ODA3 Institute

SEC-049

GAISSF Pharmaceutical Sector Implementation Guide

Version 1.1 | *Controlled Pre-Release* | *Informative*

Authoritative baseline: GAISSF-NOR-004 v1.0
59 controls across nine domains

Document Control

Field	Value
Document ID	SEC-049
Version	1.1
Status	Controlled pre-release
Classification	Informative sector implementation guidance
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd (legal and copyright notices only)
Authoritative control source	GAISSF-NOR-004 v1.0 corrected final publication edition
Control baseline	59 controls across nine domains
Publication date	Not assigned
Distribution	Website / GitHub after review gates close

Legal and Use Disclaimer

This guide is an implementation aid. It does not amend GAISSF, provide legal or regulatory advice, determine GxP applicability, establish validation adequacy, confer certification, or guarantee security, safety, product quality, clinical integrity, regulatory compliance or absence of harm. External requirements must be verified for the applicable product, process, jurisdiction and effective date.

Executive Summary

Pharmaceutical AI security intersects with patient safety, product quality, clinical integrity, pharmacovigilance, data integrity, validated-state maintenance, regulated records and supplier dependence. SEC-049 translates each authoritative GAISSF control into sector implementation considerations while preserving the distinction between normative requirements and informative guidance.

1. Purpose, Scope and Audience

This guide supports CISOs, security architects, AI governance leads, quality and validation leaders, pharmacovigilance, clinical operations, regulatory affairs, manufacturing, laboratory, privacy, legal, audit and risk functions. It covers discovery through post-market operations and supporting technology services.

2. Relationship to GAISSF

GAISSF-NOR-004 remains authoritative. The 59 control identifiers and titles are preserved. Pharmaceutical interpretations, examples, evidence suggestions and maturity statements are informative and do not create new conformance obligations.

3. Criticality Model

Tier	Name	Entry criteria	Minimum governance
Tier 1	Administrative or low-impact support	No direct GxP decision or regulated-record effect; reversible; qualified review available.	Inventory, approved use, data handling, access, basic testing, supplier terms and periodic review.
Tier 2	Controlled operational support	Operational dependency or sensitive data, but limited direct patient/product/regulated-decision impact.	Documented risk assessment, monitoring, change control, fallback and supplier assurance.
Tier 3	GxP-significant or regulated decision support	Supports regulated records, clinical conduct, safety, quality or submission evidence; human decision remains accountable.	Validation/assurance plan, traceability, qualified review, robust audit trail, periodic review, incident/deviation integration.
Tier 4	Safety-critical, quality-critical or high-autonomy regulated use	Failure can materially affect patient safety, product quality, critical clinical/safety decisions, or executes high-consequence actions.	Independent approval, rigorous assurance, hard authority limits, continuous monitoring, tested fallback/override, enhanced supplier and incident controls.

4. Use-Case Catalogue

ID	Use case	Owner	Indicative criticality
PHAR-UC-001	Generative AI for regulatory-document drafting	Regulatory Affairs	GxP-significant
PHAR-UC-002	AI-assisted medical writing	Medical Affairs	Controlled operational
PHAR-UC-003	Clinical protocol generation	Clinical Development	GxP-significant
PHAR-UC-004	Participant recruitment and eligibility screening	Clinical Operations	Safety-significant
PHAR-UC-005	Clinical-site selection	Clinical Operations	Controlled operational
PHAR-UC-006	Clinical-data anomaly detection	Clinical Data Management	GxP-significant
PHAR-UC-007	Synthetic control arms	Biostatistics	Safety-significant
PHAR-UC-008	Medical image analysis in trials	Clinical Development	Safety-significant
PHAR-UC-009	Adverse-event intake automation	Pharmacovigilance	Safety-significant
PHAR-UC-010	Adverse-event coding assistance	Pharmacovigilance	GxP-significant
PHAR-UC-011	Pharmacovigilance case prioritisation	Pharmacovigilance	Safety-critical
PHAR-UC-012	Safety signal detection	Pharmacovigilance	Safety-critical
PHAR-UC-013	Literature surveillance	Pharmacovigilance	GxP-significant
PHAR-UC-014	Benefit-risk analysis support	Safety Governance	Safety-critical
PHAR-UC-015	Target identification	Discovery Research	Research
PHAR-UC-016	Molecular generation	Discovery Research	Research
PHAR-UC-017	Compound screening	Discovery Research	Research

PHAR-UC-018	Toxicology prediction	Preclinical Safety	Safety-significant
PHAR-UC-019	Formulation optimisation	Pharmaceutical Development	GxP-significant
PHAR-UC-020	Manufacturing process optimisation	Manufacturing Science	Quality-critical
PHAR-UC-021	Batch record review	Quality Assurance	Quality-critical
PHAR-UC-022	Predictive maintenance	Engineering	Controlled operational
PHAR-UC-023	Automated visual inspection	Quality Control	Quality-critical
PHAR-UC-024	Environmental monitoring analytics	Microbiology / Quality	Quality-critical
PHAR-UC-025	Laboratory result interpretation	Quality Control	Quality-critical
PHAR-UC-026	Deviation investigation support	Quality Assurance	GxP-significant
PHAR-UC-027	CAPA recommendation support	Quality Assurance	GxP-significant
PHAR-UC-028	Quality complaint triage	Product Quality	Safety-significant
PHAR-UC-029	Supply forecasting	Supply Chain	Controlled operational
PHAR-UC-030	Cold-chain anomaly detection	Supply Chain Quality	Quality-critical
PHAR-UC-031	Counterfeit detection	Product Security	Safety-significant
PHAR-UC-032	Serialization analytics	Supply Chain / Compliance	GxP-significant
PHAR-UC-033	Controlled-document knowledge retrieval	Quality Systems	GxP-significant
PHAR-UC-034	Employee training assistant	Learning and Development	Controlled operational
PHAR-UC-035	Inspection-readiness support	Quality Assurance	GxP-significant
PHAR-UC-036	Regulatory intelligence	Regulatory Affairs	Controlled operational
PHAR-UC-037	Product-label content support	Regulatory Affairs	Safety-significant
PHAR-UC-038	Medical-information chat system	Medical Information	Safety-significant
PHAR-UC-039	Patient-facing support tool	Patient Services	Safety-significant
PHAR-UC-040	Third-party foundation-model integration	Enterprise Technology	Variable

5. Threat Register

Each entry is a scenario unless a specific confirmed source is cited. Inclusion does not establish occurrence or prevalence.

