

ODA3 INSTITUTE

CROSSWALK

GAISSF™-ISO/IEC 23894 Mapping

Source-Bounded AI Risk Management Alignment Crosswalk

GAISSF-CRO-021 | Informative crosswalk | Draft for Publication

Version 1.2 | Updated 5 October 2026

© 2026 ODA3 Pvt Ltd

Executive Summary

GAISSF-CRO-021 maps the 59-control GAISSF™ v1.0 catalogue to the publicly verifiable structure of ISO/IEC 23894:2023. The Applicable-Control Baseline is all 52 controls in D1-D8 plus D9 where Physical AI or cyber-physical actuation is in scope. The crosswalk supports risk-register integration, evidence-reuse analysis and treatment traceability while preserving the distinction between risk-management process evidence and control-effectiveness evidence.

This edition is source-bounded. The clause structure is confirmed from official and authorized sources; detailed semantic alignments are ODA3 analytical inferences pending access to the complete licensed standard. The mapping therefore does not claim full-text verification, conformity, certification or equivalence.

Measure	Result
GAISSF controls mapped	59
Strong partial	13
Partial	5
Supporting	41
Medium-High confidence	13
Medium confidence	46

1. Purpose and Intended Use

This report provides a controlled crosswalk for aligning GAISSF control implementation with AI risk-management activities, reusing qualified risk evidence, identifying residual technical validation and planning future full-text re-verification.

2. Source Boundary and Authority

The external source baseline is ISO/IEC 23894:2023. The exact external sources used are the ISO official standard record and abstract, together with the ANSI-authorized preview. The complete licensed text was not available. GAISSF-NOR-001 and GAISSF-NOR-004 are the controlling GAISSF sources. Held/internal schema or validation tooling is not a publication dependency of this crosswalk.

3. Source and Claim Classification

This report distinguishes four source/claim classes without redefining ODA3's controlling T1-T4 evidence-sourcing taxonomy: authoritative GAISSF sources; verified external public sources; ODA3 analytical mapping; and implementation recommendations.

Class	Meaning
Authoritative GAISSF source	Current GAISSF normative publication set; does not include held/internal validation tooling.
Verified external public source	ISO official metadata/abstract and authorized preview used only for publicly verifiable structure.
ODA3 analytical mapping	Source-bounded semantic interpretation; not full-text verification.
Implementation recommendation	Non-normative implementation or revalidation guidance.

4. Mapping Methodology

[Authoritative GAISSF source] GAISSF control identifiers, titles and normative framework statements are derived from the current GAISSF v1.0 normative publication set.

[Verified external source] The ISO/IEC 23894 document identity, clause hierarchy and annex headings were confirmed using the ISO official record and the ANSI-authorized five-page preview.

[ODA3 analysis] Each semantic mapping compares risk objective, scope, affected lifecycle stage, evidence, treatment and review purpose. Keyword similarity alone is not treated as alignment.

[ODA3 analysis] Relationship ratings are Strong partial, Partial, Supporting or Contextual. No rating means equivalence, conformity, certification or automatic evidence acceptance.

[Implementation recommendation] Every record includes a re-validation trigger and an ODA3-derived risk extension to operationalize GAISSF evidence needs without presenting those fields as ISO requirements.

5. Why the ODA3-Derived Risk Extension Is Necessary

[Verified external source] ISO/IEC 23894 provides risk-management guidance and a process structure for identifying, analysing, evaluating, treating, monitoring and recording AI risk.

[ODA3 analysis] GAISSF additionally requires control-specific, testable and auditable technical outcomes. The ODA3-derived extension therefore specifies the data fields needed to connect a risk-treatment decision to a GAISSF control, its VTS, its acceptance criteria and its signed evidence.

[Implementation recommendation] In practical terms: the ISO-aligned process establishes that a treatment plan should exist; the ODA3 extension records the system boundary, scenario, stakeholder, owner, treatment, measurable acceptance criterion, validation evidence, residual risk and review trigger needed for GAISSF assurance.

6. Evidence Reuse and Validation Rules

[Authoritative GAISSF source] Reusable GAISSF evidence must remain relevant, authentic, traceable, complete, current and linked to the assessed scope. Assessment evidence must demonstrate implementation and operating effectiveness, not policy intent alone.

[ODA3 analysis] ISO-aligned risk registers, treatment plans, approvals, consultation records, monitoring results and review records can be reused only after scope, authenticity, currency, completeness and effectiveness qualification.

[Authoritative GAISSF source] Held/internal GAISSF VTS paths are not part of this public crosswalk. Where a validation asset is published, current and applicable, it may be used as one method. Demo or mock HIL output is not independent assurance evidence.

[Implementation recommendation] For D6-CTL-04, organizations may add a supplementary automated incident-response validation profile for detection, containment, rollback, evidence capture and escalation. This is a recommended extension, not a new GAISSF control.

7. Relationship and Confidence Interpretation

[ODA3 analysis] Governance and regulatory controls generally receive Strong partial / Medium-High ratings because ISO/IEC 23894 structurally addresses governance, ownership, assessment, treatment, monitoring and reporting, while GAISSF adds precise technical mechanisms and test evidence.

[ODA3 analysis] Runtime, adversarial, agentic and physical-AI controls generally receive Supporting / Medium ratings because risk-management guidance can justify and monitor treatment but does not define attack corpora, technical thresholds, memory isolation, actuator interlocks or HIL pass criteria.

