

ODA3 INSTITUTE

EXECUTIVE BRIEF

GAISSF™–ISO/IEC 23894 Mapping

Executive Brief — Source-Bounded Risk Alignment and Evidence Reuse

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

Version 1.2 | Updated 5 October 2026

© 2026 ODA3 Pvt Ltd

Methodology Note

This brief summarizes the coordinated CRO-021 Technical Report. ISO/IEC 23894:2023 document identity and structure were confirmed from official metadata and an authorized preview. Detailed mappings are analytical and require revalidation when licensed full text becomes available. ISO/IEC 23894 is guidance, not a certifiable requirements standard.

Executive Decision

Adopt ISO/IEC 23894-aligned risk documentation as the common governance layer, but do not substitute it for GAISSE technical validation. Risk records explain why a treatment was selected; independent validation evidence demonstrates whether the treatment operates effectively.

Decision Boundaries

1. Evidence Reuse and Assurance Boundary

Evidence that can be reused

- AI risk policy, scope, context and risk criteria.
- Risk registers, scenario analysis, treatment plans and residual-risk approvals.
- Roles, consultation records, monitoring results and management reporting.
- Lifecycle and change-review records that remain current and within the same assessment boundary.

Evidence that still requires GAISSE validation

- Runtime adversarial, prompt-injection, jailbreak and tool-abuse testing.
- Model-integrity, provenance, drift, extraction and cryptographic testing.
- Agent authority, memory, inter-agent trust and exfiltration safeguards.
- Content-safety, privacy, supply-chain and regulatory evidence checks.
- Physical-AI HIL or certified-simulator tests and signed evidence.

Acceptance test for reused evidence

Question	Required answer
Same scope?	System, model, data, environment, supplier and intended use are materially equivalent.
Authentic and intact?	Source, owner, date, integrity and chain of custody are verifiable.
Current?	Evidence remains within its review period and no trigger has invalidated it.
Sufficient?	Evidence demonstrates the claimed process or outcome, with limitations recorded.
Effective?	Where operating effectiveness is claimed, independent validation evidence exists.

2. Coverage and Lifecycle Implications

The mapping covers all 59 GAISSE controls. Governance and regulatory controls align most strongly with ISO/IEC 23894 risk processes; technical runtime, agentic and physical controls retain the largest validation gap.

Domain	Primary lifecycle relevance	Executive implication
D1	Data, training, validation, monitoring	Risk records support treatment; independent validation supports model-integrity assurance.
D2	Validation, deployment, operation	Re-test after prompt, tool, model or interface

Domain	Primary lifecycle relevance	Executive implication
		change.
D3	Design, integration, operation, retirement	Authority and memory boundaries require technical evidence.
D4	Acquisition, integration, supplier monitoring	Supplier evidence is version- and context-dependent.
D5	Data, design, validation, user interaction	Evaluation datasets and policy assumptions must be controlled.
D6	All stages	Strong governance alignment; operating effectiveness remains testable.
D7	Impact assessment, deployment, incident response	Stakeholder and threat assumptions require periodic refresh.
D8	All stages	Legal and regulatory evidence requires annual/event-driven review.
D9	Physical integration, HIL validation, operation	Mock CI output is not evidence of physical-system assurance.

Notably absent from risk guidance alone

- Attack corpora and technical thresholds.
- Agent memory isolation and least-agency enforcement.
- Content, privacy and watermark robustness criteria.
- Actuator interlocks, safe-state timing and emergency-stop latency.
- Universal acceptable-risk, fairness, safety or legal-compliance thresholds.

3. Governance and Evidence-Reuse Framing

Evidence-Reuse Discipline

Reuse evidence only where scope, provenance, authenticity, currency, completeness and relevance are demonstrated.

Do not publish generic financial-savings or ROI claims from this crosswalk; any organization-specific efficiency analysis requires its own measured baseline and assumptions.

No universal cost saving, audit reduction, or commercial benefit is asserted.

Governance controls

- Approve reuse only after scope, authenticity, currency, completeness and effectiveness checks.
- Maintain one risk-to-control-to-validation traceability chain.
- Assign owners for treatment, residual-risk approval and revalidation.
- Treat demo or mock HIL output as engineering evidence only.
- Record expiry dates and trigger-based review conditions for reused evidence.

Incident response maturity

D6-CTL-04 retains its normative tabletop/readiness validation. More mature organizations may add an automated playbook profile for detection, containment, rollback, evidence capture and escalation. This is supplementary assurance and does not create a new GAISSF control.

4. Risks, Review Triggers and Recommended Action

Primary limitations

- The mapping is not full-text verified against a licensed ISO/IEC 23894 copy.
- Alignment does not establish assurance, conformity, legal compliance or technical effectiveness.

- ISO risk guidance does not define GAISSF pass criteria or universal acceptable-risk thresholds.
- System, threat, regulatory or source changes can invalidate earlier evidence-reuse decisions.

Mandatory review triggers

Trigger	Examples
Annual	Scheduled source, scope, evidence and residual-risk review.
System change	New model, fine-tuning, tool, agent authority, supplier, hardware or environment.
Threat change	New vulnerability, attack technique, harm scenario or near miss.
Regulatory change	New law, guidance, enforcement position, jurisdiction or sector.
Source change	Revision to ISO/IEC 23894, GAISSF, schema or validation method.
Failure	Incident, audit finding, exercise failure or validation failure.

Recommended operating action

Use CRO-021 as the common risk-alignment and evidence-reuse layer. Require GAISSF independent validation or verification before claiming that a technical control is operating effectively. Revalidate annually, after material changes and when a licensed ISO/IEC 23894 text becomes available.