ID	Scenario	Evidence status
PHAR-THR-001	Manipulation of drug-discovery training data	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-002	Poisoning of experimental datasets	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-003	Compromise of proprietary molecular data	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-004	Theft of clinical-trial information	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-005	Participant re-identification	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-006	Manipulation of eligibility-screening logic	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-007	Protocol-generation errors	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-008	Fabrication of scientific references	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-009	Inaccurate regulatory content generation	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-010	Unauthorised modification of controlled documents	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-011	Unreviewed model output inserted into regulated records	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-012	Pharmacovigilance case suppression	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-013	Adverse-event misclassification	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-014	Delayed safety-signal detection	Threat-model entry; not evidence that the

		event has occurred.
PHAR-THR-015	False safety signals	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-016	Hallucinated medical information	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-017	Batch-release decision corruption	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-018	Manufacturing parameter manipulation	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-019	Laboratory-result alteration	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-020	Visual-inspection evasion	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-021	Model drift affecting quality decisions	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-022	Unapproved model updates	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-023	Loss of validated state	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-024	Insufficient audit trails	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-025	Weak electronic-signature attribution	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-026	Training-serving skew	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-027	Prompt injection through controlled or supplier documents	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-028	Retrieval corpus poisoning	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-029	Malicious content embedded in scientific literature	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-030	Third-party model compromise	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-031	Cloud-service concentration failure	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-032	Model extraction	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-033	Sensitive-data leakage	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-034	Insecure agentic actions	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-035	Excessive system permissions	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-036	Unauthorised tool use	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-037	Supplier software-update compromise	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-038	Counterfeit-classification evasion	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-039	Cold-chain anomaly concealment	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-040	Business-continuity failure caused by AI dependency	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-041	Integrity failure in CAPA or deviation analysis	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-042	Automation bias	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-043	Underqualified human review	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-044	Inadequate segregation of duties	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-045	Incomplete traceability	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-046	Insufficient reproducibility	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-047	Inability to reconstruct model-supported	Threat-model entry; not evidence that the

	decisions	event has occurred.
PHAR-THR-048	Jurisdictionally incompatible data processing	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-049	Unauthorised cross-border data exposure	Threat-model entry; not evidence that the event has occurred.
PHAR-THR-050	Intellectual-property contamination from external models	Threat-model entry; not evidence that the event has occurred.

6. Control-by-Control Guidance

D1-CTL-01 — DATASET PROVENANCE & POISONING PREVENTION

Element	Content
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative source statement	Hash verification + source allowlist + poisoning detection.
Pharmaceutical interpretation	Protect provenance, integrity, versioning and behavioural stability of models, datasets, embeddings and adapters used across the medicinal-product lifecycle.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-001, PHAR-THR-002, PHAR-THR-021, PHAR-THR-022, PHAR-THR-023, PHAR-THR-026
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D1-CTL-02 — MODEL EXTRACTION RESISTANCE

Element	Content
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative source statement	Rate limiting + diversity detection + extraction monitoring.
Pharmaceutical interpretation	Protect provenance, integrity, versioning and behavioural stability of models, datasets, embeddings and adapters used across the medicinal-product lifecycle.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-001, PHAR-THR-002, PHAR-THR-021, PHAR-THR-022, PHAR-THR-023, PHAR-THR-026
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D1-CTL-03 — BEHAVIORAL DRIFT DETECTION

Element	Content
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative source statement	Baseline profiling + KL divergence monitoring + accuracy tracking.
Pharmaceutical interpretation	Protect provenance, integrity, versioning and behavioural stability of models, datasets, embeddings and adapters used across the medicinal-product lifecycle.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability.

	Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-001, PHAR-THR-002, PHAR-THR-021, PHAR-THR-022, PHAR-THR-023, PHAR-THR-026
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D1-CTL-04 — FEDERATED LEARNING POISONING PREVENTION

Element	Content
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative source statement	Gradient anomaly detection + robust aggregation.
Pharmaceutical interpretation	Protect provenance, integrity, versioning and behavioural stability of models, datasets, embeddings and adapters used across the medicinal-product lifecycle.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability,

	continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-001, PHAR-THR-002, PHAR-THR-021, PHAR-THR-022, PHAR-THR-023, PHAR-THR-026
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D1-CTL-05 — EMBEDDING SPACE ROBUSTNESS

Element	Content
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative source statement	Adversarial training + certified robustness measurement.
Pharmaceutical interpretation	Protect provenance, integrity, versioning and behavioural stability of models, datasets, embeddings and adapters used across the medicinal-product lifecycle.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-001, PHAR-THR-002, PHAR-THR-021, PHAR-THR-022, PHAR-THR-023, PHAR-THR-026
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and

	jurisdiction-specific review.

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

Element	Content
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative source statement	PQC signing (ML-DSA/SLH-DSA) + PQC key exchange (ML-KEM).
Pharmaceutical interpretation	Protect provenance, integrity, versioning and behavioural stability of models, datasets, embeddings and adapters used across the medicinal-product lifecycle.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-001, PHAR-THR-002, PHAR-THR-021, PHAR-THR-022, PHAR-THR-023, PHAR-THR-026
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D1-CTL-07 — LORA/ADAPTER INTEGRITY VERIFICATION

Element	Content
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative source statement	Adapter scanning + provenance verification + registry allowlist.
Pharmaceutical interpretation	Protect provenance, integrity, versioning and behavioural stability of models, datasets, embeddings and adapters used across the medicinal-product lifecycle.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and

	effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-001, PHAR-THR-002, PHAR-THR-021, PHAR-THR-022, PHAR-THR-023, PHAR-THR-026
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D1-CTL-08 — MODEL MERGE ATTACK DETECTION

Element	Content
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative source statement	Pre-registration behavioural evaluation + regression testing.
Pharmaceutical interpretation	Protect provenance, integrity, versioning and behavioural stability of models, datasets, embeddings and adapters used across the medicinal-product lifecycle.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as

	applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-001, PHAR-THR-002, PHAR-THR-021, PHAR-THR-022, PHAR-THR-023, PHAR-THR-026
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D1-CTL-09 — QUANTIZATION BACKDOOR SCREENING

Element	Content
Domain	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS
Authoritative source statement	Cross-precision behavioural comparison + delta threshold monitoring.
Pharmaceutical interpretation	Protect provenance, integrity, versioning and behavioural stability of models, datasets, embeddings and adapters used across the medicinal-product lifecycle.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-001, PHAR-THR-002, PHAR-THR-021, PHAR-THR-022, PHAR-THR-023, PHAR-THR-026
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040

Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D2-CTL-01 — DIRECT PROMPT INJECTION PREVENTION

