GAISSF Critical Infrastructure Sector Implementation Guide

SEC-042 | Version 1.1 | Refined Controlled Pre-Release
Physical AI, Cyber-Physical and OT/ICS Implementation Guidance

Published by ODA3 Institute

Document Control

Field	Controlled Value
Document ID	SEC-042
Version	1.1
Status	Refined Controlled Pre-Release
Authoritative baseline	GAISSF v1.0 - 59 controls
Publisher	ODA3 Institute
Publication channel	Website / GitHub
Publication date	Not assigned
Open gates	Named approvals; OT/ICS SME; functional-safety; subsector engineering; legal/regulatory applicability; final accessibility and publication QA

Legal, Reliance and Control-Integrity Notice

This informative sector guide does not modify GAISSF-NOR-001 or GAISSF-NOR-004. It does not constitute legal advice, establish regulatory compliance, certify functional safety, assign a Safety Integrity Level, replace process hazard analysis, or guarantee incident prevention. Exact applicability of external standards and laws must be verified by qualified personnel using controlled sources.

1. Executive Summary

SEC-042 translates the 59-control GAISSF baseline into critical-infrastructure implementation guidance for enterprise IT, OT/ICS, cyber-physical and physical-AI systems. Version 1.1 removes generic scaling, prohibits uncontrolled adversarial testing on live actuation paths, introduces air-gap and black-box-vendor protocols, synchronizes evidence formats, and adds energy, water and healthcare-infrastructure context.

Leadership decisions: define where AI may operate; bound operational authority; require representative non-production validation; maintain independent safety and fallback mechanisms; document supplier opacity and residual risk; and suspend AI-enabled functions when evidence, timing or safe-state assumptions fail.

2. OT/ICS Testing Boundary

Adversarial, poisoning, fault-injection, unsafe-command and destructive tests must be executed in a high-fidelity digital twin, hardware-in-the-loop rig or strictly isolated staging network. They must not be routed through a live production control or actuation path unless a separately approved safety case, controlled change window, rollback plan and accountable engineering authority explicitly authorize the test.

Boundary Element	Minimum Expectation
Representative environment	Mirror relevant interfaces, latency, data characteristics, protections, failure states and operator workflow.
No unintended actuation	Physically or logically prevent test traffic from reaching live actuators or safety functions.
Air-gap transfer	Use approved media, malware scanning, SHA-256 verification, dual authorization, custody manifest and reconciliation.
Latency assurance	Measure worst-case added latency/jitter against the approved deterministic timing budget.
Restoration	Verify clean restoration, configuration integrity and safe operation after testing.

3. Criticality Classification

Factor	1 - Low	3 - Material	5 - Severe
Consequence	Administrative inconvenience	Material service degradation	Potential loss of life, major environmental harm or

			systemic disruption
Autonomy	Advisory	Human-approved execution	Autonomous/high-speed execution
Speed	Hours/days to intervene	Minutes	Milliseconds/seconds
Reversibility	Easily reversible	Costly recovery	Irreversible physical effect
Detectability	Obvious	Delayed	Latent or misleading
Concentration	Single low-impact use	Multiple systems/sites	Common-mode multi-site dependency
Fallback	Proven manual mode	Constrained fallback	No credible immediate fallback
Uncertainty	Well understood	Material gaps	Opaque/novel with high uncertainty

The workbook provides customizable thresholds. The score supports triage only; engineering judgment and consequence pathways govern the approved class.

4. Cross-Control CI Implementation Baseline

Authority

Document advisory, approval, execution, suspension, override and restoration authority.

Safety independence

AI and AI-security controls must not replace or delay independently required protective functions.

Evidence

Tie evidence to system ID, site, deployed version, period, owner, scope and limitations.

Fallback

Test manual, degraded and safe-state modes with realistic staffing and communications.

Supplier opacity

Separate vendor assertion from independent boundary evidence and record residual risk.

Human factors

Test alarm fatigue, automation bias, shift workload and emergency takeover.

5. Vendor Assertion vs Independent Boundary Testing

Where a supplier will not disclose training data, model weights or internal design, the operator should not fabricate provenance. Record the vendor assertion, evidence date and limitations; independently test observable inputs, outputs, timing, network dependencies, update mechanisms, logging, failure behaviour and fallback; and submit unresolved opacity for residual-risk acceptance.

6. Subsector Annexes

Energy and Power

- Grid balancing and protection coordination
- IEC 61850/DNP3 timing and restoration
- NERC CIP applicability must be verified by jurisdiction and asset scope

Water and Wastewater

- Treatment chemistry and dosing limits
- Remote pumping, pressure and water-quality monitoring
- Manual sampling and safe dosing fallback

Healthcare Infrastructure

- Medical IoT and facilities systems
- Patient-support infrastructure and clinical engineering
- No substitution for medical-device, clinical-safety or patient-safety obligations

7. Evidence Grades and Tiers

Grade/Tier	Meaning
G1	Design evidence only
G2	Implemented configuration or procedure
G3	Operating-effectiveness evidence from controlled simulation/HIL or representative operations
G4	Independent assurance
T1	Primary organization-controlled record
T2	Verified secondary or supplier evidence
T3	Controlled simulation, digital twin or HIL evidence
T4	Independent assessment or functional-safety/security assurance

8. Day 1 Triage

Priority	Immediate action
1	Inventory AI-enabled assets, embedded vendor AI, data paths and actuation interfaces.
2	Identify CI-3/4/5 systems and prohibit unapproved autonomous or write authority.
3	Verify D9-CTL-03 human override/emergency stop and D9-CTL-02 safe-state behaviour.
4	Apply D6-CTL-01 human authority and D4-CTL-06 shadow-AI discovery adapted to OT constraints.
5	Confirm fallback, local operation and critical cloud/API dependencies.
6	Establish isolated test boundary and air-gap transfer process.
7	Record black-box supplier gaps and boundary-testing plan.
8	Preserve logs and incident evidence without impairing deterministic timing.

9. Control-by-Control CI Interpretation

D1-CTL-01 - DATASET PROVENANCE & POISONING PREVENTION

Field	CI-Specific Record
Authoritative requirement	Hash verification + source allowlist + poisoning detection.
Business objective	Preserve trustworthy operational decisions by preventing corrupted data or model state from causing unsafe control recommendations, missed degradation, service interruption or cascading cyber-physical effects (Dataset Provenance & Poisoning Prevention).
OT-adapted equivalent	Use signed offline manifests, approved removable-media transfer, local hash registries and isolated scanning when continuous repositories or CI/CD are unavailable.
CI-1 to CI-5	CI-1: Document source, model or dataset identity; perform periodic integrity review and retain a reproducible baseline. | CI-2: Add approved provenance records, version-controlled integrity checks

	and representative offline validation before material changes. | CI-3: Use automated integrity verification, independent challenge of high-impact changes and tested rollback to the last known-good model/data state. | CI-4: Require cryptographically protected provenance, dual authorization for high-impact changes, isolated adversarial testing and continuous integrity monitoring at trust boundaries. | CI-5: Use hardware-backed or independently anchored attestation where feasible, multi-party approval, redundant validation paths, safety-engineering review and evidence that integrity controls do not impair deterministic operations.
Evidence requirement	Signed JSON/CSV manifest containing asset/model/data version, hashes, source, test results, thresholds, exceptions and reviewer.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Detection of novel poisoning methods not represented in the approved test corpus; assurance against an authorized insider able to alter both data and trusted provenance records; proof that source allowlisting establishes semantic correctness.

D1-CTL-02 - MODEL EXTRACTION RESISTANCE

Field	CI-Specific Record
Authoritative requirement	Rate limiting + diversity detection + extraction monitoring.
Business objective	Preserve trustworthy operational decisions by preventing corrupted data or model state from causing unsafe control recommendations, missed degradation, service interruption or cascading cyber-physical effects (Model Extraction Resistance).
OT-adapted equivalent	Use signed offline manifests, approved removable-media transfer, local hash registries and isolated scanning when continuous repositories or CI/CD are unavailable.
CI-1 to CI-5	CI-1: Document source, model or dataset identity; perform periodic integrity review and retain a reproducible baseline. | CI-2: Add approved provenance records, version-controlled integrity checks and representative offline validation before material changes. | CI-3: Use automated integrity verification, independent challenge of high-impact changes and tested rollback to the last known-good model/data state. | CI-4: Require cryptographically protected provenance, dual authorization for high-impact changes, isolated adversarial testing and continuous integrity monitoring at trust boundaries. | CI-5: Use hardware-backed or independently anchored attestation where feasible, multi-party approval, redundant validation paths, safety-engineering review and evidence that integrity controls do not impair deterministic operations.
Evidence requirement	Signed JSON/CSV manifest containing asset/model/data version, hashes, source, test results, thresholds, exceptions and reviewer.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee that rate limits or output controls prevent all model inference; proof that protected model logic cannot be approximated through physical-process observation or compromised vendor tooling.

D1-CTL-03 - BEHAVIORAL DRIFT DETECTION

Field	CI-Specific Record
Authoritative requirement	Baseline profiling + KL divergence monitoring + accuracy tracking.
Business objective	Preserve trustworthy operational decisions by preventing corrupted data or model state from causing unsafe control recommendations, missed degradation, service interruption or cascading cyber-

	physical effects (Behavioral Drift Detection).
OT-adapted equivalent	Use signed offline manifests, approved removable-media transfer, local hash registries and isolated scanning when continuous repositories or CI/CD are unavailable.
CI-1 to CI-5	CI-1: Document source, model or dataset identity; perform periodic integrity review and retain a reproducible baseline. | CI-2: Add approved provenance records, version-controlled integrity checks and representative offline validation before material changes. | CI-3: Use automated integrity verification, independent challenge of high-impact changes and tested rollback to the last known-good model/data state. | CI-4: Require cryptographically protected provenance, dual authorization for high-impact changes, isolated adversarial testing and continuous integrity monitoring at trust boundaries. | CI-5: Use hardware-backed or independently anchored attestation where feasible, multi-party approval, redundant validation paths, safety-engineering review and evidence that integrity controls do not impair deterministic operations.
Evidence requirement	Signed JSON/CSV manifest containing asset/model/data version, hashes, source, test results, thresholds, exceptions and reviewer.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A universal drift threshold; assurance that statistically stable behaviour remains operationally safe; detection of changes hidden by sensor faults, seasonal shifts or coordinated manipulation.

