

Telecommunications Sector Implementation Guide

SEC-047 | Version 1.0 | Publication Candidate

Published by ODA3 Institute

Informative sector guidance subordinate to the authoritative GAISSF control baseline

Document Control

Field	Value
Document ID	SEC-047
Version	1.0
Status	Draft for Publication Review
Classification	Informative sector implementation guide
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
Authoritative source	GAISSF-NOR-001 v1.0, corrected final publication edition, 29 June 2026
Control baseline	59 controls across D1-D9
Publication channel	Website / GitHub

Legal, Reliance and Assessment Notice

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute. This guide provides implementation guidance and does not constitute legal, regulatory, engineering or certification advice. It does not guarantee security, safety, network availability, regulatory compliance or absence of harmful outcomes. Organisations must perform jurisdiction-specific legal review and operator-specific engineering validation. Assessment against this guide does not itself establish GAISSF certification.

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 translates the 59 authoritative GAISSF controls into telecommunications-specific implementation, evidence and assessment considerations. It does not create a separate telecommunications framework and does not assume that every telecom AI system is autonomous, safety-critical or capable of changing network state.

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
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	Segregation of duties, signed

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

6. Implementation Profiles

Profile	Use	Core expectations
Tier 1 - Foundational	Low-impact internal or advisory AI	Inventory, ownership, basic risk assessment, access control, validation, incident route
Tier 2 - Operational	Production, customer-affecting, fraud, SOC or OSS/BSS integrated systems	Automated monitoring, supplier assurance, testing, exception management, fallback
Tier 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

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
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	External or	Telemetry/AIOps	Manipulated	Plausible

	network telemetry	insider		inputs drive false diagnosis or action	
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
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-Tier Crosswalk

A5 autonomous execution and A6 emergency automation always invoke Tier 3 expectations. A4 supervised agents invoke Tier 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 classification requires documented technical boundaries and approval by the designated risk authority.

Authority	Default treatment	Tier 3 trigger	Core safeguards
A0-A1	Tier 1 or Tier 2	Critical decision, sensitive data, customer or regulatory impact	Validation, review, provenance and logging
A2-A3	Tier 2; Tier 3 for material production action	Production network, critical service, emergency/lawful function or material blast radius	Qualified approval, separation, evidence, rollback
A4	Tier 2 only in bounded non-production conditions	Any production, privileged, material or physical authority	Independent constraints, canary, kill switch, forensic logging
A5-A6	Tier 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. For 3GPP context, TS 28.105 is used for AI/ML management. TS 28.404 is limited to Quality of Experience measurement collection. TS 33.501 concerns 5G security architecture and procedures, while TS 33.502 concerns security-related events handling. Exact versions and applicability must be verified at publication.

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
Authoritative GAISSF control text	Hash verification + source allowlist + poisoning detection.
Control objective	Protect training investment (\$50k-\$500k per model) from backdoored data.
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-02 - MODEL EXTRACTION RESISTANCE

Field	Telecommunications implementation guidance
Authoritative GAISSF control text	Rate limiting + diversity detection + extraction monitoring.
Control objective	Protect \$5M+ model IP from theft via API.
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
Authoritative GAISSF control text	Baseline profiling + KL divergence monitoring + accuracy tracking.
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 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
Authoritative GAISSF control text	Gradient anomaly detection + robust aggregation.
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
Authoritative GAISSF control text	Adversarial training + certified robustness measurement.
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; 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
Authoritative GAISSF control text	PQC signing (ML-DSA/SLH-DSA) + PQC key exchange (ML-KEM).
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
Authoritative GAISSF control text	Adapter scanning + provenance verification + registry allowlist.
Control objective	Protect fine-tuning pipeline (\$50k-\$500k per model) from backdoored adapters.
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-08 - MODEL MERGE ATTACK DETECTION

Field	Telecommunications implementation guidance
Authoritative GAISSF control text	Pre-registration behavioural evaluation + regression testing.
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
Authoritative GAISSF control text	Cross-precision behavioural comparison + delta threshold monitoring.
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 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
Authoritative GAISSF control text	Input validation + adversarial pattern matching + system prompt isolation + guardrail sidecar.
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
Authoritative GAISSF control text	Contextual separation + source allowlisting + output validation + RAG sanitization pipeline.
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.
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
Authoritative GAISSF control text	Quarterly red-team prompt library + adversarial training + automated refusal monitoring.
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
Authoritative GAISSF control text	Multi-modal content scanning + steganography detection + modality-specific guardrails.
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; 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
Authoritative GAISSF control text	Parameter schema validation + allowlist enforcement + sandboxed execution.
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
Authoritative GAISSF control text	Context window segmentation + prompt anchoring + attention boundary enforcement.
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 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
Authoritative GAISSF control text	Role-based tool scoping + policy-as-code + dynamic permission revocation.