[ODA3 analysis] Shadow AI receives stronger alignment where discovery, ownership, context, treatment and monitoring form the primary control outcome, but GAISSF still requires explicit discovery coverage and evidence.

8. Coverage Summary and Lifecycle View

[ODA3 analysis] The complete 59-control register is placed in Annex B to preserve the narrative flow of the Technical Report. Annex C provides the reverse ISO-process index.

Domain	Domain title	Controls	Relationship profile	Primary lifecycle stages
D1	Model Integrity & Adversarial Robustness	9	Strong partial 0; Partial 0; Supporting 9	Data collection, processing and labelling; modelling and training; verification and validation; operation and monitoring.
D2	Runtime Security & Adversarial Defense	6	Strong partial 0; Partial 0; Supporting 6	Verification and validation; deployment; operation and monitoring; incident response and change management.
D3	Agentic Risk & Autonomous System Security	7	Strong partial 0; Partial 0; Supporting 7	System design; integration; deployment; operation and monitoring; change, transfer and decommissioning.
D4	Supply Chain & Third-Party AI Security	7	Strong partial 1; Partial 0; Supporting 6	Acquisition and sourcing; system integration; deployment; supplier monitoring; change and retirement.
D5	Content Safety & Output Integrity	6	Strong partial 0; Partial 0; Supporting 6	Data preparation; design and development; verification and validation; deployment; operation and user interaction.
D6	Governance, Accountability & Human Oversight	7	Strong partial 7; Partial 0; Supporting 0	All lifecycle stages, with emphasis on governance, approval gates, monitoring, incident response and retirement.

Domain	Domain title	Controls	Relationship profile	Primary lifecycle stages
D7	Human & Societal Harms	5	Strong partial 0; Partial 5; Supporting 0	Design and impact assessment; verification and validation; deployment; operation; stakeholder communication and incident response.
D8	Regulatory Alignment & Compliance	5	Strong partial 5; Partial 0; Supporting 0	All lifecycle stages through legal, regulatory and assurance checkpoints, with periodic re-evaluation.
D9	Physical AI Safety	7	Strong partial 0; Partial 0; Supporting 7	System design; physical integration; HIL validation; deployment; operation and monitoring; emergency response and decommissioning.

9. Operational Use Model

- Use the risk register to identify the AI asset, scenario, affected stakeholders, uncertainty, likelihood, consequence and owner.
- Link each selected treatment to the relevant GAISSF control and validation record.
- Qualify existing evidence before reuse and record any scope or freshness limitation.
- Execute the an independently controlled validation method where process evidence does not demonstrate the technical outcome.
- Record residual risk, acceptance authority, expiry and review trigger.
- Revalidate at least annually and whenever the control-specific trigger in Annex B occurs.

10. Regulatory and Standards Evolution

Regulatory and standards references evolve. D8 evidence and mappings shall be reviewed at least annually and whenever authoritative legislation, regulatory guidance, enforcement practice, ISO publications or GAISSF controlled sources change. A revision that materially affects scope, interpretation, evidence or technical validation shall trigger controlled downstream impact analysis.

11. Notably Absent from ISO/IEC 23894 Risk Guidance

The following capabilities are not demonstrated merely by following a risk-management process and remain subject to GAISSF-specific implementation and validation evidence:

- Runtime adversarial-defense thresholds for prompt injection, jailbreaks, multimodal attacks, tool-call abuse and cross-context hijacking.
- Model-integrity pass criteria for poisoning, extraction, drift, federated learning, embeddings, adapters, merges, quantization and cryptographic hardening.
- Agentic enforcement mechanisms for least agency, inter-agent trust, chained prompts, memory isolation, exfiltration prevention and secure memory lifecycle.
- Control-specific supply-chain test procedures for AI BOMs, model scanning, registry vetting, MCP behavior, external APIs, shadow AI and dependency analysis.
- Content-safety and privacy evaluation thresholds for harmful content, PII leakage, copyright, watermarking and privacy-preserving ML.
- Control-specific operating-effectiveness evidence for human intervention, audit trails, model cards, incident readiness, decommissioning, vendor governance and resilience.
- Physical-AI HIL pass criteria for harm boundaries, safe states, emergency stops, cyber-physical detection, sensor integrity, actuator commands and incident evidence preservation.
- Universal legal compliance, sector approval, fairness, safety or acceptable residual-risk thresholds.

12. Publication, Claims and Change-Control Rules

- Publish GAISSF-CRO-021 only as an informative, source-bounded, version-controlled Draft for Publication until independent crosswalk review and explicit publication approval are complete.
- Do not claim full-text verification until a licensed ISO/IEC 23894:2023 copy has been reviewed.
- Do not describe ISO/IEC 23894 as a certifiable requirements standard or claim that alignment demonstrates certification.
- Do not redistribute protected ISO/IEC text or the preview.
- Publish the Technical Report, Executive Brief, XLSX register, JSON register, version history and checksum manifest as one coordinated package.
- Record every mapping, source, validation-method, schema or claims change in version_history.md.

Annex A - Register Field Definitions

Field	Definition
mts_test_file	Validation-method reference where publicly available and applicable.
mts_package_path	Exact path inside the supplied oda3-gaissf-mts release package.
mts_test_design	High-level validation action.
mts_pass_criteria	Measurable conditions required for the validation result.
mts_evidence_artifacts	Evidence object or artifact produced by successful execution.
relationship_justification	Why the selected relationship rating applies.
revalidation_trigger	Events requiring reassessment of the mapping and evidence.
primary_ai_lifecycle_stage	Primary ISO/IEC 23894 Annex C lifecycle relevance.
source_tier_basis	Evidence tiers supporting the mapping.
context_adaptation_note	Context-specific tailoring note where a validation method cannot be universal.
supplementary_validation_profile	Optional additional assurance activity that does not create a new normative control.