D1-CTL-04 - FEDERATED LEARNING POISONING PREVENTION

Field	CI-Specific Record
Authoritative requirement	Gradient anomaly detection + robust aggregation.
Business objective	Preserve trustworthy operational decisions by preventing corrupted data or model state from causing unsafe control recommendations, missed degradation, service interruption or cascading cyber-physical effects (Federated Learning Poisoning Prevention).
OT-adapted equivalent	Use signed offline manifests, approved removable-media transfer, local hash registries and isolated scanning when continuous repositories or CI/CD are unavailable.
CI-1 to CI-5	CI-1: Document source, model or dataset identity; perform periodic integrity review and retain a reproducible baseline. | CI-2: Add approved provenance records, version-controlled integrity checks and representative offline validation before material changes. | CI-3: Use automated integrity verification, independent challenge of high-impact changes and tested rollback to the last known-good model/data state. | CI-4: Require cryptographically protected provenance, dual authorization for high-impact changes, isolated adversarial testing and continuous integrity monitoring at trust boundaries. | CI-5: Use hardware-backed or independently anchored attestation where feasible, multi-party approval, redundant validation paths, safety-engineering review and evidence that integrity controls do not impair deterministic operations.
Evidence requirement	Signed JSON/CSV manifest containing asset/model/data version, hashes, source, test results, thresholds, exceptions and reviewer.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D1-CTL-05 - EMBEDDING SPACE ROBUSTNESS

Field	CI-Specific Record
Authoritative requirement	Adversarial training + certified robustness measurement.
Business objective	Preserve trustworthy operational decisions by preventing corrupted data or model state from causing unsafe control recommendations, missed degradation, service interruption or cascading cyber-physical effects (Embedding Space Robustness).
OT-adapted equivalent	Use signed offline manifests, approved removable-media transfer, local hash registries and isolated scanning when continuous repositories or CI/CD are unavailable.
CI-1 to CI-5	CI-1: Document source, model or dataset identity; perform periodic integrity review and retain a reproducible baseline. | CI-2: Add approved provenance records, version-controlled integrity checks and representative offline validation before material changes. | CI-3: Use automated integrity verification, independent challenge of high-impact changes and tested rollback to the last known-good model/data state. | CI-4: Require cryptographically protected provenance, dual authorization for high-impact changes, isolated adversarial testing and continuous integrity monitoring at trust boundaries. | CI-5: Use hardware-backed or independently anchored attestation where feasible, multi-party approval, redundant validation paths, safety-engineering review and evidence that integrity controls do not impair deterministic operations.
Evidence requirement	Signed JSON/CSV manifest containing asset/model/data version, hashes, source, test results, thresholds, exceptions and reviewer.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

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

Field	CI-Specific Record
Authoritative requirement	PQC signing (ML-DSA/SLH-DSA) + PQC key exchange (ML-KEM).
Business objective	Preserve trustworthy operational decisions by preventing corrupted data or model state from causing unsafe control recommendations, missed degradation, service interruption or cascading cyber-physical effects (Post-Quantum Model Signing & Crypto Hardening).
OT-adapted equivalent	Use signed offline manifests, approved removable-media transfer, local hash registries and isolated scanning when continuous repositories or CI/CD are unavailable.
CI-1 to CI-5	CI-1: Document source, model or dataset identity; perform periodic integrity review and retain a reproducible baseline. | CI-2: Add approved provenance records, version-controlled integrity checks and representative offline validation before material changes. | CI-3: Use automated integrity verification, independent challenge of high-impact changes and tested rollback to the last known-good model/data state. | CI-4: Require cryptographically protected provenance, dual authorization for high-impact changes, isolated adversarial testing and continuous integrity monitoring at trust boundaries. | CI-5: Use hardware-backed or independently anchored attestation where feasible, multi-party approval, redundant validation paths, safety-engineering review and evidence that integrity controls do not impair deterministic operations.
Evidence requirement	Signed JSON/CSV manifest containing asset/model/data version, hashes, source, test results, thresholds, exceptions and reviewer.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved

	safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D1-CTL-07 - LORA/ADAPTER INTEGRITY VERIFICATION

Field	CI-Specific Record
Authoritative requirement	Adapter scanning + provenance verification + registry allowlist.
Business objective	Preserve trustworthy operational decisions by preventing corrupted data or model state from causing unsafe control recommendations, missed degradation, service interruption or cascading cyber-physical effects (Lora/Adapter Integrity Verification).
OT-adapted equivalent	Use signed offline manifests, approved removable-media transfer, local hash registries and isolated scanning when continuous repositories or CI/CD are unavailable.
CI-1 to CI-5	CI-1: Document source, model or dataset identity; perform periodic integrity review and retain a reproducible baseline. | CI-2: Add approved provenance records, version-controlled integrity checks and representative offline validation before material changes. | CI-3: Use automated integrity verification, independent challenge of high-impact changes and tested rollback to the last known-good model/data state. | CI-4: Require cryptographically protected provenance, dual authorization for high-impact changes, isolated adversarial testing and continuous integrity monitoring at trust boundaries. | CI-5: Use hardware-backed or independently anchored attestation where feasible, multi-party approval, redundant validation paths, safety-engineering review and evidence that integrity controls do not impair deterministic operations.
Evidence requirement	Signed JSON/CSV manifest containing asset/model/data version, hashes, source, test results, thresholds, exceptions and reviewer.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D1-CTL-08 - MODEL MERGE ATTACK DETECTION

Field	CI-Specific Record
Authoritative requirement	Pre-registration behavioural evaluation + regression testing.
Business objective	Preserve trustworthy operational decisions by preventing corrupted data or model state from causing unsafe control recommendations, missed degradation, service interruption or cascading cyber-physical effects (Model Merge Attack Detection).
OT-adapted equivalent	Use signed offline manifests, approved removable-media transfer, local hash registries and isolated scanning when continuous repositories or CI/CD are unavailable.
CI-1 to CI-5	CI-1: Document source, model or dataset identity; perform periodic integrity review and retain a reproducible baseline. | CI-2: Add approved provenance records, version-controlled integrity checks and representative offline validation before material changes. | CI-3: Use automated integrity verification, independent challenge of high-impact changes and tested rollback to the last known-good model/data state. | CI-4: Require cryptographically protected provenance, dual authorization for high-impact changes, isolated adversarial testing and continuous integrity monitoring at trust boundaries. | CI-5: Use hardware-backed or independently anchored attestation where feasible, multi-party approval, redundant validation paths, safety-engineering review and evidence

	that integrity controls do not impair deterministic operations.
Evidence requirement	Signed JSON/CSV manifest containing asset/model/data version, hashes, source, test results, thresholds, exceptions and reviewer.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D1-CTL-09 - QUANTIZATION BACKDOOR SCREENING

Field	CI-Specific Record
Authoritative requirement	Cross-precision behavioural comparison + delta threshold monitoring.
Business objective	Preserve trustworthy operational decisions by preventing corrupted data or model state from causing unsafe control recommendations, missed degradation, service interruption or cascading cyber-physical effects (Quantization Backdoor Screening).
OT-adapted equivalent	Use signed offline manifests, approved removable-media transfer, local hash registries and isolated scanning when continuous repositories or CI/CD are unavailable.
CI-1 to CI-5	CI-1: Document source, model or dataset identity; perform periodic integrity review and retain a reproducible baseline. | CI-2: Add approved provenance records, version-controlled integrity checks and representative offline validation before material changes. | CI-3: Use automated integrity verification, independent challenge of high-impact changes and tested rollback to the last known-good model/data state. | CI-4: Require cryptographically protected provenance, dual authorization for high-impact changes, isolated adversarial testing and continuous integrity monitoring at trust boundaries. | CI-5: Use hardware-backed or independently anchored attestation where feasible, multi-party approval, redundant validation paths, safety-engineering review and evidence that integrity controls do not impair deterministic operations.
Evidence requirement	Signed JSON/CSV manifest containing asset/model/data version, hashes, source, test results, thresholds, exceptions and reviewer.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D2-CTL-01 - DIRECT PROMPT INJECTION PREVENTION

Field	CI-Specific Record
Authoritative requirement	Input validation + adversarial pattern matching + system prompt isolation + guardrail sidecar.
Business objective	Prevent adversarial inputs or tool manipulation from bypassing authority boundaries, confusing operators or initiating unsafe operational actions (Direct Prompt Injection Prevention).
OT-adapted equivalent	Execute adversarial testing only in a digital twin, HIL rig or isolated staging zone. Production testing requires a separately approved safety case and must not expose actuation paths.
CI-1 to CI-5	CI-1: Apply input constraints and documented misuse testing in a non-production test environment. | CI-2: Add representative adversarial test cases, response logging and periodic rule/model review. | CI-3: Use isolated red-team testing, tool-call allowlists,

	privilege boundaries and independent review of bypass findings. | CI-4: Validate guardrails in a high-fidelity shadow environment; require pre-execution authorization for write or actuation tools and rapid isolation capability. | CI-5: Prohibit uncontrolled adversarial testing on production; use HIL/digital-twin testing, deterministic non-AI safety enforcement and independent safety/security acceptance.
Evidence requirement	Signed test report containing payload class, environment, target version, blocked/allowed outcome, tool call, privilege boundary, latency and restoration result.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Protection against every semantic or multimodal jailbreak; permission to test adversarial payloads against live production control paths; assurance that pattern matching alone blocks novel attacks.

D2-CTL-02 - INDIRECT PROMPT INJECTION PREVENTION

Field	CI-Specific Record
Authoritative requirement	Contextual separation + source allowlisting + output validation + RAG sanitization pipeline.
Business objective	Prevent adversarial inputs or tool manipulation from bypassing authority boundaries, confusing operators or initiating unsafe operational actions (Indirect Prompt Injection Prevention).
OT-adapted equivalent	Execute adversarial testing only in a digital twin, HIL rig or isolated staging zone. Production testing requires a separately approved safety case and must not expose actuation paths.
CI-1 to CI-5	CI-1: Apply input constraints and documented misuse testing in a non-production test environment. | CI-2: Add representative adversarial test cases, response logging and periodic rule/model review. | CI-3: Use isolated red-team testing, tool-call allowlists, privilege boundaries and independent review of bypass findings. | CI-4: Validate guardrails in a high-fidelity shadow environment; require pre-execution authorization for write or actuation tools and rapid isolation capability. | CI-5: Prohibit uncontrolled adversarial testing on production; use HIL/digital-twin testing, deterministic non-AI safety enforcement and independent safety/security acceptance.
Evidence requirement	Signed test report containing payload class, environment, target version, blocked/allowed outcome, tool call, privilege boundary, latency and restoration result.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Protection against every semantic or multimodal jailbreak; permission to test adversarial payloads against live production control paths; assurance that pattern matching alone blocks novel attacks.