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
Authoritative GAISSF control text	mTLS for agent mesh + message signing + payload validation.
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.
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
Authoritative GAISSF control text	Cross-session behavioural correlation + chain pattern detection + anomaly scoring.
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
Authoritative GAISSF control text	Sensor integrity verification + safety interlocks + fail-safe state enforcement.
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-critical, legally compliant or immune to conventional cyber threats.

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

Field	Telecommunications implementation guidance
Authoritative GAISSF control text	SPIFFE/SPIRE workload identity + short-lived certificates + continuous attestation.
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
Authoritative GAISSF control text	User-scoped memory isolation + encryption at rest + query-level access controls.
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 threats.

D3-CTL-07 - SECURE MEMORY LIFECYCLE MANAGEMENT

Field	Telecommunications implementation guidance
Authoritative GAISSF control text	Cryptographic deletion + lifecycle policy enforcement + retention auditing.
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
Authoritative GAISSF control text	Automated BOM generation + version tracking + registry synchronization.
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
Authoritative GAISSF control text	Static analysis + deserialization sandboxing + signature verification.
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
Authoritative GAISSF control text	Provenance verification + license compliance + security scorecard.
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
Authoritative GAISSF control text	Tool-call logging + anomaly detection + access control enforcement.
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
Authoritative GAISSF control text	Contractual security requirements + penetration testing + data flow mapping.
Control objective	Evaluate third-party AI APIs for security, privacy, and compliance 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
Authoritative GAISSF control text	Network traffic analysis + SaaS discovery + policy enforcement.
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
Authoritative GAISSF control text	Dependency scanning + CVE matching + automated patching.
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
Authoritative GAISSF control text	Content safety classifier + refusal engine.
Control objective	Avoid regulatory fines (EU AI Act up to €35M) + brand damage.
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
Authoritative GAISSF control text	PII detection + masking + access controls.
Control objective	Avoid GDPR fines up to €20M or 4% global revenue.
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
Authoritative GAISSF control text	n-gram overlap detection + refusal.
Control objective	Avoid copyright litigation (statutory damages up to

	\$150k per work).
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
Authoritative GAISSF control text	C2PA-compliant watermarking + tamper resistance testing.
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
Authoritative GAISSF control text	Data minimization + purpose limitation + machine unlearning.
Control objective	Comply with GDPR Art. 25 + CCPA.
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
Authoritative GAISSF control text	Differential privacy + membership inference testing.
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
Authoritative GAISSF control text	Approval workflow + policy enforcement + audit log.
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
Authoritative GAISSF control text	Structured logging + SIEM integration + retention enforcement.
Control objective	Enable forensic investigation + regulatory compliance.
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
Authoritative GAISSF control text	Standardized template + version control + public accessibility.
Control objective	Enable transparency + 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
Authoritative GAISSF control text	AI-IR runbook + tabletop exercises + containment automation.
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
Authoritative GAISSF control text	Access revocation + decommission audit + scheduled lifecycle.
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
Authoritative GAISSF control text	Contractual security requirements + annual assessment + audit rights.
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
Authoritative GAISSF control text	Failover systems + degraded mode + RTO/RPO definition.
Control objective	Ensure AI availability under stress.
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.

D7-CTL-H01 - AI-GENERATED PHISHING SIMULATION

Field	Telecommunications implementation guidance
-------	--

Authoritative GAISSF control text	Simulation campaigns + click tracking + remedial training.
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 - DEEFAKE DETECTION TRAINING

Field	Telecommunications implementation guidance
Authoritative GAISSF control text	Training modules + quiz + simulated attacks.
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 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
Authoritative GAISSF control text	Independent channel verification + policy enforcement.
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
Authoritative GAISSF control text	Tabletop exercises + IR plan + verification triggers.
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 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
Authoritative GAISSF control text	AI-generated phishing detection + SOC tuning + response automation.
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
Authoritative GAISSF control text	Risk classification framework + conformity assessment.
Control objective	Ensure compliance with binding EU law.
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-02 - ISO 42001 GAP ANALYSIS

Field	Telecommunications implementation guidance
Authoritative GAISSF control text	Gap analysis methodology + remediation tracking.
Control objective	Enable formal certification.
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
Authoritative GAISSF control text	Technical documentation + training data summary + copyright attestation.
Control objective	Comply with EU AI Act Art. 53.
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-04 - DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)

Field	Telecommunications implementation guidance
Authoritative GAISSF control text	Incident classification + notification workflow + SLA monitoring.
Control objective	Comply with DORA 4-hour notification requirement.
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
Authoritative GAISSF control text	Secure development practices + attestation.
Control objective	Enable US federal procurement.
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.