Annex B - 59-Control Mapping Register

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
D1-CTL-01 Dataset Provenance & Poisoning Prevention	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Dataset Provenance & Poisoning Prevention; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; new model version or fine-tuning; training-data or provenance change; material drift or robustness finding
D1-CTL-02 Model Extraction Resistance	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Model Extraction Resistance; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; new model version or fine-tuning; training-data or provenance change; material

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
					drift or robustness finding
D1-CTL-03 Behavioral Drift Detection	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C; 5.6; 5.7.1; 5.7.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Behavioral Drift Detection; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; new model version or fine-tuning; training-data or provenance change; material drift or robustness finding
D1-CTL-04 Federated Learning Poisoning Prevention	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Federated Learning Poisoning Prevention; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; new model version or fine-tuning; training-data or provenance change; material drift or robustness finding

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
D1-CTL-05 Embedding Space Robustness	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Embedding Space Robustness; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; new model version or fine-tuning; training-data or provenance change; material drift or robustness finding
D1-CTL-06 Post-Quantum Model Signing & Crypto Hardening	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Post-Quantum Model Signing & Crypto Hardening; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; new model version or fine-tuning; training-data or provenance change; material drift or robustness finding
D1-CTL-07 LoRA/Adapter Integrity Verification	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review LoRA/Adapter Integrity Verification; the technical	Use an independently controlled validation method	Scope-linked implementation and test records with	ODA3-derived risk extension: record the AI asset/system

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
		design, test procedure and pass criteria remain GAISSE-specific.	appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; new model version or fine-tuning; training-data or provenance change; material drift or robustness finding
D1-CTL-08 Model Merge Attack Detection	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Model Merge Attack Detection; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; new model version or fine-tuning; training-data or provenance change; material drift or robustness finding
D1-CTL-09 Quantization Backdoor Screening	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Quantization Backdoor Screening; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary,	Scope-linked implementation and test records with provenance, configuration/version, inputs,	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; new model version or fine-tuning; training-data or provenance change; material drift or robustness finding
D2-CTL-01 Direct Prompt Injection Prevention	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Direct Prompt Injection Prevention; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; runtime architecture, prompt, tool or interface change; new adversarial technique or vulnerability; significant security incident
D2-CTL-02 Indirect Prompt Injection Prevention	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Indirect Prompt Injection Prevention; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; runtime architecture, prompt, tool or interface change; new adversarial technique or vulnerability; significant security incident
D2-CTL-03 Jailbreak Resistance Testing	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Jailbreak Resistance Testing; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; runtime architecture, prompt, tool or interface change; new adversarial technique or vulnerability; significant security incident
D2-CTL-04 Multi-Modal Injection Defense	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Multi-Modal Injection Defense; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; runtime architecture, prompt, tool or interface change; new adversarial technique or vulnerability; significant security incident
D2-CTL-05 Function Call/Tool Call Injection Prevention	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Function Call/Tool Call Injection Prevention; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; runtime architecture, prompt, tool or interface change; new adversarial technique or vulnerability; significant security incident
D2-CTL-06 Cross-Context Hijacking Mitigation	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Cross-Context Hijacking Mitigation; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; runtime architecture, prompt, tool or interface change; new adversarial technique or vulnerability; significant security incident
D3-CTL-01 Least Agency Enforcement	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Least Agency Enforcement; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; agent authority, tools, memory or inter-agent topology change; new autonomous action type; material change to human oversight
D3-CTL-02 Inter-Agent Communication Security	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Inter-Agent Communication Security; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary,	Scope-linked implementation and test records with provenance, configuration/version, inputs,	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; agent authority, tools, memory or inter-agent topology change; new autonomous action type; material change to human oversight
D3-CTL-03 Agentic Prompt Chaining Detection	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Agentic Prompt Chaining Detection; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; agent authority, tools, memory or inter-agent topology change; new autonomous action type; material change to human oversight
D3-CTL-04 Embodied AI Safety Controls	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Embodied AI Safety Controls; the technical	Use an independently controlled validation method	Scope-linked implementation and test records with	ODA3-derived risk extension: record the AI asset/system

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
		design, test procedure and pass criteria remain GAISSE-specific.	appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; agent authority, tools, memory or inter-agent topology change; new autonomous action type; material change to human oversight
D3-CTL-05 Multi-Agent Trust Chain Attestation	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Multi-Agent Trust Chain Attestation; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; agent authority, tools, memory or inter-agent topology change; new autonomous action type; material change to human oversight

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
D3-CTL-06 Persistent Memory Exfiltration Prevention	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Persistent Memory Exfiltration Prevention; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; agent authority, tools, memory or inter-agent topology change; new autonomous action type; material change to human oversight
D3-CTL-07 Secure Memory Lifecycle Management	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Secure Memory Lifecycle Management; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; agent authority, tools, memory or inter-agent topology change; new autonomous action type; material change to human oversight

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
					oversight
D4-CTL-01 AI Bill Of Materials (AI BOM) Maintenance	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review AI Bill Of Materials (AI BOM) Maintenance; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; supplier, model, API, MCP server or dependency change; new supply-chain threat intelligence; contract or assurance change
D4-CTL-02 Model File & Artifact Scanning	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Model File & Artifact Scanning; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; supplier, model, API, MCP server or dependency change; new