D2-CTL-03 - JAILBREAK RESISTANCE TESTING

Field	CI-Specific Record
Authoritative requirement	Quarterly red-team prompt library + adversarial training + automated refusal monitoring.
Business objective	Prevent adversarial inputs or tool manipulation from bypassing authority boundaries, confusing operators or initiating unsafe operational actions (Jailbreak Resistance Testing).
OT-adapted equivalent	Execute adversarial testing only in a digital twin, HIL rig or isolated staging zone. Production testing requires a separately approved

	safety case and must not expose actuation paths.
CI-1 to CI-5	CI-1: Apply input constraints and documented misuse testing in a non-production test environment. | CI-2: Add representative adversarial test cases, response logging and periodic rule/model review. | CI-3: Use isolated red-team testing, tool-call allowlists, privilege boundaries and independent review of bypass findings. | CI-4: Validate guardrails in a high-fidelity shadow environment; require pre-execution authorization for write or actuation tools and rapid isolation capability. | CI-5: Prohibit uncontrolled adversarial testing on production; use HIL/digital-twin testing, deterministic non-AI safety enforcement and independent safety/security acceptance.
Evidence requirement	Signed test report containing payload class, environment, target version, blocked/allowed outcome, tool call, privilege boundary, latency and restoration result.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D2-CTL-04 - MULTI-MODAL INJECTION DEFENSE

Field	CI-Specific Record
Authoritative requirement	Multi-modal content scanning + steganography detection + modality-specific guardrails.
Business objective	Prevent adversarial inputs or tool manipulation from bypassing authority boundaries, confusing operators or initiating unsafe operational actions (Multi-Modal Injection Defense).
OT-adapted equivalent	Execute adversarial testing only in a digital twin, HIL rig or isolated staging zone. Production testing requires a separately approved safety case and must not expose actuation paths.
CI-1 to CI-5	CI-1: Apply input constraints and documented misuse testing in a non-production test environment. | CI-2: Add representative adversarial test cases, response logging and periodic rule/model review. | CI-3: Use isolated red-team testing, tool-call allowlists, privilege boundaries and independent review of bypass findings. | CI-4: Validate guardrails in a high-fidelity shadow environment; require pre-execution authorization for write or actuation tools and rapid isolation capability. | CI-5: Prohibit uncontrolled adversarial testing on production; use HIL/digital-twin testing, deterministic non-AI safety enforcement and independent safety/security acceptance.
Evidence requirement	Signed test report containing payload class, environment, target version, blocked/allowed outcome, tool call, privilege boundary, latency and restoration result.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

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

Field	CI-Specific Record
Authoritative requirement	Parameter schema validation + allowlist enforcement + sandboxed execution.

Business objective	Prevent adversarial inputs or tool manipulation from bypassing authority boundaries, confusing operators or initiating unsafe operational actions (Function Call/Tool Call Injection Prevention).
OT-adapted equivalent	Execute adversarial testing only in a digital twin, HIL rig or isolated staging zone. Production testing requires a separately approved safety case and must not expose actuation paths.
CI-1 to CI-5	CI-1: Apply input constraints and documented misuse testing in a non-production test environment. | CI-2: Add representative adversarial test cases, response logging and periodic rule/model review. | CI-3: Use isolated red-team testing, tool-call allowlists, privilege boundaries and independent review of bypass findings. | CI-4: Validate guardrails in a high-fidelity shadow environment; require pre-execution authorization for write or actuation tools and rapid isolation capability. | CI-5: Prohibit uncontrolled adversarial testing on production; use HIL/digital-twin testing, deterministic non-AI safety enforcement and independent safety/security acceptance.
Evidence requirement	Signed test report containing payload class, environment, target version, blocked/allowed outcome, tool call, privilege boundary, latency and restoration result.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D2-CTL-06 - CROSS-CONTEXT HIJACKING MITIGATION

Field	CI-Specific Record
Authoritative requirement	Context window segmentation + prompt anchoring + attention boundary enforcement.
Business objective	Prevent adversarial inputs or tool manipulation from bypassing authority boundaries, confusing operators or initiating unsafe operational actions (Cross-Context Hijacking Mitigation).
OT-adapted equivalent	Execute adversarial testing only in a digital twin, HIL rig or isolated staging zone. Production testing requires a separately approved safety case and must not expose actuation paths.
CI-1 to CI-5	CI-1: Apply input constraints and documented misuse testing in a non-production test environment. | CI-2: Add representative adversarial test cases, response logging and periodic rule/model review. | CI-3: Use isolated red-team testing, tool-call allowlists, privilege boundaries and independent review of bypass findings. | CI-4: Validate guardrails in a high-fidelity shadow environment; require pre-execution authorization for write or actuation tools and rapid isolation capability. | CI-5: Prohibit uncontrolled adversarial testing on production; use HIL/digital-twin testing, deterministic non-AI safety enforcement and independent safety/security acceptance.
Evidence requirement	Signed test report containing payload class, environment, target version, blocked/allowed outcome, tool call, privilege boundary, latency and restoration result.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D3-CTL-01 - LEAST AGENCY ENFORCEMENT

Field	CI-Specific Record
Authoritative requirement	Role-based tool scoping + policy-as-code + dynamic permission revocation.
Business objective	Maintain enforceable identity, privilege and trust boundaries across segmented and intermittently connected IT/OT environments (Least Agency Enforcement).
OT-adapted equivalent	Where continuous attestation is infeasible, use hardware roots of trust, signed build/maintenance manifests, physical key custody, scheduled offline verification and controlled maintenance access.
CI-1 to CI-5	CI-1: Document identities, roles and trust boundaries; use least privilege appropriate to the deployment. | CI-2: Use managed identities, periodic access review and offline-verifiable credentials where continuous connectivity is unavailable. | CI-3: Require strong workload identity, segmented trust zones and dual control for privileged changes. | CI-4: Use hardware roots of trust or compensating physical controls, short-lived or batched signed credentials, and monitored cross-zone access. | CI-5: Integrate identity decisions with safety authority boundaries; maintain independently enforceable deny states and tested offline operation.
Evidence requirement	Identity/credential inventory, signed configuration export, access review, offline attestation log and exception record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D3-CTL-02 - INTER-AGENT COMMUNICATION SECURITY

Field	CI-Specific Record
Authoritative requirement	mTLS for agent mesh + message signing + payload validation.
Business objective	Maintain enforceable identity, privilege and trust boundaries across segmented and intermittently connected IT/OT environments (Inter-Agent Communication Security).
OT-adapted equivalent	Where continuous attestation is infeasible, use hardware roots of trust, signed build/maintenance manifests, physical key custody, scheduled offline verification and controlled maintenance access.
CI-1 to CI-5	CI-1: Document identities, roles and trust boundaries; use least privilege appropriate to the deployment. | CI-2: Use managed identities, periodic access review and offline-verifiable credentials where continuous connectivity is unavailable. | CI-3: Require strong workload identity, segmented trust zones and dual control for privileged changes. | CI-4: Use hardware roots of trust or compensating physical controls, short-lived or batched signed credentials, and monitored cross-zone access. | CI-5: Integrate identity decisions with safety authority boundaries; maintain independently enforceable deny states and tested offline operation.
Evidence requirement	Identity/credential inventory, signed configuration export, access review, offline attestation log and exception record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D3-CTL-03 - AGENTIC PROMPT CHAINING DETECTION

Field	CI-Specific Record
Authoritative requirement	Cross-session behavioural correlation + chain pattern detection + anomaly scoring.
Business objective	Maintain enforceable identity, privilege and trust boundaries across segmented and intermittently connected IT/OT environments (Agentic Prompt Chaining Detection).
OT-adapted equivalent	Where continuous attestation is infeasible, use hardware roots of trust, signed build/maintenance manifests, physical key custody, scheduled offline verification and controlled maintenance access.
CI-1 to CI-5	CI-1: Document identities, roles and trust boundaries; use least privilege appropriate to the deployment. | CI-2: Use managed identities, periodic access review and offline-verifiable credentials where continuous connectivity is unavailable. | CI-3: Require strong workload identity, segmented trust zones and dual control for privileged changes. | CI-4: Use hardware roots of trust or compensating physical controls, short-lived or batched signed credentials, and monitored cross-zone access. | CI-5: Integrate identity decisions with safety authority boundaries; maintain independently enforceable deny states and tested offline operation.
Evidence requirement	Identity/credential inventory, signed configuration export, access review, offline attestation log and exception record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D3-CTL-04 - EMBODIED AI SAFETY CONTROLS

Field	CI-Specific Record
Authoritative requirement	Sensor integrity verification + safety interlocks + fail-safe state enforcement.
Business objective	Maintain enforceable identity, privilege and trust boundaries across segmented and intermittently connected IT/OT environments (Embodied Ai Safety Controls).
OT-adapted equivalent	Where continuous attestation is infeasible, use hardware roots of trust, signed build/maintenance manifests, physical key custody, scheduled offline verification and controlled maintenance access.
CI-1 to CI-5	CI-1: Document identities, roles and trust boundaries; use least privilege appropriate to the deployment. | CI-2: Use managed identities, periodic access review and offline-verifiable credentials where continuous connectivity is unavailable. | CI-3: Require strong workload identity, segmented trust zones and dual control for privileged changes. | CI-4: Use hardware roots of trust or compensating physical controls, short-lived or batched signed credentials, and monitored cross-zone access. | CI-5: Integrate identity decisions with safety authority boundaries; maintain independently enforceable deny states and tested offline operation.
Evidence requirement	Identity/credential inventory, signed configuration export, access review, offline attestation log and exception record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

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

Field	CI-Specific Record
Authoritative requirement	SPIFFE/SPIRE workload identity + short-lived certificates + continuous attestation.
Business objective	Maintain enforceable identity, privilege and trust boundaries across segmented and intermittently connected IT/OT environments (Multi-Agent Trust Chain Attestation).
OT-adapted equivalent	Where continuous attestation is infeasible, use hardware roots of trust, signed build/maintenance manifests, physical key custody, scheduled offline verification and controlled maintenance access.
CI-1 to CI-5	CI-1: Document identities, roles and trust boundaries; use least privilege appropriate to the deployment. | CI-2: Use managed identities, periodic access review and offline-verifiable credentials where continuous connectivity is unavailable. | CI-3: Require strong workload identity, segmented trust zones and dual control for privileged changes. | CI-4: Use hardware roots of trust or compensating physical controls, short-lived or batched signed credentials, and monitored cross-zone access. | CI-5: Integrate identity decisions with safety authority boundaries; maintain independently enforceable deny states and tested offline operation.
Evidence requirement	Identity/credential inventory, signed configuration export, access review, offline attestation log and exception record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	An assumption of continuous external connectivity or cloud control-plane access; a requirement to deploy SPIFFE/SPIRE where offline hardware identity, signed manifests or physical controls provide a justified equivalent.

