defined scope; legal compliance requires separate jurisdiction-specific analysis.
Telecommunications interpretation	Validate AI outputs before customer communication, regulatory reporting, incident action or network execution; preserve provenance and prevent misleading or unsafe content. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	output validation rules, sampling records, provenance labels, escalation logs
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D5-CTL-06 - PRIVACY-PRESERVING ML VALIDATION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Enable safe data sharing for model training.
Telecommunications interpretation	Validate AI outputs before customer communication, regulatory reporting, incident action or network execution; preserve provenance and prevent misleading or unsafe content. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	output validation rules, sampling records, provenance labels, escalation logs
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004

Field	Telecommunications implementation guidance
	where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Prevent catastrophic autonomous actions.
Telecommunications interpretation	Establish accountable ownership, risk acceptance, segregation of duties, system inventory, change governance, competence and independent oversight. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	ownership records, risk decisions, committee minutes, competence records
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D6-CTL-02 - AUDIT TRAIL COMPLETENESS

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Maintain complete, attributable and integrity-protected audit evidence supporting investigation, assurance and applicable reporting workflows.
Telecommunications interpretation	Establish accountable ownership, risk acceptance, segregation of duties, system inventory, change governance, competence and independent oversight. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	ownership records, risk decisions, committee minutes, competence records
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D6-CTL-03 - AI MODEL CARD COMPLETENESS

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not

Field	Telecommunications implementation guidance
	restate or amend normative control wording.
Control objective	Maintain sufficiently complete model and system documentation for defined use, limitations, risks, changes and evidence; documentation alone does not establish regulatory conformity.
Telecommunications interpretation	Establish accountable ownership, risk acceptance, segregation of duties, system inventory, change governance, competence and independent oversight. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	ownership records, risk decisions, committee minutes, competence records
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D6-CTL-04 - AI INCIDENT RESPONSE READINESS

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Reduce breach impact (MTTC from days to hours).
Telecommunications interpretation	Establish accountable ownership, risk acceptance, segregation of duties, system inventory, change governance, competence and independent oversight. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	ownership records, risk decisions, committee minutes, competence records
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D6-CTL-05 - MODEL DEPRECATION & DECOMMISSIONING

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not

Field	Telecommunications implementation guidance
	restate or amend normative control wording.
Control objective	Prevent zombie AI systems with stale access.
Telecommunications interpretation	Establish accountable ownership, risk acceptance, segregation of duties, system inventory, change governance, competence and independent oversight. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	ownership records, risk decisions, committee minutes, competence records
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Manage supply chain risk.
Telecommunications interpretation	Establish accountable ownership, risk acceptance, segregation of duties, system inventory, change governance, competence and independent oversight. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	ownership records, risk decisions, committee minutes, competence records
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D6-CTL-07 - AI RESILIENCE & BUSINESS CONTINUITY

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Ensure AI availability under stress.
Telecommunications interpretation	Establish accountable ownership, risk acceptance,

Field	Telecommunications implementation guidance
	segregation of duties, system inventory, change governance, competence and independent oversight. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	ownership records, risk decisions, committee minutes, competence records
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D7-CTL-H01 - AI-GENERATED PHISHING SIMULATION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Reduce human vulnerability (primary attack vector).
Telecommunications interpretation	Assess privacy, discrimination, accessibility, public-interest and subscriber harm, especially where models affect identity, fraud blocking, service eligibility or communications data. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	impact assessments, fairness testing, complaint and reversal analysis
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D7-CTL-H02 - DEEPPFAKE DETECTION TRAINING

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Prevent CEO/executive impersonation fraud.
Telecommunications interpretation	Assess privacy, discrimination, accessibility, public-interest and subscriber harm, especially where models affect identity, fraud blocking, service eligibility or communications data. For this control, implementation should be tied to the

Field	Telecommunications implementation guidance
	specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	impact assessments, fairness testing, complaint and reversal analysis
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Prevent wire fraud via voice deepfake.
Telecommunications interpretation	Assess privacy, discrimination, accessibility, public-interest and subscriber harm, especially where models affect identity, fraud blocking, service eligibility or communications data. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	impact assessments, fairness testing, complaint and reversal analysis
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D7-CTL-H04 - AI SOCIAL ENGINEERING IR