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
					supply-chain threat intelligence; contract or assurance change
D4-CTL-03 Model Hub & Registry Vetting	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C; 5.4.5; 6.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Model Hub & Registry Vetting; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; supplier, model, API, MCP server or dependency change; new supply-chain threat intelligence; contract or assurance change
D4-CTL-04 MCP Server Behavioral Monitoring	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C; 5.6; 5.7.1; 5.7.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review MCP Server Behavioral Monitoring; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; supplier, model,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
					API, MCP server or dependency change; new supply-chain threat intelligence; contract or assurance change
D4-CTL-05 Third-Party AI API Security Assessment	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C; 5.4.5; 6.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Third-Party AI API Security Assessment; the technical design, test procedure and pass criteria remain GAISSF-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; supplier, model, API, MCP server or dependency change; new supply-chain threat intelligence; contract or assurance change
D4-CTL-06 Shadow AI Discovery & Governance	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for Shadow AI Discovery & Governance, but it does not prescribe the GAISSF-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
					applicable validation-method revision; supplier, model, API, MCP server or dependency change; new supply-chain threat intelligence; contract or assurance change
D4-CTL-07 AI Software Composition Analysis (SCA)	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review AI Software Composition Analysis (SCA); the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; supplier, model, API, MCP server or dependency change; new supply-chain threat intelligence; contract or assurance change
D5-CTL-01 Harmful Content Blocking	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C; 5.4.5; 6.2; Annex A	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Harmful Content Blocking; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
				periods.	review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; content policy, data category, privacy requirement or output modality change; new harm taxonomy or evaluation method
D5-CTL-02 PII Leakage Prevention	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review PII Leakage Prevention; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; content policy, data category, privacy requirement or output modality change; new harm taxonomy or evaluation method
D5-CTL-03 Copyright Detection	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C; 5.4.5; 6.2; Annex A	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Copyright Detection; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
				periods.	review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; content policy, data category, privacy requirement or output modality change; new harm taxonomy or evaluation method
D5-CTL-04 AI Watermarking Robustness	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C; 5.4.5; 6.2; Annex A	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review AI Watermarking Robustness; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; content policy, data category, privacy requirement or output modality change; new harm taxonomy or evaluation method
D5-CTL-05 Privacy-By-Design Verification	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C; 5.4.5; 6.2; Annex A	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Privacy-By-Design Verification; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
				periods.	review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; content policy, data category, privacy requirement or output modality change; new harm taxonomy or evaluation method
D5-CTL-06 Privacy-Preserving ML Validation	4; 5.3; 5.4.1; 5.5; 6.3.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5.2; 6.5.3; 6.6; 6.7; Annex B; Annex C; 5.4.5; 6.2; Annex A	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Privacy-Preserving ML Validation; the technical design, test procedure and pass criteria remain GAISSE-specific.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; content policy, data category, privacy requirement or output modality change; new harm taxonomy or evaluation method
D6-CTL-01 Human-In-The-Loop For High-Risk Actions	4; 5.1; 5.2; 5.3; 5.4.1; 5.4.2; 5.4.3; 5.4.4; 5.4.5; 5.5; 5.6; 5.7; 6.2; 6.3; 6.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C; 6.3.3	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for Human-In-The-Loop For High-Risk Actions, but it does not prescribe the GAISSE-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
				periods.	review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; governance, owner, policy or approval-process change; major incident or exercise finding; business continuity or decommissioning change Context note: The supplied human-in-the-loop validation is a reference pattern. The blocked action, intervention point, escalation path, response time and acceptance criteria shall be adapted to the specific high-risk context, such as clinical decision support, financial authorization or autonomous-vehicle intervention.
D6-CTL-02 Audit Trail Completeness	4; 5.1; 5.2; 5.3; 5.4.1; 5.4.2; 5.4.3; 5.4.4; 5.4.5; 5.5; 5.6; 5.7; 6.2; 6.3; 6.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C; 5.7.1; 5.7.2	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for Audit Trail Completeness, but it does not prescribe the GAISSE-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; governance, owner, policy or approval-process change; major incident or exercise finding; business continuity or decommissioning change

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
D6-CTL-03 AI Model Card Completeness	4; 5.1; 5.2; 5.3; 5.4.1; 5.4.2; 5.4.3; 5.4.4; 5.4.5; 5.5; 5.6; 5.7; 6.2; 6.3; 6.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for AI Model Card Completeness, but it does not prescribe the GAISSE-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; governance, owner, policy or approval-process change; major incident or exercise finding; business continuity or decommissioning change
D6-CTL-04 AI Incident Response Readiness	4; 5.1; 5.2; 5.3; 5.4.1; 5.4.2; 5.4.3; 5.4.4; 5.4.5; 5.5; 5.6; 5.7; 6.2; 6.3; 6.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C; 5.7.1; 5.7.2	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for AI Incident Response Readiness, but it does not prescribe the GAISSE-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; governance, owner, policy or approval-process change; major incident or exercise finding; business continuity or