D3-CTL-06 - PERSISTENT MEMORY EXFILTRATION PREVENTION

Field	CI-Specific Record
Authoritative requirement	User-scoped memory isolation + encryption at rest + query-level access controls.
Business objective	Maintain enforceable identity, privilege and trust boundaries across segmented and intermittently connected IT/OT environments (Persistent Memory Exfiltration Prevention).
OT-adapted equivalent	Where continuous attestation is infeasible, use hardware roots of trust, signed build/maintenance manifests, physical key custody, scheduled offline verification and controlled maintenance access.
CI-1 to CI-5	CI-1: Document identities, roles and trust boundaries; use least privilege appropriate to the deployment. | CI-2: Use managed identities, periodic access review and offline-verifiable credentials where continuous connectivity is unavailable. | CI-3: Require strong workload identity, segmented trust zones and dual control for privileged changes. | CI-4: Use hardware roots of trust or compensating physical controls, short-lived or batched signed credentials, and monitored cross-zone access. | CI-5: Integrate identity decisions with safety authority boundaries; maintain independently enforceable deny states and tested offline operation.
Evidence requirement	Identity/credential inventory, signed configuration export, access review, offline attestation log and exception record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D3-CTL-07 - SECURE MEMORY LIFECYCLE MANAGEMENT

Field	CI-Specific Record
Authoritative requirement	Cryptographic deletion + lifecycle policy enforcement + retention auditing.
Business objective	Maintain enforceable identity, privilege and trust boundaries across segmented and intermittently connected IT/OT environments (Secure Memory Lifecycle Management).
OT-adapted equivalent	Where continuous attestation is infeasible, use hardware roots of trust, signed build/maintenance manifests, physical key custody, scheduled offline verification and controlled maintenance access.
CI-1 to CI-5	CI-1: Document identities, roles and trust boundaries; use least privilege appropriate to the deployment. | CI-2: Use managed identities, periodic access review and offline-verifiable credentials where continuous connectivity is unavailable. | CI-3: Require strong workload identity, segmented trust zones and dual control for privileged changes. | CI-4: Use hardware roots of trust or compensating physical controls, short-lived or batched signed credentials, and monitored cross-zone access. | CI-5: Integrate identity decisions with safety authority boundaries; maintain independently enforceable deny states and tested offline operation.
Evidence requirement	Identity/credential inventory, signed configuration export, access review, offline attestation log and exception record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

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

Field	CI-Specific Record
Authoritative requirement	Automated BOM generation + version tracking + registry synchronization.
Business objective	Make AI-enabled assets and supplier dependencies visible enough to manage outages, vulnerabilities, unsupported components and unauthorized deployment (Ai Bill Of Materials (Ai Bom) Maintenance).
OT-adapted equivalent	Where vendor internals are unavailable, record vendor assertions separately from independently observed boundary behaviour, network dependencies, update paths and failure modes.
CI-1 to CI-5	CI-1: Maintain a basic inventory of AI-enabled assets, suppliers and interfaces. | CI-2: Add version, owner, data path, network zone and support-status records. | CI-3: Require supplier evidence or documented boundary testing where internals are unavailable; monitor unauthorized AI use. | CI-4: Maintain site-level dependency maps, signed inventory changes and contingency plans for opaque suppliers. | CI-5: Use independent boundary assurance, contractual escalation, replacement/containment plans and executive acceptance of unresolved supplier opacity.
Evidence requirement	AI/asset BOM, supplier disclosure record, dependency map, boundary-test report and unsupported-component decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	An assumption that suppliers disclose model weights or training data; acceptance of vendor assertions as conclusive evidence where independent boundary testing is feasible.

D4-CTL-02 - MODEL FILE & ARTIFACT SCANNING

Field	CI-Specific Record
Authoritative requirement	Static analysis + deserialization sandboxing + signature verification.
Business objective	Make AI-enabled assets and supplier dependencies visible enough to manage outages, vulnerabilities, unsupported components and unauthorized deployment (Model File & Artifact Scanning).
OT-adapted equivalent	Where vendor internals are unavailable, record vendor assertions separately from independently observed boundary behaviour, network dependencies, update paths and failure modes.
CI-1 to CI-5	CI-1: Maintain a basic inventory of AI-enabled assets, suppliers and interfaces. | CI-2: Add version, owner, data path, network zone and support-status records. | CI-3: Require supplier evidence or documented boundary testing where internals are unavailable; monitor unauthorized AI use. | CI-4: Maintain site-level dependency maps, signed inventory changes and contingency plans for opaque suppliers. | CI-5: Use independent boundary assurance, contractual escalation, replacement/containment plans and executive acceptance of unresolved supplier opacity.
Evidence requirement	AI/asset BOM, supplier disclosure record, dependency map, boundary-test report and unsupported-component decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D4-CTL-03 - MODEL HUB & REGISTRY VETTING

Field	CI-Specific Record
Authoritative requirement	Provenance verification + license compliance + security scorecard.
Business objective	Make AI-enabled assets and supplier dependencies visible enough to manage outages, vulnerabilities, unsupported components and unauthorized deployment (Model Hub & Registry Vetting).
OT-adapted equivalent	Where vendor internals are unavailable, record vendor assertions separately from independently observed boundary behaviour, network dependencies, update paths and failure modes.
CI-1 to CI-5	CI-1: Maintain a basic inventory of AI-enabled assets, suppliers and interfaces. | CI-2: Add version, owner, data path, network zone and support-status records. | CI-3: Require supplier evidence or documented boundary testing where internals are unavailable; monitor unauthorized AI use. | CI-4: Maintain site-level dependency maps, signed inventory changes and contingency plans for opaque suppliers. | CI-5: Use independent boundary assurance, contractual escalation, replacement/containment plans and executive acceptance of unresolved supplier opacity.
Evidence requirement	AI/asset BOM, supplier disclosure record, dependency map, boundary-test report and unsupported-component decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D4-CTL-04 - MCP SERVER BEHAVIORAL MONITORING

Field	CI-Specific Record
Authoritative requirement	Tool-call logging + anomaly detection + access control enforcement.
Business objective	Make AI-enabled assets and supplier dependencies visible enough to

	manage outages, vulnerabilities, unsupported components and unauthorized deployment (Mcp Server Behavioral Monitoring).
OT-adapted equivalent	Where vendor internals are unavailable, record vendor assertions separately from independently observed boundary behaviour, network dependencies, update paths and failure modes.
CI-1 to CI-5	CI-1: Maintain a basic inventory of AI-enabled assets, suppliers and interfaces. | CI-2: Add version, owner, data path, network zone and support-status records. | CI-3: Require supplier evidence or documented boundary testing where internals are unavailable; monitor unauthorized AI use. | CI-4: Maintain site-level dependency maps, signed inventory changes and contingency plans for opaque suppliers. | CI-5: Use independent boundary assurance, contractual escalation, replacement/containment plans and executive acceptance of unresolved supplier opacity.
Evidence requirement	AI/asset BOM, supplier disclosure record, dependency map, boundary-test report and unsupported-component decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

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

Field	CI-Specific Record
Authoritative requirement	Contractual security requirements + penetration testing + data flow mapping.
Business objective	Make AI-enabled assets and supplier dependencies visible enough to manage outages, vulnerabilities, unsupported components and unauthorized deployment (Third-Party Ai Api Security Assessment).
OT-adapted equivalent	Where vendor internals are unavailable, record vendor assertions separately from independently observed boundary behaviour, network dependencies, update paths and failure modes.
CI-1 to CI-5	CI-1: Maintain a basic inventory of AI-enabled assets, suppliers and interfaces. | CI-2: Add version, owner, data path, network zone and support-status records. | CI-3: Require supplier evidence or documented boundary testing where internals are unavailable; monitor unauthorized AI use. | CI-4: Maintain site-level dependency maps, signed inventory changes and contingency plans for opaque suppliers. | CI-5: Use independent boundary assurance, contractual escalation, replacement/containment plans and executive acceptance of unresolved supplier opacity.
Evidence requirement	AI/asset BOM, supplier disclosure record, dependency map, boundary-test report and unsupported-component decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D4-CTL-06 - SHADOW AI DISCOVERY & GOVERNANCE

Field	CI-Specific Record
Authoritative requirement	Network traffic analysis + SaaS discovery + policy enforcement.
Business objective	Make AI-enabled assets and supplier dependencies visible enough to manage outages, vulnerabilities, unsupported components and unauthorized deployment (Shadow Ai Discovery & Governance).
OT-adapted equivalent	Where vendor internals are unavailable, record vendor assertions separately from independently observed boundary behaviour,

	network dependencies, update paths and failure modes.
CI-1 to CI-5	CI-1: Maintain a basic inventory of AI-enabled assets, suppliers and interfaces. | CI-2: Add version, owner, data path, network zone and support-status records. | CI-3: Require supplier evidence or documented boundary testing where internals are unavailable; monitor unauthorized AI use. | CI-4: Maintain site-level dependency maps, signed inventory changes and contingency plans for opaque suppliers. | CI-5: Use independent boundary assurance, contractual escalation, replacement/containment plans and executive acceptance of unresolved supplier opacity.
Evidence requirement	AI/asset BOM, supplier disclosure record, dependency map, boundary-test report and unsupported-component decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Visibility into every offline engineering workstation, removable-media workflow or embedded vendor feature; authorization to deploy discovery agents where they could affect validated OT configurations.