Element	Content
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative source statement	Input validation + adversarial pattern matching + system prompt isolation + guardrail sidecar.
Pharmaceutical interpretation	Prevent and detect hostile or malformed inputs, unsafe runtime behaviour, identity abuse and compromise of deployed pharmaceutical AI services.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-027, PHAR-THR-029, PHAR-THR-030, PHAR-THR-033, PHAR-THR-035, PHAR-THR-036
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D2-CTL-02 — INDIRECT PROMPT INJECTION PREVENTION

Element	Content
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative source statement	Contextual separation + source allowlisting + output validation + RAG sanitization pipeline.
Pharmaceutical interpretation	Prevent and detect hostile or malformed inputs, unsafe runtime behaviour, identity abuse and compromise of deployed

	pharmaceutical AI services.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-027, PHAR-THR-029, PHAR-THR-030, PHAR-THR-033, PHAR-THR-035, PHAR-THR-036
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D2-CTL-03 — JAILBREAK RESISTANCE TESTING

Element	Content
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative source statement	Quarterly red-team prompt library + adversarial training + automated refusal monitoring.
Pharmaceutical interpretation	Prevent and detect hostile or malformed inputs, unsafe runtime behaviour, identity abuse and compromise of deployed pharmaceutical AI services.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications,

	manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-027, PHAR-THR-029, PHAR-THR-030, PHAR-THR-033, PHAR-THR-035, PHAR-THR-036
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D2-CTL-04 — MULTI-MODAL INJECTION DEFENSE

Element	Content
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative source statement	Multi-modal content scanning + steganography detection + modality-specific guardrails.
Pharmaceutical interpretation	Prevent and detect hostile or malformed inputs, unsafe runtime behaviour, identity abuse and compromise of deployed pharmaceutical AI services.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.

Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-027, PHAR-THR-029, PHAR-THR-030, PHAR-THR-033, PHAR-THR-035, PHAR-THR-036
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative source statement	Parameter schema validation + allowlist enforcement + sandboxed execution.
Pharmaceutical interpretation	Prevent and detect hostile or malformed inputs, unsafe runtime behaviour, identity abuse and compromise of deployed pharmaceutical AI services.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-027, PHAR-THR-029, PHAR-THR-030, PHAR-THR-033, PHAR-THR-035, PHAR-THR-036
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D2-CTL-06 — CROSS-CONTEXT HIJACKING MITIGATION

Element	Content
Domain	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE
Authoritative source statement	Context window segmentation + prompt anchoring + attention boundary enforcement.
Pharmaceutical interpretation	Prevent and detect hostile or malformed inputs, unsafe runtime behaviour, identity abuse and compromise of deployed pharmaceutical AI services.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-027, PHAR-THR-029, PHAR-THR-030, PHAR-THR-033, PHAR-THR-035, PHAR-THR-036
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D3-CTL-01 — LEAST AGENCY ENFORCEMENT

Element	Content
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative source statement	Role-based tool scoping + policy-as-code + dynamic permission revocation.
Pharmaceutical interpretation	Constrain delegation, tools, permissions and autonomous actions in agentic workflows that can affect regulated records, safety, quality or operations.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.

GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-034, PHAR-THR-035, PHAR-THR-036, PHAR-THR-042, PHAR-THR-044, PHAR-THR-047
Mapped use cases	PHAR-UC-001, PHAR-UC-011, PHAR-UC-021, PHAR-UC-026, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D3-CTL-02 — INTER-AGENT COMMUNICATION SECURITY

Element	Content
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative source statement	mTLS for agent mesh + message signing + payload validation.
Pharmaceutical interpretation	Constrain delegation, tools, permissions and autonomous actions in agentic workflows that can affect regulated records, safety, quality or operations.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.

Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-034, PHAR-THR-035, PHAR-THR-036, PHAR-THR-042, PHAR-THR-044, PHAR-THR-047
Mapped use cases	PHAR-UC-001, PHAR-UC-011, PHAR-UC-021, PHAR-UC-026, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D3-CTL-03 — AGENTIC PROMPT CHAINING DETECTION

Element	Content
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative source statement	Cross-session behavioural correlation + chain pattern detection + anomaly scoring.
Pharmaceutical interpretation	Constrain delegation, tools, permissions and autonomous actions in agentic workflows that can affect regulated records, safety, quality or operations.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-034, PHAR-THR-035, PHAR-THR-036, PHAR-THR-042, PHAR-THR-044, PHAR-THR-047
Mapped use cases	PHAR-UC-001, PHAR-UC-011, PHAR-UC-021, PHAR-UC-026, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability,

	establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D3-CTL-04 — EMBODIED AI SAFETY CONTROLS

Element	Content
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative source statement	Sensor integrity verification + safety interlocks + fail-safe state enforcement.
Pharmaceutical interpretation	Constrain delegation, tools, permissions and autonomous actions in agentic workflows that can affect regulated records, safety, quality or operations.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-034, PHAR-THR-035, PHAR-THR-036, PHAR-THR-042, PHAR-THR-044, PHAR-THR-047
Mapped use cases	PHAR-UC-001, PHAR-UC-011, PHAR-UC-021, PHAR-UC-026, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative source statement	SPIFFE/SPIRE workload identity + short-lived certificates + continuous attestation.
Pharmaceutical interpretation	Constrain delegation, tools, permissions and autonomous actions in agentic workflows that can affect regulated records, safety, quality or operations.

Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-034, PHAR-THR-035, PHAR-THR-036, PHAR-THR-042, PHAR-THR-044, PHAR-THR-047
Mapped use cases	PHAR-UC-001, PHAR-UC-011, PHAR-UC-021, PHAR-UC-026, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D3-CTL-06 — PERSISTENT MEMORY EXFILTRATION PREVENTION

Element	Content
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative source statement	User-scoped memory isolation + encryption at rest + query-level access controls.
Pharmaceutical interpretation	Constrain delegation, tools, permissions and autonomous actions in agentic workflows that can affect regulated records, safety, quality or operations.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions,

	complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-034, PHAR-THR-035, PHAR-THR-036, PHAR-THR-042, PHAR-THR-044, PHAR-THR-047
Mapped use cases	PHAR-UC-001, PHAR-UC-011, PHAR-UC-021, PHAR-UC-026, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D3-CTL-07 — SECURE MEMORY LIFECYCLE MANAGEMENT