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
					decommissioning change Supplementary: Recommended supplementary automated validation profile (not a new GAISSE control): exercise automated detection, containment, rollback, evidence capture and escalation actions against approved AI incident-response playbooks, with human authorization retained where required.
D6-CTL-05 Model Deprecation & Decommissioning	4; 5.1; 5.2; 5.3; 5.4.1; 5.4.2; 5.4.3; 5.4.4; 5.4.5; 5.5; 5.6; 5.7; 6.2; 6.3; 6.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C; 5.7.1; 5.7.2	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for Model Deprecation & Decommissioning, but it does not prescribe the GAISSE-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; governance, owner, policy or approval-process change; major incident or exercise finding; business continuity or decommissioning change
D6-CTL-06 Third-Party AI Vendor Governance	4; 5.1; 5.2; 5.3; 5.4.1; 5.4.2; 5.4.3; 5.4.4; 5.4.5; 5.5; 5.6; 5.7; 6.2; 6.3; 6.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C; 6.3.3; 6.4.2; 6.5.3	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for Third-Party AI Vendor Governance, but it does not prescribe the GAISSE-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; governance, owner, policy or approval-process change; major incident or exercise finding; business continuity or decommissioning change
D6-CTL-07 AI Resilience & Business Continuity	4; 5.1; 5.2; 5.3; 5.4.1; 5.4.2; 5.4.3; 5.4.4; 5.4.5; 5.5; 5.6; 5.7; 6.2; 6.3; 6.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C; 5.7.1; 5.7.2	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for AI Resilience & Business Continuity, but it does not prescribe the GAISSE-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; governance, owner, policy or approval-process change; major incident or exercise finding; business continuity or decommissioning change
D7-CTL-H01 AI-Generated Phishing Simulation	4; 5.4.1; 5.4.5; 5.5; 5.6; 6.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C	Partial / Medium ISO/IEC 23894 supports identification, analysis, treatment and monitoring of the risks addressed by AI-Generated Phishing Simulation, but only partially addresses the operational safeguards and evidence granularity required by GAISSE.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; new human/social harm scenario; training or authentication process change; material external threat trend
D7-CTL-H02 Deepfake Detection Training	4; 5.4.1; 5.4.5; 5.5; 5.6; 6.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C	Partial / Medium ISO/IEC 23894 supports identification, analysis, treatment and monitoring of the risks addressed by Deepfake Detection Training, but only partially addresses the operational safeguards and evidence granularity required by GAISSF.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; new human/social harm scenario; training or authentication process change; material external threat trend
D7-CTL-H03 Out-Of-Band Authentication	4; 5.4.1; 5.4.5; 5.5; 5.6; 6.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C	Partial / Medium ISO/IEC 23894 supports identification, analysis, treatment and monitoring of the risks addressed by Out-Of-Band Authentication, but only partially addresses the operational safeguards and evidence granularity required by GAISSF.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; new human/social harm scenario; training or authentication process change; material external threat trend
D7-CTL-H04 AI Social Engineering IR	4; 5.4.1; 5.4.5; 5.5; 5.6; 6.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C	Partial / Medium ISO/IEC 23894 supports identification, analysis, treatment and monitoring of the risks addressed by AI Social Engineering IR, but only partially addresses the operational safeguards and evidence granularity required by GAISSF.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; new human/social harm scenario; training or authentication process change; material external threat trend
D7-CTL-H05 AI-Enhanced External Attack Defense	4; 5.4.1; 5.4.5; 5.5; 5.6; 6.2; 6.3.3; 6.3.4; 6.4.2; 6.4.3; 6.4.4; 6.5; 6.6; 6.7; Annex A; Annex B; Annex C	Partial / Medium ISO/IEC 23894 supports identification, analysis, treatment and monitoring of the risks addressed by AI-Enhanced External Attack Defense, but only partially addresses the operational safeguards and evidence granularity required by GAISSF.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; new human/social harm scenario; training or authentication process change; material external threat trend
D8-CTL-01 EU AI Act Risk Tier Mapping	4; 5.1-5.7; 6.1-6.7; Annex A; Annex B; Annex C	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for EU AI Act Risk Tier Mapping, but it does not prescribe the GAISSF-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; change in law, regulation or authoritative guidance; new jurisdiction or sector; regulatory enforcement development
D8-CTL-02 ISO 42001 Gap Analysis	4; 5.1-5.7; 6.1-6.7; Annex A; Annex B; Annex C	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for ISO 42001 Gap Analysis, but it does not prescribe the GAISSF-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; change in law, regulation or authoritative guidance; new jurisdiction or sector; regulatory enforcement development
D8-CTL-03 GPAI Technical Documentation Verification	4; 5.1-5.7; 6.1-6.7; Annex A; Annex B; Annex C	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for GPAI Technical Documentation Verification, but it does not prescribe the GAISSF-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSF control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSF or applicable validation-method revision; change in law, regulation or authoritative guidance; new jurisdiction or sector; regulatory enforcement development
D8-CTL-04 DORA Ict Incident Reporting (Financial Sector)	4; 5.1-5.7; 6.1-6.7; Annex A; Annex B; Annex C; 5.6; 5.7.1; 5.7.2; 6.6; 6.7	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for DORA Ict Incident Reporting (Financial Sector), but it does not prescribe the GAISSF-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; change in law, regulation or authoritative guidance; new jurisdiction or sector; regulatory enforcement development
D8-CTL-05 Nist Sp 800-218A Compliance Check	4; 5.1-5.7; 6.1-6.7; Annex A; Annex B; Annex C	Strong partial / Medium-High ISO/IEC 23894 strongly aligns with the governance, ownership, assessment, treatment, monitoring and reporting processes needed for Nist Sp 800-218A Compliance Check, but it does not prescribe the GAISSE-specific technical mechanism, measurable threshold or validation evidence needed to demonstrate the control outcome.	Use an independently controlled validation method appropriate to the control, system boundary, threat/harm scenario and assurance objective. Define acceptance criteria, sample size, test conditions and limitations for the specific implementation. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; change in law, regulation or authoritative guidance; new jurisdiction or sector; regulatory enforcement development
D9-CTL-01 Physical Harm Boundary Enforcement	4; 5.3; 5.4.1; 5.4.4; 5.5; 6.3; 6.4; 6.5; 6.6; 6.7; Annex B; Annex C; 6.3.2; 6.3.3; 6.4.2; 6.4.3; 6.5.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Physical Harm Boundary Enforcement; the technical design, test procedure and pass criteria remain GAISSE-specific.	D9 is additional/conditional. Where Physical AI or cyber-physical actuation is in scope, use system- and hazard-appropriate	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders,