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

Field	CI-Specific Record
Authoritative requirement	Dependency scanning + CVE matching + automated patching.
Business objective	Make AI-enabled assets and supplier dependencies visible enough to manage outages, vulnerabilities, unsupported components and unauthorized deployment (Ai Software Composition Analysis (Sca)).
OT-adapted equivalent	Where vendor internals are unavailable, record vendor assertions separately from independently observed boundary behaviour, network dependencies, update paths and failure modes.
CI-1 to CI-5	CI-1: Maintain a basic inventory of AI-enabled assets, suppliers and interfaces. | CI-2: Add version, owner, data path, network zone and support-status records. | CI-3: Require supplier evidence or documented boundary testing where internals are unavailable; monitor unauthorized AI use. | CI-4: Maintain site-level dependency maps, signed inventory changes and contingency plans for opaque suppliers. | CI-5: Use independent boundary assurance, contractual escalation, replacement/containment plans and executive acceptance of unresolved supplier opacity.
Evidence requirement	AI/asset BOM, supplier disclosure record, dependency map, boundary-test report and unsupported-component decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A guarantee against zero-day attack paths, authorized-insider misuse or failures outside the tested system boundary; proof of safety, legal compliance or operating effectiveness from design evidence alone.

D5-CTL-01 - HARMFUL CONTENT BLOCKING

Field	CI-Specific Record
Authoritative requirement	Content safety classifier + refusal engine.
Business objective	Prevent generated or transformed content from misleading operators, corrupting approved procedures or causing unsafe service decisions (Harmful Content Blocking).
OT-adapted equivalent	Ground outputs in locally approved procedures and offline repositories; generated instructions must not supersede controlled operating documents.
CI-1 to CI-5	CI-1: Apply task-specific output restrictions and competent review for operational content. | CI-2: Add source grounding, prohibited-content tests and clear operator escalation. | CI-3: Test for misleading instructions, fabricated procedures and unsafe

	operational ambiguity in representative workflows. | CI-4: Prevent direct execution of unverified generated procedures; require authoritative source checks and dual approval for high-impact content. | CI-5: Keep generated content outside deterministic protection functions; use approved procedures, independent validation and emergency fallback communications.
Evidence requirement	Approved source list, output-test corpus, review records, blocked-output log and procedure-control linkage.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A universal definition of harmful content; assurance that filtering prevents misleading but superficially benign operational instructions; permission for generated content to replace approved operating procedures.

D5-CTL-02 - PII LEAKAGE PREVENTION

Field	CI-Specific Record
Authoritative requirement	PII detection + masking + access controls.
Business objective	Prevent generated or transformed content from misleading operators, corrupting approved procedures or causing unsafe service decisions (Pii Leakage Prevention).
OT-adapted equivalent	Ground outputs in locally approved procedures and offline repositories; generated instructions must not supersede controlled operating documents.
CI-1 to CI-5	CI-1: Apply task-specific output restrictions and competent review for operational content. | CI-2: Add source grounding, prohibited-content tests and clear operator escalation. | CI-3: Test for misleading instructions, fabricated procedures and unsafe operational ambiguity in representative workflows. | CI-4: Prevent direct execution of unverified generated procedures; require authoritative source checks and dual approval for high-impact content. | CI-5: Keep generated content outside deterministic protection functions; use approved procedures, independent validation and emergency fallback communications.
Evidence requirement	Approved source list, output-test corpus, review records, blocked-output log and procedure-control linkage.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A universal definition of harmful content; assurance that filtering prevents misleading but superficially benign operational instructions; permission for generated content to replace approved operating procedures.

D5-CTL-03 - COPYRIGHT DETECTION

Field	CI-Specific Record
Authoritative requirement	n-gram overlap detection + refusal.
Business objective	Prevent generated or transformed content from misleading operators, corrupting approved procedures or causing unsafe service decisions (Copyright Detection).
OT-adapted equivalent	Ground outputs in locally approved procedures and offline repositories; generated instructions must not supersede controlled operating documents.
CI-1 to CI-5	CI-1: Apply task-specific output restrictions and competent review for operational content. | CI-2: Add source grounding, prohibited-content tests and clear operator escalation. | CI-3: Test for misleading instructions, fabricated procedures and unsafe operational ambiguity in representative workflows. | CI-4: Prevent direct execution of unverified generated procedures; require authoritative source checks and dual approval for high-impact

	content. | CI-5: Keep generated content outside deterministic protection functions; use approved procedures, independent validation and emergency fallback communications.
Evidence requirement	Approved source list, output-test corpus, review records, blocked-output log and procedure-control linkage.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A universal definition of harmful content; assurance that filtering prevents misleading but superficially benign operational instructions; permission for generated content to replace approved operating procedures.

D5-CTL-04 - AI WATERMARKING ROBUSTNESS

Field	CI-Specific Record
Authoritative requirement	C2PA-compliant watermarking + tamper resistance testing.
Business objective	Prevent generated or transformed content from misleading operators, corrupting approved procedures or causing unsafe service decisions (Ai Watermarking Robustness).
OT-adapted equivalent	Ground outputs in locally approved procedures and offline repositories; generated instructions must not supersede controlled operating documents.
CI-1 to CI-5	CI-1: Apply task-specific output restrictions and competent review for operational content. | CI-2: Add source grounding, prohibited-content tests and clear operator escalation. | CI-3: Test for misleading instructions, fabricated procedures and unsafe operational ambiguity in representative workflows. | CI-4: Prevent direct execution of unverified generated procedures; require authoritative source checks and dual approval for high-impact content. | CI-5: Keep generated content outside deterministic protection functions; use approved procedures, independent validation and emergency fallback communications.
Evidence requirement	Approved source list, output-test corpus, review records, blocked-output log and procedure-control linkage.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A universal definition of harmful content; assurance that filtering prevents misleading but superficially benign operational instructions; permission for generated content to replace approved operating procedures.

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

Field	CI-Specific Record
Authoritative requirement	Data minimization + purpose limitation + machine unlearning.
Business objective	Prevent generated or transformed content from misleading operators, corrupting approved procedures or causing unsafe service decisions (Privacy-By-Design Verification).
OT-adapted equivalent	Ground outputs in locally approved procedures and offline repositories; generated instructions must not supersede controlled operating documents.
CI-1 to CI-5	CI-1: Apply task-specific output restrictions and competent review for operational content. | CI-2: Add source grounding, prohibited-content tests and clear operator escalation. | CI-3: Test for misleading instructions, fabricated procedures and unsafe operational ambiguity in representative workflows. | CI-4: Prevent direct execution of unverified generated procedures; require authoritative source checks and dual approval for high-impact content. | CI-5: Keep generated content outside deterministic protection functions; use approved procedures, independent validation and emergency fallback communications.

Evidence requirement	Approved source list, output-test corpus, review records, blocked-output log and procedure-control linkage.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A universal definition of harmful content; assurance that filtering prevents misleading but superficially benign operational instructions; permission for generated content to replace approved operating procedures.

D5-CTL-06 - PRIVACY-PRESERVING ML VALIDATION

Field	CI-Specific Record
Authoritative requirement	Differential privacy + membership inference testing.
Business objective	Prevent generated or transformed content from misleading operators, corrupting approved procedures or causing unsafe service decisions (Privacy-Preserving Ml Validation).
OT-adapted equivalent	Ground outputs in locally approved procedures and offline repositories; generated instructions must not supersede controlled operating documents.
CI-1 to CI-5	CI-1: Apply task-specific output restrictions and competent review for operational content. | CI-2: Add source grounding, prohibited-content tests and clear operator escalation. | CI-3: Test for misleading instructions, fabricated procedures and unsafe operational ambiguity in representative workflows. | CI-4: Prevent direct execution of unverified generated procedures; require authoritative source checks and dual approval for high-impact content. | CI-5: Keep generated content outside deterministic protection functions; use approved procedures, independent validation and emergency fallback communications.
Evidence requirement	Approved source list, output-test corpus, review records, blocked-output log and procedure-control linkage.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A universal definition of harmful content; assurance that filtering prevents misleading but superficially benign operational instructions; permission for generated content to replace approved operating procedures.

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

Field	CI-Specific Record
Authoritative requirement	Approval workflow + policy enforcement + audit log.
Business objective	Ensure accountable humans retain practical authority to review, reject, suspend and recover AI-enabled operations under normal and emergency conditions (Human-In-The-Loop For High-Risk Actions).
OT-adapted equivalent	Provide physically and logically independent override routes, shift-specific competence, alarm-flood procedures and restoration authority.
CI-1 to CI-5	CI-1: Define decision owner, review point and override route. | CI-2: Train operators and test that review occurs in normal operations. | CI-3: Measure automation bias, alarm suppression and escalation performance under realistic workload. | CI-4: Require explicit approval for high-consequence actions, independent override channels and shift-aware staffing. | CI-5: Use hard authority limits, tested emergency stop/takeover, recurrent simulator exercises and safety-function independence.
Evidence requirement	Authority matrix, approval/override logs, simulator exercise results, staffing/competence records and restoration decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests

	SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Proof that a nominal human-in-the-loop has time, competence, information and authority to intervene; assurance that an override remains usable during alarm floods or degraded communications.

D6-CTL-02 - AUDIT TRAIL COMPLETENESS

Field	CI-Specific Record
Authoritative requirement	Structured logging + SIEM integration + retention enforcement.
Business objective	Ensure accountable humans retain practical authority to review, reject, suspend and recover AI-enabled operations under normal and emergency conditions (Audit Trail Completeness).
OT-adapted equivalent	Provide physically and logically independent override routes, shift-specific competence, alarm-flood procedures and restoration authority.
CI-1 to CI-5	CI-1: Define decision owner, review point and override route. | CI-2: Train operators and test that review occurs in normal operations. | CI-3: Measure automation bias, alarm suppression and escalation performance under realistic workload. | CI-4: Require explicit approval for high-consequence actions, independent override channels and shift-aware staffing. | CI-5: Use hard authority limits, tested emergency stop/takeover, recurrent simulator exercises and safety-function independence.
Evidence requirement	Authority matrix, approval/override logs, simulator exercise results, staffing/competence records and restoration decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Proof that a nominal human-in-the-loop has time, competence, information and authority to intervene; assurance that an override remains usable during alarm floods or degraded communications.

D6-CTL-03 - AI MODEL CARD COMPLETENESS

Field	CI-Specific Record
Authoritative requirement	Standardized template + version control + public accessibility.
Business objective	Ensure accountable humans retain practical authority to review, reject, suspend and recover AI-enabled operations under normal and emergency conditions (Ai Model Card Completeness).
OT-adapted equivalent	Provide physically and logically independent override routes, shift-specific competence, alarm-flood procedures and restoration authority.
CI-1 to CI-5	CI-1: Define decision owner, review point and override route. | CI-2: Train operators and test that review occurs in normal operations. | CI-3: Measure automation bias, alarm suppression and escalation performance under realistic workload. | CI-4: Require explicit approval for high-consequence actions, independent override channels and shift-aware staffing. | CI-5: Use hard authority limits, tested emergency stop/takeover, recurrent simulator exercises and safety-function independence.
Evidence requirement	Authority matrix, approval/override logs, simulator exercise results, staffing/competence records and restoration decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Proof that a nominal human-in-the-loop has time, competence, information and authority to intervene; assurance that an override remains usable during alarm floods or degraded communications.