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Enable rapid response to deepfake attacks.
Telecommunications interpretation	Assess privacy, discrimination, accessibility, public-interest and subscriber harm, especially where models affect identity, fraud blocking, service eligibility or communications data. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation

Field	Telecommunications implementation guidance
	and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	impact assessments, fairness testing, complaint and reversal analysis
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Defend against AI-powered offensive campaigns.
Telecommunications interpretation	Assess privacy, discrimination, accessibility, public-interest and subscriber harm, especially where models affect identity, fraud blocking, service eligibility or communications data. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	impact assessments, fairness testing, complaint and reversal analysis
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Identify and document applicable EU AI Act risk-classification and related obligations for the defined scope without treating the mapping as a legal-compliance determination.
Telecommunications interpretation	Map obligations by jurisdiction and service context, preserve evidence, support auditability and avoid claiming that GAISSF implementation alone establishes legal compliance. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation

Field	Telecommunications implementation guidance
	and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	obligation register, legal review, audit trails, retention rationale
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D8-CTL-02 - ISO 42001 GAP ANALYSIS

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Identify and document gaps against ISO/IEC 42001 requirements for the defined scope without implying certification or conformity.
Telecommunications interpretation	Map obligations by jurisdiction and service context, preserve evidence, support auditability and avoid claiming that GAISSF implementation alone establishes legal compliance. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	obligation register, legal review, audit trails, retention rationale
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D8-CTL-03 - GPAI TECHNICAL DOCUMENTATION VERIFICATION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Verify that required GPAI technical-documentation evidence is identified and maintained where Article 53 applies; applicability and sufficiency require separate legal analysis.
Telecommunications interpretation	Map obligations by jurisdiction and service context, preserve evidence, support auditability and avoid claiming that GAISSF implementation alone establishes legal compliance. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.

Field	Telecommunications implementation guidance
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	obligation register, legal review, audit trails, retention rationale
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Assess DORA ICT incident-reporting applicability and evidence requirements for in-scope financial-sector relationships; telecom relevance may be direct, contractual or not applicable.
Telecommunications interpretation	Map obligations by jurisdiction and service context, preserve evidence, support auditability and avoid claiming that GAISSF implementation alone establishes legal compliance. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	obligation register, legal review, audit trails, retention rationale
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Assess secure-development alignment against NIST SP 800-218A for the defined scope without implying procurement eligibility, certification or compliance.
Telecommunications interpretation	Map obligations by jurisdiction and service context, preserve evidence, support auditability and avoid claiming that GAISSF implementation alone establishes legal compliance. For this control, implementation should be tied to the

Field	Telecommunications implementation guidance
	specific network domain, authority level, subscriber impact and recovery dependency.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	obligation register, legal review, audit trails, retention rationale
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D9-CTL-01 - PHYSICAL HARM BOUNDARY ENFORCEMENT

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Ensure AI systems cannot cause physical harm by operating outside defined safety boundaries, regardless of model output or adversarial manipulation.
Telecommunications interpretation	For AI affecting physical telecom assets, sites, power, cooling, robotics or maintenance, apply safety boundaries, human intervention, environmental constraints and emergency isolation. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency. D9 is additional/conditional and applies only where Physical AI or cyber-physical actuation is in scope. Use PAI-SF™ v1.0 alongside D9 as applicable.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	hazard analysis, interlock tests, emergency-stop evidence, maintenance approvals
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D9-CTL-02 - SAFE STATE AND GRACEFUL DEGRADATION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Define and implement a minimum-risk condition for each AI-controlled physical system, reached automatically when AI confidence falls below threshold, anomaly is detected, or

Field	Telecommunications implementation guidance
	human override is activated.
Telecommunications interpretation	For AI affecting physical telecom assets, sites, power, cooling, robotics or maintenance, apply safety boundaries, human intervention, environmental constraints and emergency isolation. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency. D9 is additional/conditional and applies only where Physical AI or cyber-physical actuation is in scope. Use PAI-SF™ v1.0 alongside D9 as applicable.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	hazard analysis, interlock tests, emergency-stop evidence, maintenance approvals
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D9-CTL-03 - HUMAN OVERRIDE AND EMERGENCY STOP

