

ODA3 INSTITUTE

CROSSWALK

GAISSF™-ISO/IEC 27001 Mapping

Information Security Management System Alignment Crosswalk

GAISSF-CRO-020 | Informative crosswalk | Draft for Publication

Version 1.0 | Updated 5 October 2026

© 2026 ODA3 Pvt Ltd

Document ID	ODA3 Institute GAISSF-CRO-020 GAISSF™–ISO/IEC 27001 Mapping GAISSF-CRO-020
Title	GAISSF™–ISO/IEC 27001:2022 Mapping
Version	1.0
Status	Draft for Publication
Classification	Informative crosswalk / public
Publisher	ODA3 Institute
Updated	5 October 2026
External baseline	ISO/IEC 27001:2022, Edition 3; Amendment 1:2024 tracked separately

PUBLICATION BOUNDARY. This informative crosswalk maps GAISSF™ control outcomes to ISO/IEC 27001:2022 clauses and Annex A controls. It does not reproduce the standard, replace an authorized copy, establish equivalence, evidence sufficiency, operating effectiveness, certification, legal compliance, or automatic conformance.

1. Purpose and Scope

GAISSF-CRO-020 supports comparative analysis, control reuse, evidence qualification, implementation planning and gap identification between GAISSF™ v1.0 and ISO/IEC 27001:2022. It covers all 59 GAISSF controls and the ISO/IEC 27001 management-system and Annex A structure used by the source package. The GAISSF Applicable-Control Baseline is all 52 controls in D1-D8 plus D9 where Physical AI or cyber-physical actuation is in scope.

2. Source and Copyright Boundary

The source package states that the complete licensed ISO/IEC 27001:2022(E), Third edition, was used as an internal controlled reference for the original mapping. That licensed standard is not redistributed in this public package. This update independently rechecked only the public ISO status and amendment metadata; it did not re-read the licensed full text because that file was not included in the supplied package.

3. Mapping Method

Each relationship was assessed against objective, scope, trigger, asset/system boundary, lifecycle stage, evidence and operating-effectiveness expectations. Similar terminology alone is insufficient. ISO/IEC 27001 certification or implementation evidence can support evidence-reuse analysis, but does not automatically satisfy a GAISSF control or establish GAISSF conformance.

4. Relationship and Confidence Taxonomy

Rating	Meaning	Permitted interpretation
Direct enablement	The GAISSF control explicitly performs or governs an ISO mapping activity.	Supports execution; does not establish ISO conformity.
Strong partial	Substantial objective, scope and evidence overlap.	Evidence may be reused after qualification; residual remains.
Partial	Related coverage with material differences.	Supporting evidence only.
Supporting	General governance or assurance support.	Do not treat as control satisfaction.
Contextual	External-regime or comparison context.	No equivalence or compliance inference.

5. Evidence-Reuse Decision Rules

1. Confirm that the ISO/IEC 27001 ISMS scope, assets, suppliers and evidence period match the GAISSF assessment boundary.
2. Use the ISO/IEC 27001 Statement of Applicability as an external evidence index for that management system. It is not the GAISSF Applicable-Control Baseline and is not automatic proof that a GAISSF control is implemented or effective.
3. Reject policy-only evidence where the GAISSF control outcome requires technical execution, system behavior, validation or operating-effectiveness evidence.

4. Preserve provenance, approvals, integrity, sampling basis, chain of custody, scope, configuration/version, reviewer identity, date and limitations. Retention follows the approved records schedule and applicable legal, contractual and evidence-preservation requirements; GAISSF conformance tiers do not define universal retention periods.
5. Use an independently controlled validation method where ISO/IEC 27001 evidence does not demonstrate the GAISSF outcome. Where a GAISSF validation asset is published, current and applicable, it may be used as one method; held/internal VTS, benchmark or test-harness material is not a public dependency.
6. Document accepted, partially accepted and rejected reuse decisions with rationale.

6. Notably Absent from the ISO/IEC 27001 Baseline

ISO/IEC 27001 provides a mature information-security management system and broad organizational, people, physical and technological controls. It does not prescribe most AI-specific mechanisms as discrete test outcomes, including prompt-injection resistance, jailbreak testing, agent permission boundaries, model extraction resistance, model backdoor and adapter/merge/quantization integrity testing, AI BOM semantics, model-hub vetting, MCP behavioral monitoring, harmful-content thresholds, watermark robustness, deepfake defenses, AI-specific regulatory mappings, or functional-safety mechanisms for physical AI.