D6-CTL-04 - AI INCIDENT RESPONSE READINESS

Field	CI-Specific Record
Authoritative requirement	AI-IR runbook + tabletop exercises + containment automation.
Business objective	Ensure accountable humans retain practical authority to review, reject, suspend and recover AI-enabled operations under normal and emergency conditions (Ai Incident Response Readiness).
OT-adapted equivalent	Provide physically and logically independent override routes, shift-specific competence, alarm-flood procedures and restoration authority.
CI-1 to CI-5	CI-1: Define decision owner, review point and override route. | CI-2: Train operators and test that review occurs in normal operations. | CI-3: Measure automation bias, alarm suppression and escalation performance under realistic workload. | CI-4: Require explicit approval for high-consequence actions, independent override channels and shift-aware staffing. | CI-5: Use hard authority limits, tested emergency stop/takeover, recurrent simulator exercises and safety-function independence.
Evidence requirement	Authority matrix, approval/override logs, simulator exercise results, staffing/competence records and restoration decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Proof that a nominal human-in-the-loop has time, competence, information and authority to intervene; assurance that an override remains usable during alarm floods or degraded communications.

D6-CTL-05 - MODEL DEPRECATION & DECOMMISSIONING

Field	CI-Specific Record
Authoritative requirement	Access revocation + decommission audit + scheduled lifecycle.
Business objective	Ensure accountable humans retain practical authority to review, reject, suspend and recover AI-enabled operations under normal and emergency conditions (Model Deprecation & Decommissioning).
OT-adapted equivalent	Provide physically and logically independent override routes, shift-specific competence, alarm-flood procedures and restoration authority.
CI-1 to CI-5	CI-1: Define decision owner, review point and override route. | CI-2: Train operators and test that review occurs in normal operations. | CI-3: Measure automation bias, alarm suppression and escalation performance under realistic workload. | CI-4: Require explicit approval for high-consequence actions, independent override channels and shift-aware staffing. | CI-5: Use hard authority limits, tested emergency stop/takeover, recurrent simulator exercises and safety-function independence.
Evidence requirement	Authority matrix, approval/override logs, simulator exercise results, staffing/competence records and restoration decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Proof that a nominal human-in-the-loop has time, competence, information and authority to intervene; assurance that an override remains usable during alarm floods or degraded communications.

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

Field	CI-Specific Record
Authoritative requirement	Contractual security requirements + annual assessment + audit rights.
Business objective	Ensure accountable humans retain practical authority to review, reject, suspend and recover AI-enabled operations under normal and emergency conditions (Third-Party Ai Vendor Governance).
OT-adapted equivalent	Provide physically and logically independent override routes, shift-

	specific competence, alarm-flood procedures and restoration authority.
CI-1 to CI-5	CI-1: Define decision owner, review point and override route. | CI-2: Train operators and test that review occurs in normal operations. | CI-3: Measure automation bias, alarm suppression and escalation performance under realistic workload. | CI-4: Require explicit approval for high-consequence actions, independent override channels and shift-aware staffing. | CI-5: Use hard authority limits, tested emergency stop/takeover, recurrent simulator exercises and safety-function independence.
Evidence requirement	Authority matrix, approval/override logs, simulator exercise results, staffing/competence records and restoration decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Proof that a nominal human-in-the-loop has time, competence, information and authority to intervene; assurance that an override remains usable during alarm floods or degraded communications.

D6-CTL-07 - AI RESILIENCE & BUSINESS CONTINUITY

Field	CI-Specific Record
Authoritative requirement	Failover systems + degraded mode + RTO/RPO definition.
Business objective	Ensure accountable humans retain practical authority to review, reject, suspend and recover AI-enabled operations under normal and emergency conditions (Ai Resilience & Business Continuity).
OT-adapted equivalent	Provide physically and logically independent override routes, shift-specific competence, alarm-flood procedures and restoration authority.
CI-1 to CI-5	CI-1: Define decision owner, review point and override route. | CI-2: Train operators and test that review occurs in normal operations. | CI-3: Measure automation bias, alarm suppression and escalation performance under realistic workload. | CI-4: Require explicit approval for high-consequence actions, independent override channels and shift-aware staffing. | CI-5: Use hard authority limits, tested emergency stop/takeover, recurrent simulator exercises and safety-function independence.
Evidence requirement	Authority matrix, approval/override logs, simulator exercise results, staffing/competence records and restoration decision.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Proof that a nominal human-in-the-loop has time, competence, information and authority to intervene; assurance that an override remains usable during alarm floods or degraded communications.

D7-CTL-H01 - AI-GENERATED PHISHING SIMULATION

Field	CI-Specific Record
Authoritative requirement	Simulation campaigns + click tracking + remedial training.
Business objective	Reduce foreseeable human, workforce and public harms arising from alarm handling, automation bias, accessibility limits and operational decision support (Ai-Generated Phishing Simulation).
OT-adapted equivalent	Integrate with control-room human-factors, fatigue, alarm-management and emergency-operating analyses.
CI-1 to CI-5	CI-1: Identify affected people and foreseeable operational harms. | CI-2: Add human-factors review, accessibility and complaint/escalation routes. | CI-3: Test alarm fatigue, shift-work cognitive load, disparate effects and emergency usability. | CI-4: Require multidisciplinary human-factors and safety review with monitored override and near-miss learning. | CI-5: Integrate with formal human-reliability and process-safety analysis; do not treat AI assurance as a substitute for those disciplines.

Evidence requirement	Human-factors assessment, alarm-management test, accessibility review, near-miss record and corrective action.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A substitute for human-factors engineering, staffing analysis, accessibility assessment or process-safety review; evidence that absence of complaints means absence of harm.

D7-CTL-H02 - DEEPFAKE DETECTION TRAINING

Field	CI-Specific Record
Authoritative requirement	Training modules + quiz + simulated attacks.
Business objective	Reduce foreseeable human, workforce and public harms arising from alarm handling, automation bias, accessibility limits and operational decision support (Deepfake Detection Training).
OT-adapted equivalent	Integrate with control-room human-factors, fatigue, alarm-management and emergency-operating analyses.
CI-1 to CI-5	CI-1: Identify affected people and foreseeable operational harms. | CI-2: Add human-factors review, accessibility and complaint/escalation routes. | CI-3: Test alarm fatigue, shift-work cognitive load, disparate effects and emergency usability. | CI-4: Require multidisciplinary human-factors and safety review with monitored override and near-miss learning. | CI-5: Integrate with formal human-reliability and process-safety analysis; do not treat AI assurance as a substitute for those disciplines.
Evidence requirement	Human-factors assessment, alarm-management test, accessibility review, near-miss record and corrective action.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A substitute for human-factors engineering, staffing analysis, accessibility assessment or process-safety review; evidence that absence of complaints means absence of harm.

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

Field	CI-Specific Record
Authoritative requirement	Independent channel verification + policy enforcement.
Business objective	Reduce foreseeable human, workforce and public harms arising from alarm handling, automation bias, accessibility limits and operational decision support (Out-Of-Band Authentication).
OT-adapted equivalent	Integrate with control-room human-factors, fatigue, alarm-management and emergency-operating analyses.
CI-1 to CI-5	CI-1: Identify affected people and foreseeable operational harms. | CI-2: Add human-factors review, accessibility and complaint/escalation routes. | CI-3: Test alarm fatigue, shift-work cognitive load, disparate effects and emergency usability. | CI-4: Require multidisciplinary human-factors and safety review with monitored override and near-miss learning. | CI-5: Integrate with formal human-reliability and process-safety analysis; do not treat AI assurance as a substitute for those disciplines.
Evidence requirement	Human-factors assessment, alarm-management test, accessibility review, near-miss record and corrective action.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A substitute for human-factors engineering, staffing analysis, accessibility assessment or process-safety review; evidence that absence of complaints means absence of harm.

D7-CTL-H04 - AI SOCIAL ENGINEERING IR

Field	CI-Specific Record
Authoritative requirement	Tabletop exercises + IR plan + verification triggers.
Business objective	Reduce foreseeable human, workforce and public harms arising from alarm handling, automation bias, accessibility limits and operational decision support (Ai Social Engineering Ir).
OT-adapted equivalent	Integrate with control-room human-factors, fatigue, alarm-management and emergency-operating analyses.
CI-1 to CI-5	CI-1: Identify affected people and foreseeable operational harms. | CI-2: Add human-factors review, accessibility and complaint/escalation routes. | CI-3: Test alarm fatigue, shift-work cognitive load, disparate effects and emergency usability. | CI-4: Require multidisciplinary human-factors and safety review with monitored override and near-miss learning. | CI-5: Integrate with formal human-reliability and process-safety analysis; do not treat AI assurance as a substitute for those disciplines.
Evidence requirement	Human-factors assessment, alarm-management test, accessibility review, near-miss record and corrective action.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A substitute for human-factors engineering, staffing analysis, accessibility assessment or process-safety review; evidence that absence of complaints means absence of harm.

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

Field	CI-Specific Record
Authoritative requirement	AI-generated phishing detection + SOC tuning + response automation.
Business objective	Reduce foreseeable human, workforce and public harms arising from alarm handling, automation bias, accessibility limits and operational decision support (Ai-Enhanced External Attack Defense).
OT-adapted equivalent	Integrate with control-room human-factors, fatigue, alarm-management and emergency-operating analyses.
CI-1 to CI-5	CI-1: Identify affected people and foreseeable operational harms. | CI-2: Add human-factors review, accessibility and complaint/escalation routes. | CI-3: Test alarm fatigue, shift-work cognitive load, disparate effects and emergency usability. | CI-4: Require multidisciplinary human-factors and safety review with monitored override and near-miss learning. | CI-5: Integrate with formal human-reliability and process-safety analysis; do not treat AI assurance as a substitute for those disciplines.
Evidence requirement	Human-factors assessment, alarm-management test, accessibility review, near-miss record and corrective action.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A substitute for human-factors engineering, staffing analysis, accessibility assessment or process-safety review; evidence that absence of complaints means absence of harm.