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Ensure humans can always override AI control of physical systems unconditionally — including under adversarial conditions where the AI system may be attempting to prevent override.
Telecommunications interpretation	For AI affecting physical telecom assets, sites, power, cooling, robotics or maintenance, apply safety boundaries, human intervention, environmental constraints and emergency isolation. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency. D9 is additional/conditional and applies only where Physical AI or cyber-physical actuation is in scope. Use PAI-SF™ v1.0 alongside D9 as applicable.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	hazard analysis, interlock tests, emergency-stop evidence, maintenance approvals
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D9-CTL-04 - CYBER-PHYSICAL ATTACK DETECTION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Detect adversarial attacks targeting the cyber-physical interface — sensor spoofing, actuator hijacking, command injection, and AI inference manipulation — before they cause physical harm.
Telecommunications interpretation	For AI affecting physical telecom assets, sites, power, cooling, robotics or maintenance, apply safety boundaries, human intervention, environmental constraints and emergency isolation. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency. D9 is additional/conditional and applies only where Physical AI or cyber-physical actuation is in scope. Use PAI-SF™ v1.0 alongside D9 as applicable.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	hazard analysis, interlock tests, emergency-stop evidence, maintenance approvals
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D9-CTL-05 - PHYSICAL ENVIRONMENT INTEGRITY MONITORING

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Continuously verify the integrity and reliability of physical environment sensor data on which AI decisions are based, preventing AI actions grounded in corrupted, degraded, or spoofed environmental inputs.
Telecommunications interpretation	For AI affecting physical telecom assets, sites, power, cooling, robotics or maintenance, apply safety boundaries, human intervention, environmental constraints and emergency isolation. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency. D9 is additional/conditional and applies only where Physical AI or cyber-physical actuation is in scope. Use PAI-SF™ v1.0 alongside D9 as applicable.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	hazard analysis, interlock tests, emergency-stop evidence, maintenance approvals
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.

Field	Telecommunications implementation guidance
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D9-CTL-06 - ACTUATOR COMMAND VERIFICATION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Verify every actuator command against physical safety constraints, operational bounds, and system state before execution — preventing AI model errors, adversarial manipulations, or software defects from translating directly into unsafe physical actions.
Telecommunications interpretation	For AI affecting physical telecom assets, sites, power, cooling, robotics or maintenance, apply safety boundaries, human intervention, environmental constraints and emergency isolation. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency. D9 is additional/conditional and applies only where Physical AI or cyber-physical actuation is in scope. Use PAI-SF™ v1.0 alongside D9 as applicable.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	hazard analysis, interlock tests, emergency-stop evidence, maintenance approvals
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

D9-CTL-07 - PHYSICAL INCIDENT EVIDENCE PRESERVATION

Field	Telecommunications implementation guidance
Normative source	Refer to GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 where published and current. This sector guide does not restate or amend normative control wording.
Control objective	Preserve comprehensive, tamper-evident, time-stamped evidence of AI system state, sensor inputs, model outputs, actuator commands, and human interactions immediately before, during, and after any physical AI incident.
Telecommunications interpretation	For AI affecting physical telecom assets, sites, power, cooling, robotics or maintenance, apply safety boundaries, human intervention, environmental constraints and emergency isolation. For this control, implementation should be tied to the specific network domain, authority level, subscriber impact and recovery dependency. D9 is additional/conditional and applies only where Physical AI or cyber-physical actuation is in scope. Use PAI-SF™ v1.0 alongside D9 as applicable.
Minimum expectation	Document scope, owner, data, model, access, validation and evidence.

Field	Telecommunications implementation guidance
Critical-telecom expectation	Separate recommendation from execution; enforce dual approval where material; canary, rollback, kill switch and forensic logging.
Authority restrictions	Least privilege; bounded tools; approved domains; maintenance windows; human intervention capability.
Evidence examples	hazard analysis, interlock tests, emergency-stop evidence, maintenance approvals
Testing	Inspect design and configuration; sample records; challenge inputs; test degraded mode and rollback where applicable.
Common failure pattern	Generic policy only; unbounded scope; missing owner; untested assumptions; supplier evidence accepted without validation.
Notably absent	No assumption that the system is autonomous, safety-critical, legally compliant or immune to conventional cyber threats.

Publication recommendation: Suitable for public draft publication as Draft for Publication / Public / External Review Open. Telecommunications engineering, jurisdiction-specific legal/regulatory, accessibility/editorial and explicit final release authorization remain open as Final Publication gates. Public draft publication does not imply that those reviews or approvals have been completed.