Element	Content
Domain	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY
Authoritative source statement	Cryptographic deletion + lifecycle policy enforcement + retention auditing.
Pharmaceutical interpretation	Constrain delegation, tools, permissions and autonomous actions in agentic workflows that can affect regulated records, safety, quality or operations.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and

	effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-034, PHAR-THR-035, PHAR-THR-036, PHAR-THR-042, PHAR-THR-044, PHAR-THR-047
Mapped use cases	PHAR-UC-001, PHAR-UC-011, PHAR-UC-021, PHAR-UC-026, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative source statement	Automated BOM generation + version tracking + registry synchronization.
Pharmaceutical interpretation	Govern model, data, cloud, CRO/CMO, laboratory, platform and foundation-model suppliers across acquisition, change and exit.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-030, PHAR-THR-031, PHAR-THR-037, PHAR-THR-048, PHAR-THR-049, PHAR-THR-050
Mapped use cases	PHAR-UC-040, PHAR-UC-006, PHAR-UC-020, PHAR-UC-029
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D4-CTL-02 — MODEL FILE & ARTIFACT SCANNING

Element	Content
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY

Authoritative source statement	Static analysis + deserialization sandboxing + signature verification.
Pharmaceutical interpretation	Govern model, data, cloud, CRO/CMO, laboratory, platform and foundation-model suppliers across acquisition, change and exit.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-030, PHAR-THR-031, PHAR-THR-037, PHAR-THR-048, PHAR-THR-049, PHAR-THR-050
Mapped use cases	PHAR-UC-040, PHAR-UC-006, PHAR-UC-020, PHAR-UC-029
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D4-CTL-03 — MODEL HUB & REGISTRY VETTING

Element	Content
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative source statement	Provenance verification + license compliance + security scorecard.
Pharmaceutical interpretation	Govern model, data, cloud, CRO/CMO, laboratory, platform and foundation-model suppliers across acquisition, change and exit.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions,

	complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-030, PHAR-THR-031, PHAR-THR-037, PHAR-THR-048, PHAR-THR-049, PHAR-THR-050
Mapped use cases	PHAR-UC-040, PHAR-UC-006, PHAR-UC-020, PHAR-UC-029
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D4-CTL-04 — MCP SERVER BEHAVIORAL MONITORING

Element	Content
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative source statement	Tool-call logging + anomaly detection + access control enforcement.
Pharmaceutical interpretation	Govern model, data, cloud, CRO/CMO, laboratory, platform and foundation-model suppliers across acquisition, change and exit.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-030, PHAR-THR-031, PHAR-THR-037, PHAR-THR-048,

	PHAR-THR-049, PHAR-THR-050
Mapped use cases	PHAR-UC-040, PHAR-UC-006, PHAR-UC-020, PHAR-UC-029
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative source statement	Contractual security requirements + penetration testing + data flow mapping.
Pharmaceutical interpretation	Govern model, data, cloud, CRO/CMO, laboratory, platform and foundation-model suppliers across acquisition, change and exit.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-030, PHAR-THR-031, PHAR-THR-037, PHAR-THR-048, PHAR-THR-049, PHAR-THR-050
Mapped use cases	PHAR-UC-040, PHAR-UC-006, PHAR-UC-020, PHAR-UC-029
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D4-CTL-06 — SHADOW AI DISCOVERY & GOVERNANCE

Element	Content
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative source statement	Network traffic analysis + SaaS discovery + policy enforcement.
Pharmaceutical interpretation	Govern model, data, cloud, CRO/CMO, laboratory, platform and foundation-model suppliers across acquisition, change and exit.
Applicability	Apply based on intended use, GxP determination, criticality,

	data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-030, PHAR-THR-031, PHAR-THR-037, PHAR-THR-048, PHAR-THR-049, PHAR-THR-050
Mapped use cases	PHAR-UC-040, PHAR-UC-006, PHAR-UC-020, PHAR-UC-029
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY
Authoritative source statement	Dependency scanning + CVE matching + automated patching.
Pharmaceutical interpretation	Govern model, data, cloud, CRO/CMO, laboratory, platform and foundation-model suppliers across acquisition, change and exit.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.

Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-030, PHAR-THR-031, PHAR-THR-037, PHAR-THR-048, PHAR-THR-049, PHAR-THR-050
Mapped use cases	PHAR-UC-040, PHAR-UC-006, PHAR-UC-020, PHAR-UC-029
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D5-CTL-01 — HARMFUL CONTENT BLOCKING

Element	Content
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative source statement	Content safety classifier + refusal engine.
Pharmaceutical interpretation	Maintain accuracy, grounding, source traceability, controlled-language boundaries and review of generated or classified content.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-007, PHAR-THR-008, PHAR-THR-009, PHAR-THR-010, PHAR-THR-011, PHAR-THR-013
Mapped use cases	PHAR-UC-001, PHAR-UC-002, PHAR-UC-009, PHAR-UC-013, PHAR-UC-033
Limitations and confidence	Sector interpretation does not determine legal applicability,

	establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D5-CTL-02 — PII LEAKAGE PREVENTION

Element	Content
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative source statement	PII detection + masking + access controls.
Pharmaceutical interpretation	Maintain accuracy, grounding, source traceability, controlled-language boundaries and review of generated or classified content.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-007, PHAR-THR-008, PHAR-THR-009, PHAR-THR-010, PHAR-THR-011, PHAR-THR-013
Mapped use cases	PHAR-UC-001, PHAR-UC-002, PHAR-UC-009, PHAR-UC-013, PHAR-UC-033
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D5-CTL-03 — COPYRIGHT DETECTION

Element	Content
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative source statement	n-gram overlap detection + refusal.
Pharmaceutical interpretation	Maintain accuracy, grounding, source traceability, controlled-language boundaries and review of generated or classified content.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership;

	integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-007, PHAR-THR-008, PHAR-THR-009, PHAR-THR-010, PHAR-THR-011, PHAR-THR-013
Mapped use cases	PHAR-UC-001, PHAR-UC-002, PHAR-UC-009, PHAR-UC-013, PHAR-UC-033
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D5-CTL-04 — AI WATERMARKING ROBUSTNESS

Element	Content
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative source statement	C2PA-compliant watermarking + tamper resistance testing.
Pharmaceutical interpretation	Maintain accuracy, grounding, source traceability, controlled-language boundaries and review of generated or classified content.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as

	applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-007, PHAR-THR-008, PHAR-THR-009, PHAR-THR-010, PHAR-THR-011, PHAR-THR-013
Mapped use cases	PHAR-UC-001, PHAR-UC-002, PHAR-UC-009, PHAR-UC-013, PHAR-UC-033
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative source statement	Data minimization + purpose limitation + machine unlearning.
Pharmaceutical interpretation	Maintain accuracy, grounding, source traceability, controlled-language boundaries and review of generated or classified content.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-007, PHAR-THR-008, PHAR-THR-009, PHAR-THR-010, PHAR-THR-011, PHAR-THR-013
Mapped use cases	PHAR-UC-001, PHAR-UC-002, PHAR-UC-009, PHAR-UC-013, PHAR-UC-033
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality,

	compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D5-CTL-06 — PRIVACY-PRESERVING ML VALIDATION