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

Field	CI-Specific Record
Authoritative requirement	Risk classification framework + conformity assessment.
Business objective	Maintain verifiable obligation, documentation and assurance records without overstating regulatory equivalence or certification status (Eu Ai Act Risk Tier Mapping).
OT-adapted equivalent	Use local evidence repositories and signed transfer manifests; verify applicability and editions before formal reliance.

CI-1 to CI-5	CI-1: Maintain an obligation register and record the basis for applicability decisions. | CI-2: Map controls to verified jurisdictional and contractual obligations; retain review evidence. | CI-3: Use qualified legal/regulatory review and trace evidence to the deployed system/version. | CI-4: Coordinate notification, recordkeeping and assurance across sites and critical suppliers. | CI-5: Require executive acceptance of unresolved conflicts and independent verification; no mapping is treated as automatic compliance.
Evidence requirement	Obligation register, applicability rationale, verified source/version, evidence crosswalk and qualified review record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A claim of legal equivalence, certification reciprocity or automatic compliance with any cited framework; jurisdiction-specific legal advice.

D8-CTL-02 - ISO 42001 GAP ANALYSIS

Field	CI-Specific Record
Authoritative requirement	Gap analysis methodology + remediation tracking.
Business objective	Maintain verifiable obligation, documentation and assurance records without overstating regulatory equivalence or certification status (Iso 42001 Gap Analysis).
OT-adapted equivalent	Use local evidence repositories and signed transfer manifests; verify applicability and editions before formal reliance.
CI-1 to CI-5	CI-1: Maintain an obligation register and record the basis for applicability decisions. | CI-2: Map controls to verified jurisdictional and contractual obligations; retain review evidence. | CI-3: Use qualified legal/regulatory review and trace evidence to the deployed system/version. | CI-4: Coordinate notification, recordkeeping and assurance across sites and critical suppliers. | CI-5: Require executive acceptance of unresolved conflicts and independent verification; no mapping is treated as automatic compliance.
Evidence requirement	Obligation register, applicability rationale, verified source/version, evidence crosswalk and qualified review record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A claim of legal equivalence, certification reciprocity or automatic compliance with any cited framework; jurisdiction-specific legal advice.

D8-CTL-03 - GPAI TECHNICAL DOCUMENTATION VERIFICATION

Field	CI-Specific Record
Authoritative requirement	Technical documentation + training data summary + copyright attestation.
Business objective	Maintain verifiable obligation, documentation and assurance records without overstating regulatory equivalence or certification status (Gpai Technical Documentation Verification).
OT-adapted equivalent	Use local evidence repositories and signed transfer manifests; verify applicability and editions before formal reliance.
CI-1 to CI-5	CI-1: Maintain an obligation register and record the basis for applicability decisions. | CI-2: Map controls to verified jurisdictional and contractual obligations; retain review evidence. | CI-3: Use qualified legal/regulatory review and trace evidence to the deployed system/version. | CI-4: Coordinate notification, recordkeeping and assurance across sites and critical suppliers. | CI-5: Require executive acceptance of unresolved conflicts and independent verification; no mapping is treated as automatic compliance.
Evidence requirement	Obligation register, applicability rationale, verified source/version, evidence crosswalk and qualified review record.

Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A claim of legal equivalence, certification reciprocity or automatic compliance with any cited framework; jurisdiction-specific legal advice.

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

Field	CI-Specific Record
Authoritative requirement	Incident classification + notification workflow + SLA monitoring.
Business objective	Maintain verifiable obligation, documentation and assurance records without overstating regulatory equivalence or certification status (Dora Ict Incident Reporting (Financial Sector)).
OT-adapted equivalent	Use local evidence repositories and signed transfer manifests; verify applicability and editions before formal reliance.
CI-1 to CI-5	CI-1: Maintain an obligation register and record the basis for applicability decisions. | CI-2: Map controls to verified jurisdictional and contractual obligations; retain review evidence. | CI-3: Use qualified legal/regulatory review and trace evidence to the deployed system/version. | CI-4: Coordinate notification, recordkeeping and assurance across sites and critical suppliers. | CI-5: Require executive acceptance of unresolved conflicts and independent verification; no mapping is treated as automatic compliance.
Evidence requirement	Obligation register, applicability rationale, verified source/version, evidence crosswalk and qualified review record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A claim of legal equivalence, certification reciprocity or automatic compliance with any cited framework; jurisdiction-specific legal advice.

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

Field	CI-Specific Record
Authoritative requirement	Secure development practices + attestation.
Business objective	Maintain verifiable obligation, documentation and assurance records without overstating regulatory equivalence or certification status (Nist Sp 800-218A Compliance Check).
OT-adapted equivalent	Use local evidence repositories and signed transfer manifests; verify applicability and editions before formal reliance.
CI-1 to CI-5	CI-1: Maintain an obligation register and record the basis for applicability decisions. | CI-2: Map controls to verified jurisdictional and contractual obligations; retain review evidence. | CI-3: Use qualified legal/regulatory review and trace evidence to the deployed system/version. | CI-4: Coordinate notification, recordkeeping and assurance across sites and critical suppliers. | CI-5: Require executive acceptance of unresolved conflicts and independent verification; no mapping is treated as automatic compliance.
Evidence requirement	Obligation register, applicability rationale, verified source/version, evidence crosswalk and qualified review record.
Testing boundary	document/configuration inspection and representative offline test; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	A claim of legal equivalence, certification reciprocity or automatic compliance with any cited framework; jurisdiction-specific legal advice.

D9-CTL-01 - PHYSICAL HARM BOUNDARY ENFORCEMENT

Field	CI-Specific Record
Authoritative requirement	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.
Business objective	Prevent AI-enabled sensing, decision or actuation from defeating physical safety limits, protective functions or safe-state behaviour (Physical Harm Boundary Enforcement).
OT-adapted equivalent	Integrate with the existing functional-safety lifecycle, LOPA/SIF records and deterministic timing budget; security monitoring must not delay protective action.
CI-1 to CI-5	CI-1: Document physical interfaces, safe limits and prohibited actuation; keep AI advisory unless separately approved. | CI-2: Validate safe-state behavior and operator override in an isolated representative environment. | CI-3: Use redundant sensing, command validation, independent monitoring and tested manual takeover. | CI-4: Integrate with LOPA/SIF or equivalent safety lifecycle; verify latency, fail-safe behavior and separation from basic process control. | CI-5: Use independently certified or otherwise justified safety mechanisms, hardwired interlocks where required, HIL testing, emergency-stop validation and independent functional-safety assurance.
Evidence requirement	HIL/digital-twin report, safety-boundary specification, SIF/LOPA linkage, command/override logs, latency assessment and safe-state test.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Replacement of HAZOP, FMEA, LOPA, SIF/SIL engineering, hardware interlocks or statutory process-safety duties; a guarantee that AI security monitors preserve deterministic timing without measured latency evidence.

D9-CTL-02 - SAFE STATE AND GRACEFUL DEGRADATION

Field	CI-Specific Record
Authoritative requirement	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.
Business objective	Prevent AI-enabled sensing, decision or actuation from defeating physical safety limits, protective functions or safe-state behaviour (Safe State And Graceful Degradation).
OT-adapted equivalent	Integrate with the existing functional-safety lifecycle, LOPA/SIF records and deterministic timing budget; security monitoring must not delay protective action.
CI-1 to CI-5	CI-1: Document physical interfaces, safe limits and prohibited actuation; keep AI advisory unless separately approved. | CI-2: Validate safe-state behavior and operator override in an isolated representative environment. | CI-3: Use redundant sensing, command validation, independent monitoring and tested manual takeover. | CI-4: Integrate with LOPA/SIF or equivalent safety lifecycle; verify latency, fail-safe behavior and separation from basic process control. | CI-5: Use independently certified or otherwise justified safety mechanisms, hardwired interlocks where required, HIL testing, emergency-stop validation and independent

	functional-safety assurance.
Evidence requirement	HIL/digital-twin report, safety-boundary specification, SIF/LOPA linkage, command/override logs, latency assessment and safe-state test.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Replacement of HAZOP, FMEA, LOPA, SIF/SIL engineering, hardware interlocks or statutory process-safety duties; a guarantee that AI security monitors preserve deterministic timing without measured latency evidence.

D9-CTL-03 - HUMAN OVERRIDE AND EMERGENCY STOP

Field	CI-Specific Record
Authoritative requirement	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.
Business objective	Prevent AI-enabled sensing, decision or actuation from defeating physical safety limits, protective functions or safe-state behaviour (Human Override And Emergency Stop).
OT-adapted equivalent	Integrate with the existing functional-safety lifecycle, LOPA/SIF records and deterministic timing budget; security monitoring must not delay protective action.
CI-1 to CI-5	CI-1: Document physical interfaces, safe limits and prohibited actuation; keep AI advisory unless separately approved. | CI-2: Validate safe-state behavior and operator override in an isolated representative environment. | CI-3: Use redundant sensing, command validation, independent monitoring and tested manual takeover. | CI-4: Integrate with LOPA/SIF or equivalent safety lifecycle; verify latency, fail-safe behavior and separation from basic process control. | CI-5: Use independently certified or otherwise justified safety mechanisms, hardwired interlocks where required, HIL testing, emergency-stop validation and independent functional-safety assurance.
Evidence requirement	HIL/digital-twin report, safety-boundary specification, SIF/LOPA linkage, command/override logs, latency assessment and safe-state test.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Replacement of HAZOP, FMEA, LOPA, SIF/SIL engineering, hardware interlocks or statutory process-safety duties; a guarantee that AI security monitors preserve deterministic timing without measured latency evidence.

D9-CTL-04 - CYBER-PHYSICAL ATTACK DETECTION

Field	CI-Specific Record
Authoritative requirement	Three-layer anomaly detection: (1) Sensor layer — statistical validation of sensor readings against physical models; flag readings deviating >3σ 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.
Business objective	Prevent AI-enabled sensing, decision or actuation from defeating physical safety limits, protective functions or safe-state behaviour (Cyber-Physical Attack Detection).
OT-adapted equivalent	Integrate with the existing functional-safety lifecycle, LOPA/SIF records and deterministic timing budget; security monitoring must not delay protective action.
CI-1 to CI-5	CI-1: Document physical interfaces, safe limits and prohibited actuation; keep AI advisory unless separately approved. | CI-2: Validate safe-state behavior and operator override in an isolated representative environment. | CI-3: Use redundant sensing, command validation, independent monitoring and tested manual takeover. | CI-4: Integrate with LOPA/SIF or equivalent safety lifecycle; verify latency, fail-safe behavior and separation from basic process control. | CI-5: Use independently certified or otherwise justified safety mechanisms, hardwired interlocks where required, HIL testing, emergency-stop validation and independent functional-safety assurance.
Evidence requirement	HIL/digital-twin report, safety-boundary specification, SIF/LOPA linkage, command/override logs, latency assessment and safe-state test.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Replacement of HAZOP, FMEA, LOPA, SIF/SIL engineering, hardware interlocks or statutory process-safety duties; a guarantee that AI security monitors preserve deterministic timing without measured latency evidence.