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			simulation/HIL/physical testing and safe-state/override evidence as applicable. Do not infer universal SIL/DAL levels or certification from this crosswalk.	identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; hardware, firmware, actuator, sensor or deployment-environment change; HIL/simulator change; physical safety incident or near miss
D9-CTL-02 Safe State And Graceful Degradation	4; 5.3; 5.4.1; 5.4.4; 5.5; 6.3; 6.4; 6.5; 6.6; 6.7; Annex B; Annex C; 6.3.2; 6.3.3; 6.4.2; 6.4.3; 6.5.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Safe State And Graceful Degradation; the technical design, test procedure and pass criteria remain GAISSE-specific.	D9 is additional/conditional. Where Physical AI or cyber-physical actuation is in scope, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. Do not infer universal SIL/DAL levels or certification from this crosswalk.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; hardware, firmware, actuator, sensor or deployment-environment change; HIL/simulator change; physical safety incident or near miss
D9-CTL-03 Human Override And Emergency Stop	4; 5.3; 5.4.1; 5.4.4; 5.5; 6.3; 6.4; 6.5; 6.6; 6.7; Annex B; Annex C; 5.4.5; 6.2; 6.3.3; Annex A; 6.3.2; 6.4.2; 6.4.3; 6.5.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Human Override And Emergency Stop; the technical design, test procedure and pass criteria remain GAISSE-specific.	D9 is additional/conditional. Where Physical AI or cyber-physical actuation is in	Scope-linked implementation and test records with provenance,	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
			scope, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. Do not infer universal SIL/DAL levels or certification from this crosswalk.	configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; hardware, firmware, actuator, sensor or deployment-environment change; HIL/simulator change; physical safety incident or near miss
D9-CTL-04 Cyber-Physical Attack Detection	4; 5.3; 5.4.1; 5.4.4; 5.5; 6.3; 6.4; 6.5; 6.6; 6.7; Annex B; Annex C; 6.3.2; 6.3.3; 6.4.2; 6.4.3; 6.5.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Cyber-Physical Attack Detection; the technical design, test procedure and pass criteria remain GAISSE-specific.	D9 is additional/conditional. Where Physical AI or cyber-physical actuation is in scope, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. Do not infer universal SIL/DAL levels or certification from this crosswalk.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; hardware, firmware, actuator, sensor or deployment-environment change; HIL/simulator change; physical safety incident or near miss
D9-CTL-05 Physical Environment Integrity Monitoring	4; 5.3; 5.4.1; 5.4.4; 5.5; 6.3; 6.4; 6.5; 6.6; 6.7; Annex B; Annex C; 5.6; 5.7.1; 5.7.2; 6.3.2; 6.3.3; 6.4.2; 6.4.3; 6.5.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review	D9 is additional/conditional.	Scope-linked implementation	ODA3-derived risk extension:

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
		Physical Environment Integrity Monitoring; the technical design, test procedure and pass criteria remain GAISSE-specific.	Where Physical AI or cyber-physical actuation is in scope, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. Do not infer universal SIL/DAL levels or certification from this crosswalk.	and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; hardware, firmware, actuator, sensor or deployment-environment change; HIL/simulator change; physical safety incident or near miss
D9-CTL-06 Actuator Command Verification	4; 5.3; 5.4.1; 5.4.4; 5.5; 6.3; 6.4; 6.5; 6.6; 6.7; Annex B; Annex C; 6.3.2; 6.3.3; 6.4.2; 6.4.3; 6.5.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Actuator Command Verification; the technical design, test procedure and pass criteria remain GAISSE-specific.	D9 is additional/conditional. Where Physical AI or cyber-physical actuation is in scope, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. Do not infer universal SIL/DAL levels or certification from this crosswalk.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; hardware, firmware, actuator, sensor or deployment-environment change; HIL/simulator change; physical safety incident or near miss

ID / Title	ISO/IEC 23894 anchors	Rating / rationale	Validation method / evidence expectation	Evidence artifacts	Risk extension / re-validation trigger
D9-CTL-07 Physical Incident Evidence Preservation	4; 5.3; 5.4.1; 5.4.4; 5.5; 6.3; 6.4; 6.5; 6.6; 6.7; Annex B; Annex C; 5.6; 5.7.1; 5.7.2; 6.3.2; 6.3.3; 6.4.2; 6.4.3; 6.5.2	Supporting / Medium ISO/IEC 23894 provides the risk-management process used to justify, prioritize and review Physical Incident Evidence Preservation; the technical design, test procedure and pass criteria remain GAISSE-specific.	D9 is additional/conditional. Where Physical AI or cyber-physical actuation is in scope, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. Do not infer universal SIL/DAL levels or certification from this crosswalk.	Scope-linked implementation and test records with provenance, configuration/version, inputs, outputs, exceptions, reviewer identity, date, and limitations. Retention follows the approved records schedule and applicable legal, contractual, mission and evidence-preservation requirements; GAISSE conformance tiers do not define universal retention periods.	ODA3-derived risk extension: record the AI asset/system boundary, threat or harm scenario, affected stakeholders, likelihood/consequence rationale, risk owner, treatment decision, measurable acceptance criteria, validation evidence, residual risk, review trigger and linkage to the GAISSE control/validation method. Trigger: annual scheduled review; revision to ISO/IEC 23894; material GAISSE or applicable validation-method revision; hardware, firmware, actuator, sensor or deployment-environment change; HIL/simulator change; physical safety incident or near miss