Element	Content
Domain	D5: CONTENT SAFETY & OUTPUT INTEGRITY
Authoritative source statement	Differential privacy + membership inference testing.
Pharmaceutical interpretation	Maintain accuracy, grounding, source traceability, controlled-language boundaries and review of generated or classified content.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-007, PHAR-THR-008, PHAR-THR-009, PHAR-THR-010, PHAR-THR-011, PHAR-THR-013
Mapped use cases	PHAR-UC-001, PHAR-UC-002, PHAR-UC-009, PHAR-UC-013, PHAR-UC-033
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative source statement	Approval workflow + policy enforcement + audit log.
Pharmaceutical interpretation	Establish accountability, intended-use approval, GxP determination, human oversight, evidence, escalation and periodic governance.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and

	effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-022, PHAR-THR-023, PHAR-THR-024, PHAR-THR-025, PHAR-THR-042, PHAR-THR-043
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D6-CTL-02 — AUDIT TRAIL COMPLETENESS

Element	Content
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative source statement	Structured logging + SIEM integration + retention enforcement.
Pharmaceutical interpretation	Establish accountability, intended-use approval, GxP determination, human oversight, evidence, escalation and periodic governance.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.

Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-022, PHAR-THR-023, PHAR-THR-024, PHAR-THR-025, PHAR-THR-042, PHAR-THR-043
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D6-CTL-03 — AI MODEL CARD COMPLETENESS

Element	Content
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative source statement	Standardized template + version control + public accessibility.
Pharmaceutical interpretation	Establish accountability, intended-use approval, GxP determination, human oversight, evidence, escalation and periodic governance.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-022, PHAR-THR-023, PHAR-THR-024, PHAR-THR-025, PHAR-THR-042, PHAR-THR-043
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate

	for generic sector interpretation pending organization- and jurisdiction-specific review.

D6-CTL-04 — AI INCIDENT RESPONSE READINESS

Element	Content
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative source statement	AI-IR runbook + tabletop exercises + containment automation.
Pharmaceutical interpretation	Establish accountability, intended-use approval, GxP determination, human oversight, evidence, escalation and periodic governance.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-022, PHAR-THR-023, PHAR-THR-024, PHAR-THR-025, PHAR-THR-042, PHAR-THR-043
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D6-CTL-05 — MODEL DEPRECATION & DECOMMISSIONING

Element	Content
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative source statement	Access revocation + decommission audit + scheduled lifecycle.
Pharmaceutical interpretation	Establish accountability, intended-use approval, GxP determination, human oversight, evidence, escalation and periodic governance.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.

GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-022, PHAR-THR-023, PHAR-THR-024, PHAR-THR-025, PHAR-THR-042, PHAR-THR-043
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative source statement	Contractual security requirements + annual assessment + audit rights.
Pharmaceutical interpretation	Establish accountability, intended-use approval, GxP determination, human oversight, evidence, escalation and periodic governance.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.

Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-022, PHAR-THR-023, PHAR-THR-024, PHAR-THR-025, PHAR-THR-042, PHAR-THR-043
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D6-CTL-07 — AI RESILIENCE & BUSINESS CONTINUITY

Element	Content
Domain	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT
Authoritative source statement	Failover systems + degraded mode + RTO/RPO definition.
Pharmaceutical interpretation	Establish accountability, intended-use approval, GxP determination, human oversight, evidence, escalation and periodic governance.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-022, PHAR-THR-023, PHAR-THR-024, PHAR-THR-025, PHAR-THR-042, PHAR-THR-043
Mapped use cases	PHAR-UC-006, PHAR-UC-012, PHAR-UC-020, PHAR-UC-025, PHAR-UC-040
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate

	for generic sector interpretation pending organization- and jurisdiction-specific review.

D7-CTL-H01 — AI-GENERATED PHISHING SIMULATION

Element	Content
Domain	D7: HUMAN & SOCIETAL HARMS
Authoritative source statement	Simulation campaigns + click tracking + remedial training.
Pharmaceutical interpretation	Assess participant, patient, workforce and societal harms, including bias, accessibility, privacy, exclusion and automation bias.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-005, PHAR-THR-006, PHAR-THR-042, PHAR-THR-043, PHAR-THR-048, PHAR-THR-049
Mapped use cases	PHAR-UC-004, PHAR-UC-007, PHAR-UC-008, PHAR-UC-039
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D7-CTL-H02 — DEEPFAKE DETECTION TRAINING

Element	Content
Domain	D7: HUMAN & SOCIETAL HARMS
Authoritative source statement	Training modules + quiz + simulated attacks.
Pharmaceutical interpretation	Assess participant, patient, workforce and societal harms, including bias, accessibility, privacy, exclusion and automation bias.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity,

	traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-005, PHAR-THR-006, PHAR-THR-042, PHAR-THR-043, PHAR-THR-048, PHAR-THR-049
Mapped use cases	PHAR-UC-004, PHAR-UC-007, PHAR-UC-008, PHAR-UC-039
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D7: HUMAN & SOCIETAL HARMS
Authoritative source statement	Independent channel verification + policy enforcement.
Pharmaceutical interpretation	Assess participant, patient, workforce and societal harms, including bias, accessibility, privacy, exclusion and automation bias.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.

Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-005, PHAR-THR-006, PHAR-THR-042, PHAR-THR-043, PHAR-THR-048, PHAR-THR-049
Mapped use cases	PHAR-UC-004, PHAR-UC-007, PHAR-UC-008, PHAR-UC-039
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D7-CTL-H04 — AI SOCIAL ENGINEERING IR

Element	Content
Domain	D7: HUMAN & SOCIETAL HARMS
Authoritative source statement	Tabletop exercises + IR plan + verification triggers.
Pharmaceutical interpretation	Assess participant, patient, workforce and societal harms, including bias, accessibility, privacy, exclusion and automation bias.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-005, PHAR-THR-006, PHAR-THR-042, PHAR-THR-043, PHAR-THR-048, PHAR-THR-049
Mapped use cases	PHAR-UC-004, PHAR-UC-007, PHAR-UC-008, PHAR-UC-039
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D7: HUMAN & SOCIETAL HARMS
Authoritative source statement	AI-generated phishing detection + SOC tuning + response automation.
Pharmaceutical interpretation	Assess participant, patient, workforce and societal harms, including bias, accessibility, privacy, exclusion and automation bias.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-005, PHAR-THR-006, PHAR-THR-042, PHAR-THR-043, PHAR-THR-048, PHAR-THR-049
Mapped use cases	PHAR-UC-004, PHAR-UC-007, PHAR-UC-008, PHAR-UC-039
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D8: REGULATORY ALIGNMENT & COMPLIANCE
Authoritative source statement	Risk classification framework + conformity assessment.
Pharmaceutical interpretation	Map legal, regulatory, privacy, resilience and sector obligations without treating GAISSF as a compliance guarantee.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-

	assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-004, PHAR-THR-024, PHAR-THR-048, PHAR-THR-049
Mapped use cases	PHAR-UC-001, PHAR-UC-006, PHAR-UC-009, PHAR-UC-020, PHAR-UC-036
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D8-CTL-02 — ISO 42001 GAP ANALYSIS

Element	Content
Domain	D8: REGULATORY ALIGNMENT & COMPLIANCE
Authoritative source statement	Gap analysis methodology + remediation tracking.
Pharmaceutical interpretation	Map legal, regulatory, privacy, resilience and sector obligations without treating GAISSF as a compliance guarantee.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory

	artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-004, PHAR-THR-024, PHAR-THR-048, PHAR-THR-049
Mapped use cases	PHAR-UC-001, PHAR-UC-006, PHAR-UC-009, PHAR-UC-020, PHAR-UC-036
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D8-CTL-03 — GPAI TECHNICAL DOCUMENTATION VERIFICATION

Element	Content
Domain	D8: REGULATORY ALIGNMENT & COMPLIANCE
Authoritative source statement	Technical documentation + training data summary + copyright attestation.
Pharmaceutical interpretation	Map legal, regulatory, privacy, resilience and sector obligations without treating GAISSF as a compliance guarantee.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-004, PHAR-THR-024, PHAR-THR-048, PHAR-THR-049
Mapped use cases	PHAR-UC-001, PHAR-UC-006, PHAR-UC-009, PHAR-UC-020, PHAR-UC-036
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content

Domain	D8: REGULATORY ALIGNMENT & COMPLIANCE
Authoritative source statement	Incident classification + notification workflow + SLA monitoring.
Pharmaceutical interpretation	Map legal, regulatory, privacy, resilience and sector obligations without treating GAISSF as a compliance guarantee.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-004, PHAR-THR-024, PHAR-THR-048, PHAR-THR-049
Mapped use cases	PHAR-UC-001, PHAR-UC-006, PHAR-UC-009, PHAR-UC-020, PHAR-UC-036
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

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

Element	Content
Domain	D8: REGULATORY ALIGNMENT & COMPLIANCE
Authoritative source statement	Secure development practices + attestation.
Pharmaceutical interpretation	Map legal, regulatory, privacy, resilience and sector obligations without treating GAISSF as a compliance guarantee.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications,

	manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-004, PHAR-THR-024, PHAR-THR-048, PHAR-THR-049
Mapped use cases	PHAR-UC-001, PHAR-UC-006, PHAR-UC-009, PHAR-UC-020, PHAR-UC-036
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D9-CTL-01 — PHYSICAL HARM BOUNDARY ENFORCEMENT

Element	Content
Domain	D9: PHYSICAL AI SAFETY
Authoritative source statement	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.
Pharmaceutical interpretation	Apply cyber-physical safety controls where AI interacts with manufacturing equipment, laboratories, robotics, cold chain or other physical processes.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability,

	continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-017, PHAR-THR-018, PHAR-THR-019, PHAR-THR-020, PHAR-THR-039, PHAR-THR-040
Mapped use cases	PHAR-UC-020, PHAR-UC-022, PHAR-UC-023, PHAR-UC-024, PHAR-UC-030
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D9-CTL-02 — SAFE STATE AND GRACEFUL DEGRADATION

Element	Content
Domain	D9: PHYSICAL AI SAFETY
Authoritative source statement	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.
Pharmaceutical interpretation	Apply cyber-physical safety controls where AI interacts with manufacturing equipment, laboratories, robotics, cold chain or other physical processes.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-017, PHAR-THR-018, PHAR-THR-019, PHAR-THR-020, PHAR-THR-039, PHAR-THR-040

Mapped use cases	PHAR-UC-020, PHAR-UC-022, PHAR-UC-023, PHAR-UC-024, PHAR-UC-030
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D9-CTL-03 — HUMAN OVERRIDE AND EMERGENCY STOP

Element	Content
Domain	D9: PHYSICAL AI SAFETY
Authoritative source statement	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.
Pharmaceutical interpretation	Apply cyber-physical safety controls where AI interacts with manufacturing equipment, laboratories, robotics, cold chain or other physical processes.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-017, PHAR-THR-018, PHAR-THR-019, PHAR-THR-020, PHAR-THR-039, PHAR-THR-040
Mapped use cases	PHAR-UC-020, PHAR-UC-022, PHAR-UC-023, PHAR-UC-024, PHAR-UC-030
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D9-CTL-04 — CYBER-PHYSICAL ATTACK DETECTION

Element	Content
Domain	D9: PHYSICAL AI SAFETY
Authoritative source statement	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.
Pharmaceutical interpretation	Apply cyber-physical safety controls where AI interacts with manufacturing equipment, laboratories, robotics, cold chain or other physical processes.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-017, PHAR-THR-018, PHAR-THR-019, PHAR-THR-020, PHAR-THR-039, PHAR-THR-040
Mapped use cases	PHAR-UC-020, PHAR-UC-022, PHAR-UC-023, PHAR-UC-024, PHAR-UC-030
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D9-CTL-05 — PHYSICAL ENVIRONMENT INTEGRITY MONITORING

Element	Content
Domain	D9: PHYSICAL AI SAFETY
Authoritative source statement	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.
Pharmaceutical interpretation	Apply cyber-physical safety controls where AI interacts with manufacturing equipment, laboratories, robotics, cold chain or other physical processes.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-017, PHAR-THR-018, PHAR-THR-019, PHAR-THR-020, PHAR-THR-039, PHAR-THR-040
Mapped use cases	PHAR-UC-020, PHAR-UC-022, PHAR-UC-023, PHAR-UC-024, PHAR-UC-030
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D9-CTL-06 — ACTUATOR COMMAND VERIFICATION

Element	Content
Domain	D9: PHYSICAL AI SAFETY
Authoritative source statement	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.
Pharmaceutical interpretation	Apply cyber-physical safety controls where AI interacts with manufacturing equipment, laboratories, robotics, cold chain or other physical processes.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-017, PHAR-THR-018, PHAR-THR-019, PHAR-THR-020, PHAR-THR-039, PHAR-THR-040
Mapped use cases	PHAR-UC-020, PHAR-UC-022, PHAR-UC-023, PHAR-UC-024, PHAR-UC-030
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

D9-CTL-07 — PHYSICAL INCIDENT EVIDENCE PRESERVATION

Element	Content
Domain	D9: PHYSICAL AI SAFETY
Authoritative source statement	(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.