D9-CTL-05 - PHYSICAL ENVIRONMENT INTEGRITY MONITORING

Field	CI-Specific Record
Authoritative requirement	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.
Business objective	Prevent AI-enabled sensing, decision or actuation from defeating physical safety limits, protective functions or safe-state behaviour (Physical Environment Integrity Monitoring).
OT-adapted equivalent	Integrate with the existing functional-safety lifecycle, LOPA/SIF records and deterministic timing budget; security monitoring must not delay protective action.
CI-1 to CI-5	CI-1: Document physical interfaces, safe limits and prohibited actuation; keep AI advisory unless separately approved. | CI-2: Validate safe-state behavior and operator override in an isolated representative environment. | CI-3: Use redundant sensing, command validation, independent monitoring and tested manual takeover. | CI-4: Integrate with LOPA/SIF or equivalent safety lifecycle; verify latency, fail-safe behavior and separation from basic process control. | CI-5: Use independently certified or otherwise justified safety mechanisms, hardwired interlocks where required, HIL testing, emergency-stop validation and independent functional-safety assurance.

Evidence requirement	HIL/digital-twin report, safety-boundary specification, SIF/LOPA linkage, command/override logs, latency assessment and safe-state test.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Replacement of HAZOP, FMEA, LOPA, SIF/SIL engineering, hardware interlocks or statutory process-safety duties; a guarantee that AI security monitors preserve deterministic timing without measured latency evidence.

D9-CTL-06 - ACTUATOR COMMAND VERIFICATION

Field	CI-Specific Record
Authoritative requirement	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.
Business objective	Prevent AI-enabled sensing, decision or actuation from defeating physical safety limits, protective functions or safe-state behaviour (Actuator Command Verification).
OT-adapted equivalent	Integrate with the existing functional-safety lifecycle, LOPA/SIF records and deterministic timing budget; security monitoring must not delay protective action.
CI-1 to CI-5	CI-1: Document physical interfaces, safe limits and prohibited actuation; keep AI advisory unless separately approved. | CI-2: Validate safe-state behavior and operator override in an isolated representative environment. | CI-3: Use redundant sensing, command validation, independent monitoring and tested manual takeover. | CI-4: Integrate with LOPA/SIF or equivalent safety lifecycle; verify latency, fail-safe behavior and separation from basic process control. | CI-5: Use independently certified or otherwise justified safety mechanisms, hardwired interlocks where required, HIL testing, emergency-stop validation and independent functional-safety assurance.
Evidence requirement	HIL/digital-twin report, safety-boundary specification, SIF/LOPA linkage, command/override logs, latency assessment and safe-state test.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Replacement of HAZOP, FMEA, LOPA, SIF/SIL engineering, hardware interlocks or statutory process-safety duties; a guarantee that AI security monitors preserve deterministic timing without measured latency evidence.

D9-CTL-07 - PHYSICAL INCIDENT EVIDENCE PRESERVATION

Field	CI-Specific Record
Authoritative requirement	(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.
Business objective	Prevent AI-enabled sensing, decision or actuation from defeating physical safety limits, protective functions or safe-state behaviour (Physical Incident Evidence Preservation).
OT-adapted equivalent	Integrate with the existing functional-safety lifecycle, LOPA/SIF records and deterministic timing budget; security monitoring must not delay protective action.
CI-1 to CI-5	CI-1: Document physical interfaces, safe limits and prohibited actuation; keep AI advisory unless separately approved. | CI-2: Validate safe-state behavior and operator override in an isolated representative environment. | CI-3: Use redundant sensing, command validation, independent monitoring and tested manual takeover. | CI-4: Integrate with LOPA/SIF or equivalent safety lifecycle; verify latency, fail-safe behavior and separation from basic process control. | CI-5: Use independently certified or otherwise justified safety mechanisms, hardwired interlocks where required, HIL testing, emergency-stop validation and independent functional-safety assurance.
Evidence requirement	HIL/digital-twin report, safety-boundary specification, SIF/LOPA linkage, command/override logs, latency assessment and safe-state test.
Testing boundary	high-fidelity digital twin, hardware-in-the-loop rig, or strictly isolated staging network; Adversarial, poisoning, fault-injection and unsafe-command tests SHALL NOT be routed through a live production control or actuation path unless a separately approved safety case, change window and rollback plan explicitly authorize the test.
Notably Absent	Replacement of HAZOP, FMEA, LOPA, SIF/SIL engineering, hardware interlocks or statutory process-safety duties; a guarantee that AI security monitors preserve deterministic timing without measured latency evidence.

10. Threat Register Summary

ID	Threat	Primary Controls	Owner	Evidence Boundary
CI-THR-001	Manipulated sensor data	D1-CTL-01; D1-CTL-03; D9-CTL-05	OT engineering / CISO	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-002	Training-data poisoning	D1-CTL-01; D1-CTL-04	Data owner / CISO	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-003	Compromised model update	D1-CTL-04; D3-CTL-05; D4-CTL-01	Model owner / OT engineering	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-004	Prompt injection affecting operator assistant	D2-CTL-01; D2-CTL-02; D6-CTL-01	CISO / operations	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.

CI-THR-005	Indirect prompt injection	D2-CTL-01; D2-CTL-02; D5-CTL-01	CISO / application owner	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-006	Unauthorized tool execution	D2-CTL-03; D3-CTL-01; D6-CTL-01	CISO / system owner	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-007	Excessive agent permissions	D2-CTL-03; D3-CTL-01; D4-CTL-01	CISO / system owner	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-008	Cloud/API outage	D4-CTL-01; D4-CTL-04; D9-CTL-02	Resilience lead / operations	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-009	Model drift or concept drift	D1-CTL-03; D6-CTL-01	Model owner / operations	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-010	Automation bias and alarm suppression	D6-CTL-01; D7-CTL-01; D7-CTL-02	Operations / human factors	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-011	Common-mode model failure across sites	D1-CTL-03; D4-CTL-01; D9-CTL-02	Enterprise architecture / resilience	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-012	Unsafe AI-generated code/configuration	D2-CTL-03; D4-CTL-03; D9-CTL-06	Engineering authority / CISO	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-013	Loss of audit logging	D4-CTL-05; D9-CTL-07	CISO / evidence custodian	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-014	Opaque supplier AI component	D1-CTL-01; D4-CTL-01; D8-CTL-03	Procurement / system owner	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-015	Unauthorized shadow AI	D4-CTL-06; D3-CTL-01	CISO / site manager	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-016	Emergency-mode failure	D6-CTL-01; D9-CTL-02;	Operations / safety lead	Public, verified telemetry

		D9-CTL-03		on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-017	Sensor spoofing	D9-CTL-04; D9-CTL-05; D1-CTL-01	OT engineering / safety lead	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-018	Actuator command injection	D9-CTL-01; D9-CTL-06; D3-CTL-01	OT engineering / CISO	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-019	Safety monitor bypass	D9-CTL-01; D9-CTL-03; D9-CTL-07	Functional safety lead	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-020	Adversarial physical input	D2-CTL-04; D9-CTL-04; D9-CTL-05	Engineering / security testing	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-021	Sensor calibration drift	D1-CTL-03; D9-CTL-05	Maintenance / engineering	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.
CI-THR-022	Compromised OT hardware or firmware	D4-CTL-01; D3-CTL-05; D9-CTL-06	Supply chain / CISO	Public, verified telemetry on AI-specific OT incidents remains incomplete; no quantitative likelihood is assigned.

11. Standards Alignment Rules

Mappings in this package are conceptual alignment aids, not claims that a GAISSF control satisfies a law, standard or certification requirement. Exact clauses, editions, asset scope and jurisdiction must be verified against controlled primary sources. External copyrighted standards are not reproduced.

12. Notably Absent

- No assumption of universal vendor cooperation.
- No substitution for HAZOP, FMEA, LOPA, SIF/SIL engineering or sector safety obligations.
- No guarantee that AI guardrails preserve deterministic timing without measured evidence.
- No authorization for uncontrolled production adversarial testing.
- No quantitative likelihood or outage estimate without organization-specific evidence.
- No automatic compliance or certification equivalence.

13. Publication Readiness

Substantive refinement is complete and all 59 controls are present across JSON, CSV and workbooks. Public release remains gated by named document approvals, independent OT/ICS and functional-safety review, subsector review, jurisdiction-specific legal/regulatory verification, controlled-source mapping verification, accessibility review and final publication QA.

Appendix A - Control Reconciliation

Check	Result
Expected controls	59
JSON controls	59
Unique IDs	59
D9 controls	7
Missing/duplicates	None detected
Normative IDs/titles	Preserved from v1.0 source package

Appendix B - Disposition Summary

ID	Feedback	Disposition
DISP-101	Generic criticality scaling	Accepted - domain-specific CI-1 to CI-5 scaling added.
DISP-102	Generic Notably Absent	Accepted - control/domain-specific technical boundaries added.
DISP-103	Production adversarial testing	Accepted - explicit prohibition and isolated/HIL rule added.
DISP-104	IT/SaaS business objectives	Accepted - reframed around safety, availability and cyber-physical consequences.
DISP-105	Evidence disconnect	Accepted - explicit formats, grades, tiers and CI-EV-023 to 026 added.
DISP-106	Subsector nuance	Accepted - energy, water and healthcare-infrastructure annexes/matrix added.
DISP-107	Quantitative likelihood/outage estimates	Rejected unless local evidence exists; qualitative fields retained.
DISP-108	Regulatory equivalence mapping	Modified - conceptual alignment only, verification required.
DISP-109	Blank reviewer names	Not fabricated; role-based review gates recorded as Open.
DISP-110	D9 allegedly missing from JSON	Verified false for v1.0 source: 59 controls and 7 D9 records were present; automated parity retained.