Annex C - Reverse ISO/IEC 23894 Process Index

Reference	Topic	Source-bounded explanation	Mapped GAISSF controls
4	Principles of AI risk management	Risk-management principles applied to AI-specific uncertainty, impacts and organizational objectives.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D8-CTL-01, D8-CTL-02, D8-CTL-03, D8-CTL-04, D8-CTL-05, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
5.1	Framework - General	General design and operation of the risk-management framework.	D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07
5.2	Leadership and commitment	Leadership sponsorship and accountability for AI risk management.	D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07
5.3	Integration	Integration of AI risk management into governance, processes and decision-making.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
5.4.1	Understanding the organization and its context	External/internal context, roles, objectives, constraints and stakeholders.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
5.4.2	Articulating risk-management commitment	Policy, commitment and management direction.	D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07
5.4.3	Roles, authorities, responsibilities and accountabilities	Ownership and accountability for risk decisions and activities.	D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07
5.4.4	Allocating resources	People, competence, data, technology, time and funding for risk management.	D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
5.4.5	Communication and consultation	Internal and external communication and stakeholder consultation.	D4-CTL-03, D4-CTL-05, D5-CTL-01, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D9-CTL-03
5.5	Implementation	Operational implementation of the risk-management framework.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03,

Reference	Topic	Source-bounded explanation	Mapped GAISSF controls
			D7-CTL-H04, D7-CTL-H05, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
5.6	Evaluation	Evaluation of framework design, implementation and effectiveness.	D1-CTL-03, D4-CTL-04, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D8-CTL-04, D9-CTL-05, D9-CTL-07
5.7.1	Adapting	Adaptation to changes in context, systems, impacts and risk.	D1-CTL-03, D4-CTL-04, D6-CTL-02, D6-CTL-04, D6-CTL-05, D6-CTL-07, D8-CTL-04, D9-CTL-05, D9-CTL-07
5.7.2	Continually improving	Continual improvement of the risk-management framework.	D1-CTL-03, D4-CTL-04, D6-CTL-02, D6-CTL-04, D6-CTL-05, D6-CTL-07, D8-CTL-04, D9-CTL-05, D9-CTL-07
6.1	Risk-management process - General	Application of a structured and iterative risk-management process.	No direct anchor
6.2	Communication and consultation	Communication and consultation throughout the process.	D4-CTL-03, D4-CTL-05, D5-CTL-01, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D9-CTL-03
6.3.2	Defining the scope	Boundaries, assumptions, decisions, assets and lifecycle scope.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
6.3.3	External and internal context	Context and stakeholder factors relevant to a specific assessment.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-06, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
6.3.4	Defining risk criteria	Likelihood, consequence, acceptability, prioritization and decision criteria.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05
6.4.2	Risk identification	Identification of threats, harms, events, causes, consequences and affected stakeholders.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-06, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
6.4.3	Risk analysis	Analysis of likelihood, consequence, uncertainty, controls and residual risk.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-

Reference	Topic	Source-bounded explanation	Mapped GAISSF controls
			CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
6.4.4	Risk evaluation	Comparison against criteria and prioritization for treatment.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05
6.5.2	Selection of risk-treatment options	Selection and justification of treatments, including avoidance, modification, sharing and acceptance.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
6.5.3	Preparing and implementing treatment plans	Treatment plan, ownership, resources, schedule, acceptance criteria and residual-risk approval.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-06
6.6	Monitoring and review	Monitoring assumptions, controls, indicators, incidents and changes.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D8-CTL-04, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
6.7	Recording and reporting	Risk records, decisions, evidence, reporting and traceability.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D8-CTL-04, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
Annex A	Objectives	Examples of objectives that can be affected by AI risk.	D5-CTL-01, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D8-CTL-01, D8-CTL-02, D8-CTL-03, D8-CTL-04, D8-CTL-05, D9-CTL-03
Annex B	Risk sources	Illustrative AI risk sources for identification and analysis.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05,

Reference	Topic	Source-bounded explanation	Mapped GAISSF controls
			D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D8-CTL-01, D8-CTL-02, D8-CTL-03, D8-CTL-04, D8-CTL-05, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07
Annex C	AI system lifecycle	Application of risk management across AI lifecycle stages.	D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-02, D2-CTL-03, D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-06, D6-CTL-07, D7-CTL-H01, D7-CTL-H02, D7-CTL-H03, D7-CTL-H04, D7-CTL-H05, D8-CTL-01, D8-CTL-02, D8-CTL-03, D8-CTL-04, D8-CTL-05, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06, D9-CTL-07

Annex D - GAISSE Domain to AI Lifecycle Map

Domain	Primary lifecycle stage alignment
D1	Data collection, processing and labelling; modelling and training; verification and validation; operation and monitoring.
D2	Verification and validation; deployment; operation and monitoring; incident response and change management.
D3	System design; integration; deployment; operation and monitoring; change, transfer and decommissioning.
D4	Acquisition and sourcing; system integration; deployment; supplier monitoring; change and retirement.
D5	Data preparation; design and development; verification and validation; deployment; operation and user interaction.
D6	All lifecycle stages, with emphasis on governance, approval gates, monitoring, incident response and retirement.
D7	Design and impact assessment; verification and validation; deployment; operation; stakeholder communication and incident response.
D8	All lifecycle stages through legal, regulatory and assurance checkpoints, with periodic re-evaluation.
D9	System design; physical integration; HIL validation; deployment; operation and monitoring; emergency response and decommissioning.