Pharmaceutical interpretation	Apply cyber-physical safety controls where AI interacts with manufacturing equipment, laboratories, robotics, cold chain or other physical processes.
Applicability	Apply based on intended use, GxP determination, criticality, data/record impact, autonomy and supplier dependency; document justified exclusions.
Recommended practices	Define an approved control design; assign accountable ownership; integrate with quality/change/incident processes; test operation and effectiveness; retain attributable evidence.
GxP and validation	Where GxP-relevant, preserve validated state, data integrity, traceability, change control, qualified review and reconstructability. Use intended-use and risk-based acceptance criteria; include representative normal, edge, adversarial and failure scenarios; re-assess after material change.
Safety, quality, clinical and PV	Escalate where failure could delay, suppress, distort or miscommunicate information material to participant or patient safety. Assess whether failure could affect specifications, manufacturing parameters, laboratory results, batch decisions, complaints, storage or distribution. Preserve protocol, eligibility, endpoint, data lineage, statistical and source-document integrity where applicable. Test omission, prioritisation, coding and signal-detection failure modes where safety workflows are in scope.
Data integrity	Maintain attributable, legible, contemporaneous, original/true-copy, accurate, complete, consistent, enduring and available records as applicable.
Third parties	Obtain model/data/service transparency sufficient for risk assessment, change notification, incident support, auditability, continuity and exit.
Illustrative evidence	Approved design; risk/GxP assessment; configuration; test results; model/data version records; access/audit logs; monitoring; review and change records. Examples are informative, not mandatory artifacts.
Assessment questions	Is scope approved? Is ownership clear? Can operation and effectiveness be evidenced? Are failures detected and escalated? Can affected decisions and records be reconstructed?
Mapped threats	PHAR-THR-017, PHAR-THR-018, PHAR-THR-019, PHAR-THR-020, PHAR-THR-039, PHAR-THR-040
Mapped use cases	PHAR-UC-020, PHAR-UC-022, PHAR-UC-023, PHAR-UC-024, PHAR-UC-030
Limitations and confidence	Sector interpretation does not determine legal applicability, establish validation adequacy, or guarantee safety, quality, compliance or security. High for GAISSF source fidelity; Moderate for generic sector interpretation pending organization- and jurisdiction-specific review.

7. Lifecycle, Validation and Change Control

Apply controlled gates from use-case intake through retirement. Define intended use, GxP and regulated-record impact, criticality, data/model provenance, threat model, test and acceptance criteria, approval, deployment, access, monitoring, drift, change control, periodic review, incident/deviation/CAPA and supplier exit. For probabilistic or externally updated systems, establish repeated-test methods, version pinning or change detection, traceable prompts/retrieval sources and reconstructable review evidence.

8. Incident, Deviation, CAPA and Escalation

Use coordinated triage across cybersecurity, AI failure, data integrity, quality, clinical, pharmacovigilance, privacy, supplier and continuity pathways. Preserve evidence, assess patient/product/batch/record impact, contain or suspend where needed, reconcile affected records, and obtain qualified legal/regulatory review before external reporting decisions.

9. Evidence and Assessment

Maintain attributable, time-bounded and scope-specific evidence including inventory, intended-use and GxP determinations, architecture, model/data records, supplier reviews, risk/threat assessments, validation/assurance, access/audit logs, changes, monitoring, human reviews, incidents, deviations, CAPAs and periodic reviews.

10. Maturity Model

Level	Description
1 — Initial	Ad hoc and reactive.
2 — Repeatable	Documented minimum process.
3 — Defined	Integrated quality, security, validation and supplier governance.
4 — Managed	Measured effectiveness and residual risk.
5 — Adaptive	Controlled continuous assurance and improvement.

11. Implementation Roadmap

Period	Priority actions	Completion evidence
First 30 days	Inventory, restrict unapproved regulated use, identify Tier 3/4, assign owners and escalation.	Approved inventory and ownership/risk record.
Days 31–90	GxP/criticality determinations, supplier reviews, review rules, change and incident/deviation linkage, priority testing.	Signed determinations, procedures and test evidence.
Months 4–6	Expand validation, monitoring, traceability, resilience and training.	Assurance records, dashboards and closed high-risk findings.
Months 7–12	Institutionalize periodic review, metrics, continuous assurance and cross-site consistency.	Management review and repeat assessment.

12. Notably Absent

- **No reliable public evidence was identified that autonomous AI compromise of pharmaceutical manufacturing is widespread.** Treat as a plausible high-impact scenario, not a prevalence claim. Confidence: Moderate; public reporting is incomplete.
- **No claim is made that malicious manipulation of a pharmaceutical AI system has directly caused confirmed patient harm at scale.** Do not infer occurrence from threat plausibility. Confidence: Moderate; confidential incidents may not be public.
- **No evidence supports routine regulator acceptance of fully autonomous regulated decisions without accountable human and organizational controls.** Default to explicit decision rights, qualified oversight and traceability. Confidence: High as a guide boundary; jurisdiction-specific review remains required.
- **No universal global regulatory classification or validation method for pharmaceutical AI is assumed.** Determine requirements by jurisdiction, intended use and lifecycle stage. Confidence: High.
- **Public incident datasets do not provide complete coverage of AI failures in pharmaceutical operations.** Frequency estimates are not supplied. Confidence: High.
- **Conventional cybersecurity controls alone are not shown to be sufficient for GxP-relevant AI systems.** Integrate quality, validation, data integrity, human oversight and regulated escalation. Confidence: High as an implementation principle.
- **Model accuracy alone is not treated as evidence of clinical, safety, quality or regulatory fitness.** Assess intended use, data, robustness, security, human factors, traceability and lifecycle control. Confidence: High.

- **The guide does not establish that every listed threat has occurred.** Threat entries are explicitly classified as scenarios unless confirmed evidence is cited. Confidence: High.