D9-CTL-01 - PHYSICAL HARM BOUNDARY ENFORCEMENT

Field	Telecommunications implementation guidance
Authoritative GAISSF control text	Independent safety monitor (hardware or DO-178C Level A / IEC 61508 SIL 3 certified software) running in parallel with AI inference. Safety monitor enforces: maximum force/velocity/temperature/current limits; geofencing for autonomous systems; exclusion zones; rate-of-change limits for safety-critical parameters. AI output gated through safety monitor — monitor vetoes any out-of-boundary command without AI system awareness.
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.
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
Authoritative GAISSF control text	For each AI-controlled system, document: safe state definition (autonomous vehicle: controlled stop; surgical robot: tool withdrawal; industrial arm: immediate stop and hold); transition time to safe state (must be within stopping distance/reaction time for physical context); trigger conditions for safe state entry; recovery procedure. Implement degraded mode ladder: Full AI control → AI-assisted human control → Manual-only → Safe state.
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 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.
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
Authoritative GAISSF control text	Hardware emergency stop: physical E-stop accessible without any software mediation. AI system must not be able to disable, delay, or circumvent E-stop. Software override: human operator interface that immediately transfers control to safe state. Override must be possible when: AI communication is disrupted; AI system is under adversarial attack; AI model is producing anomalous outputs. Override authority must be unconditional — no AI reasoning, confidence scoring, or approval process may delay or prevent

	override activation.
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.
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
Authoritative GAISSF control text	Three-layer anomaly detection: (1) Sensor layer — statistical validation of sensor readings against physical models; flag readings deviating $>3\sigma$ from model prediction; cross-validate against redundant sensor channels. (2) Actuator layer — monitor command streams for sequences inconsistent with operating context; flag commands outside physically feasible envelope. (3) AI inference layer — apply GAISSF® D2-CTL-01 (Prompt Injection Detection) equivalent for physical AI inputs; monitor input feature distributions for adversarial perturbation signatures. All detections trigger immediate safe state entry (D9-CTL-02) and incident record with root_cause_category = Adversarial_Attack, root_cause_specific_type = Cyber_Physical_Attack.
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.
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
Authoritative GAISSF control text	Sensor integrity monitoring covering: (1) Hardware health — sensor self-test results, calibration drift indicators, environmental exposure limits. Alert when sensor confidence falls below threshold. (2) Data plausibility — real-time statistical validation against physical laws, historical baselines, and redundant sensor cross-validation. (3) Degraded sensor handling — explicit policy for each sensor failure mode: degrade gracefully (reduce AI authority, increase human oversight) or enter safe state. (4) Calibration management — automated alert when calibration certificates expire; block AI system from operational use with expired sensor calibration.
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.
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-06 - ACTUATOR COMMAND VERIFICATION

Field	Telecommunications implementation guidance
Authoritative GAISSF control text	Pre-execution verification gate on every actuator command: (1) Physical bounds check — command value within safe operating envelope for current system state. (2) Sequence plausibility check — command consistent with prior sequence; flag implausible state transitions for human review. (3) Rate-of-change check — rate of change does not exceed safe limits (acceleration rate, force application rate, temperature change rate). (4) Dual-approval for irreversible actions — actuator commands causing irreversible physical changes (cutting, welding, demolition, high-energy discharge) require hardware interlock confirmation. Verification gate implemented in IEC 61508 SIL 3 certified software or hardware logic independent of AI model.
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.
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
Authoritative GAISSF control text	(1) Continuous ring-buffer recording — minimum 60-second rolling buffer of: all sensor inputs (raw and processed); all AI model inputs and outputs; all actuator commands; all safety monitor decisions; all human override activations; system health telemetry. Safety-critical systems retain 300 seconds minimum. (2) Incident freeze — on any safety-relevant event, automatically freeze buffer and begin extended logging. Frozen buffer write-protected. (3) Cryptographic integrity — all records SHA-256 hashed and ECDSA signed at point of creation. For Optimized tier: CRYSTALS-Dilithium signing (post-quantum). (4) Regulatory retention — ICAO Annex 13: 5 years minimum; EU AI Act Art. 19: 10 years; DORA Art. 12: 5 years. (5) UAIF® integration — automatically populate UAIF® incident record from evidence package.
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.
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.

Publication recommendation: Publication Candidate - substantive review corrections incorporated. Final telecom engineering, jurisdiction-specific legal/regulatory, accessibility and page-by-page visual sign-off remain open.

16. Publication Readiness Report

Item	Result
Files planned	9 coordinated deliverables
Authoritative input	GAISSE-NOR-001 v1.0 corrected final publication edition, 29 June 2026
Control count	59
Cross-file control IDs	Matched across DOCX, CSV, JSON and workbooks
JSON validation	Parsed; unique IDs; required fields present
Open reviews	Telecommunications engineering, jurisdiction-specific legal/regulatory, accessibility and final editorial review
Known limitation	Sector interpretations are generic and require operator-specific validation
Recommendation	Ready with minor corrections after specialist review