Annex E - Domain-Level Practitioner Interpretation

D1 - Model Integrity & Adversarial Robustness

ISO/IEC 23894 can structure the identification, analysis, treatment and monitoring of model-integrity risks, but the risk process does not establish poisoning-detection thresholds, extraction resistance, drift tolerances, embedding robustness or cryptographic acceptance criteria. Reuse context, risk-owner, treatment and monitoring records; retain GAISSE validation results as the operating-effectiveness evidence.

D2 - Runtime Security & Adversarial Defense

The ISO risk process helps define misuse scenarios, affected stakeholders, likelihood, consequence, treatment priority and monitoring. It does not prescribe prompt-injection corpora, jailbreak success thresholds, multimodal attack coverage, tool-call restrictions or cross-context isolation. Runtime tests should be repeated after prompt, model, tool, retrieval or interface changes.

D3 - Agentic Risk & Autonomous System Security

Agentic risks require explicit authority boundaries, action inventories, tool permissions, trust relationships, memory controls and human intervention points. ISO-aligned risk records can justify those decisions, while GAISSE validation evidence demonstrates whether least agency, inter-agent security, prompt-chain detection, memory isolation and embodied safeguards operate as intended.

D4 - Supply Chain & Third-Party AI Security

Supplier and dependency risks align well with context, communication, treatment, monitoring and review. However, evidence reuse is valid only where the same supplier, model, API, MCP server, artifact, version and deployment context remain in scope. AI BOM, scanning, registry-vetting, behavioral-monitoring and SCA evidence should be refreshed after supplier or component change.

D5 - Content Safety & Output Integrity

Risk-management records can document harmful-output, privacy, copyright and transparency scenarios and treatment choices. They do not define universal content thresholds, leakage tolerances, watermark robustness or privacy-preserving ML acceptance criteria. Evaluation datasets, policies and legal assumptions should be versioned with each validation result.

D6 - Governance, Accountability & Human Oversight

This domain has the strongest process alignment because ISO/IEC 23894 emphasizes governance, accountability, resources, communication, evaluation and improvement. The remaining gap is operating-effectiveness evidence: intervention timing, audit completeness, model-card sufficiency, incident exercise performance, decommissioning closure, vendor oversight and resilience test results.

D7 - Human & Societal Harms

The ISO risk structure supports stakeholder identification, consultation, harm scenarios, treatment and monitoring. GAISSE adds concrete simulation, training, authentication and response evidence. Organizations should reassess these controls when threat tactics, user populations, communication channels or societal impact assumptions change.

D8 - Regulatory Alignment & Compliance

Risk and governance records can support regulatory mapping and evidence traceability, but legal applicability and authoritative guidance change over time. D8 evidence should be reviewed at least annually and whenever a jurisdiction, sector, intended use, model classification, reporting rule or enforcement position changes.

D9 - Physical AI Safety

Physical-AI controls require system-specific safety envelopes and HIL or certified-simulator evidence. ISO risk guidance can support hazard scenarios, risk criteria, treatment selection and monitoring, but it does not establish stopping distances, emergency-stop latency, sensor-failure response, actuator-command limits or incident-evidence timing. Mock-mode CI output is not physical independent assurance evidence.

Annex F - Re-validation Decision Workflow

A mapping or evidence-reuse decision should be reopened when any of the following events occurs. The record-level trigger in Annex B is controlling where it is more specific.

Trigger class	Examples	Required action
Scheduled	Annual review; planned governance review	Confirm source editions, system scope, owners, evidence freshness, residual risk and validation-method validity.
System change	New model version, fine-tuning, prompt/tool change, new agent authority, hardware or environment change	Reassess context and risk; rerun affected validation; update treatment and residual-risk approval.
Threat change	New vulnerability, adversarial technique, supplier issue, social-engineering pattern or physical threat	Update scenarios and likelihood; validate detection and treatment effectiveness.
Regulatory change	New law, regulator guidance, enforcement action, jurisdiction or sector rule	Revalidate D8 applicability, evidence and public claims.
Source change	Revision to ISO/IEC 23894, GAISSE normative documents, schema or validation method	Perform semantic impact analysis and issue controlled mapping revision.
Incident or failure	Security event, harm, near miss, audit finding, failed exercise or failed validation	Correct the control, reassess residual risk and verify corrective-action effectiveness.

Evidence Reuse Decision Record

- Identify the original evidence owner, source system, collection date and assessed scope.
- Confirm that the current AI system, model, data, environment, supplier and intended use remain materially equivalent.
- Verify authenticity, integrity, completeness, retention and chain of custody.
- Determine whether the evidence demonstrates process completion, implementation or operating effectiveness.
- Record accepted limitations, compensating tests, residual gaps, approval and expiry date.
- Link the decision to the GAISSE control, selected validation/evidence record and re-validation trigger.