13. External Reference Register

ID	Issuer / title	Status	Scope limitation	Official URL
SRC-001	US Food and Drug Administration — Guiding Principles of Good AI Practice in Drug Development	2026; Regulatory principles / non-binding context	Does not itself establish universal validation or compliance requirements.	https://www.fda.gov/about-fda/artificial-intelligence-drug-development/guiding-principles-good-ai-practice-drug-development
SRC-002	European Medicines Agency — Reflection paper on the use of AI in the medicinal product lifecycle	2024; Scientific reflection paper	Applicability depends on lifecycle stage, regulatory use and current agency position.	https://www.ema.europa.eu/en/use-artificial-intelligence-ai-medicinal-product-lifecycle
SRC-003	US Food and Drug Administration — E6(R3) Good Clinical Practice (GCP)	2025; FDA guidance adopting ICH E6(R3)	Clinical-trial scope; regional implementation and annex status must be verified.	https://www.fda.gov/regulatory-information/search-fda-guidance-documents/e6r3-good-clinical-practice-gcp
SRC-004	European Commission — EudraLex Volume 4, Annex 11 - Computerised Systems	2011; EU GMP guidance	Current revision, national interpretation and product/manufacturing applicability must be verified.	https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en
SRC-005	US Food and Drug Administration — 21 CFR Part 11 - Electronic Records; Electronic Signatures	Current codification to be verified; Regulation	Applicability depends on predicate rules and record use.	https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11
SRC-006	NIST — Artificial Intelligence Risk Management Framework (AI RMF 1.0)	2023; Voluntary framework	Not pharmaceutical regulation and not a compliance certification.	https://www.nist.gov/itl/ai-risk-management-framework
SRC-007	NIST — Cybersecurity Framework 2.0	2024; Voluntary framework	Requires tailoring; does not replace GxP or product-specific requirements.	https://www.nist.gov/cyberframework
SRC-008	ICH — ICH Q9 Quality Risk Management	Current adopted revision to be verified; Harmonised guideline	Regional implementation and current revision must be confirmed.	https://www.ich.org/page/quality-guidelines

14. Publication Gates

Public release requires qualified pharmaceutical quality/GxP, pharmacovigilance, clinical, manufacturing/laboratory, privacy/legal, jurisdictional regulatory and publication review; named approvals; final licence/trademark wording; and cross-artifact QA.

15. Publication-Readiness Decision

PUBLICATION READY WITH OPEN SPECIALIST REVIEW GATES — CONTROLLED PRE-RELEASE ONLY.

Verified Feedback Update Addendum - Version 1.1

This addendum records verified improvements incorporated across the SEC-049 package. It supplements the existing control-by-control guide without altering the authoritative GAISSF control identifiers, titles or source statements.

Machine-readable schema parity

The SEC-049 JSON schema now excludes inherited generic VTS, ROI, insurance and unsupported commercial-impact fields. Authoritative requirements remain identified as GAISSF controlled Tier 1 sources. The validation report now includes semantic-parity checks.

D8-CTL-04 applicability boundary

The authoritative DORA control remains unchanged. A pharmaceutical organisation is not subject to DORA merely because it uses AI. Direct applicability requires a documented financial-sector, covered ICT-provider, affiliate, contractual or other legal nexus. Where no nexus exists, record a justified Not Applicable decision and separately map applicable pharmaceutical quality, safety, privacy and incident-reporting pathways.

D9-CTL-07 retention boundary

ICAO and DORA periods in the authoritative source are source-specific examples, not universal pharmaceutical retention rules. For pharmaceutical systems, record the applicable GxP predicate rule, clinical, pharmacovigilance, product, privacy, litigation-hold or local legal basis, together with owner, approval, integrity controls and reassessment trigger.

Physical and OT scope

The workbook now records physical/OT interaction, affected equipment or process, actuator authority, safety-function dependency, override or emergency-stop dependency, site or area and the rationale for D9 applicability.

Criticality safeguard

Numeric scoring is an indicative screening aid only. Blank or undetermined factors must not default to Tier 1. GxP significance, direct regulated-record impact, material patient or product risk, and high-consequence autonomous action may require qualitative escalation regardless of score. The approved tier requires named approval and rationale.

Exceptions and justified exclusions

Record the system and control, factual rationale, risk assessment, compensating safeguards, residual risk, Quality and Information Security approvals, legal or regulatory review where relevant, expiry date and reassessment trigger.

Legacy and embedded AI

Document validated-state constraints, unavailable model internals, unsupported suppliers, logging and provenance limitations, compensating controls and a time-bound remediation or retirement plan. Periodic risk acceptance is required.

Threat model maintenance

Refresh the threat model after a new use case, model or provider change, new tool authority, material architecture change, physical/OT connection, confirmed vulnerability or incident, regulatory change, drift or control failure, or new supplier dependency.

Workbook usability

The workbook now includes a Quick Start workflow, physical/OT fields, blank-by-default criticality inputs, an Exceptions Register, flat Control-Threat and Control-Use Case mapping sheets, and a Tier 3/4 Action Plan.

Additional verified references

ID	Instrument	Status	Applicability limitation
SRC-009	Regulation (EU) 2022/2554 (DORA)	Binding EU regulation	Financial-sector scope; not generally applicable to pharmaceutical entities without a documented nexus.
SRC-010	Regulation (EU) 2024/1689 (Artificial Intelligence Act)	Binding EU regulation with phased application	Depends on role, system classification, use, territory and applicable transition dates.
SRC-011	ISO/IEC 42001:2023	International management-system standard	Conformity or certification is separate from GAISSF and does not establish pharmaceutical regulatory compliance.
SRC-012	NIST SP 800-218A (2024)	Final NIST Special Publication	Voluntary unless adopted; not pharmaceutical regulation and no universal attestation or retention rule is inferred.

Glossary additions

Criticality tier: Informative SEC-049 implementation classification; not a regulator-approved category or GAISSF conformance tier.

Physical/OT interaction: Direct or indirect AI influence over equipment, actuators, industrial controls, laboratory automation, cold-chain systems or other physical processes.

Legacy system: Existing system whose architecture, validation state, supplier support or technical constraints materially limit implementation of current controls.

Validated state: Controlled condition in which a system remains fit for its approved intended use under documented configuration and change controls.

QMS: Quality management system governing applicable procedures, records, deviations, change and CAPA.

Publication status

NOT PUBLICATION READY - CONTROLLED PRE-RELEASE ONLY. Structural and feedback-remediation validation has passed, but qualified pharmaceutical quality/GxP, pharmacovigilance, clinical, manufacturing/laboratory, privacy, legal and jurisdiction-specific review gates remain open.