7. Detailed 59-Control Crosswalk

ISO references are identifiers only. Read each mapping together with its relationship, confidence, evidence-reuse rationale, validation expectation and residual gap. D9 is additional/conditional; where Physical AI is in scope, use GAISSE D9 alongside PAI-SF™ v1.0 as applicable. CSX-PAISF-004 is mapping only and does not establish equivalence, evidence sufficiency or automatic conformance.

GAISSE control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D1-CTL-01 Dataset Provenance & Poisoning Prevention	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.12; 5.13; 5.14; 5.15; 5.33; 5.34; 8.10; 8.11; 8.12; 8.15; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information security governance, secure development, vulnerability management and integrity controls, but does not prescribe this AI-model integrity technique, implementation-specific validation, or GAISSE validation asset threshold.
D1-CTL-02 Model Extraction Resistance	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.15; 5.16; 5.17; 5.18; 8.5; 8.18	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information security governance, secure development, vulnerability management and integrity controls, but does not prescribe this AI-model integrity technique, implementation-specific validation, or GAISSE validation asset threshold.

GAISSE control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D1-CTL-03 Behavioral Drift Detection	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.22; 8.15; 8.16; 8.17	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information security governance, secure development, vulnerability management and integrity controls, but does not prescribe this AI-model integrity technique, implementation-specific validation, or GAISSE validation asset threshold.
D1-CTL-04 Federated Learning Poisoning Prevention	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information security governance, secure development, vulnerability management and integrity controls, but does not prescribe this AI-model integrity technique, implementation-specific validation, or GAISSE validation asset threshold.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D1-CTL-05 Embedding Space Robustness	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information security governance, secure development, vulnerability management and integrity controls, but does not prescribe this AI-model integrity technique, implementation-specific validation, or GAISSF validation asset threshold.
D1-CTL-06 Post-Quantum Model Signing & Crypto Hardening	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.33; 8.9; 8.24; 8.25; 8.29; 8.31	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information security governance, secure development, vulnerability management and integrity controls, but does not prescribe this AI-model integrity technique, implementation-specific validation, or GAISSF validation asset threshold.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D1-CTL-07 LoRA/Adapter Integrity Verification	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.33; 8.9; 8.24; 8.25; 8.29; 8.31; 5.9; 5.21; 8.4; 8.8; 8.26; 8.28; 8.30; 8.32	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information security governance, secure development, vulnerability management and integrity controls, but does not prescribe this AI-model integrity technique, implementation-specific validation, or GAISSF validation asset threshold.
D1-CTL-08 Model Merge Attack Detection	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29; 5.9; 5.21; 8.4; 8.9; 8.25; 8.26; 8.28; 8.30; 8.32	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information security governance, secure development, vulnerability management and integrity controls, but does not prescribe this AI-model integrity technique, implementation-specific validation, or GAISSF validation asset threshold.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D1-CTL-09 Quantization Backdoor Screening	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29; 5.9; 5.21; 8.4; 8.9; 8.25; 8.26; 8.28; 8.30; 8.32	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information security governance, secure development, vulnerability management and integrity controls, but does not prescribe this AI-model integrity technique, implementation-specific validation, or GAISSF validation asset threshold.
D2-CTL-01 Direct Prompt Injection Prevention	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports threat, access, secure-development, logging and monitoring controls, but does not prescribe this AI-specific prompt, jailbreak, multimodal or context-hijacking defense or test threshold.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D2-CTL-02 Indirect Prompt Injection Prevention	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports threat, access, secure-development, logging and monitoring controls, but does not prescribe this AI-specific prompt, jailbreak, multimodal or context-hijacking defense or test threshold.
D2-CTL-03 Jailbreak Resistance Testing	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports threat, access, secure-development, logging and monitoring controls, but does not prescribe this AI-specific prompt, jailbreak, multimodal or context-hijacking defense or test threshold.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D2-CTL-04 Multi-Modal Injection Defense	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports threat, access, secure-development, logging and monitoring controls, but does not prescribe this AI-specific prompt, jailbreak, multimodal or context-hijacking defense or test threshold.
D2-CTL-05 Function Call/Tool Call Injection Prevention	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29; 5.15; 5.16; 5.17; 5.18; 8.5; 8.18	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports threat, access, secure-development, logging and monitoring controls, but does not prescribe this AI-specific prompt, jailbreak, multimodal or context-hijacking defense or test threshold.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D2-CTL-06 Cross-Context Hijacking Mitigation	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports threat, access, secure-development, logging and monitoring controls, but does not prescribe this AI-specific prompt, jailbreak, multimodal or context-hijacking defense or test threshold.
D3-CTL-01 Least Agency Enforcement	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.15; 5.16; 5.17; 5.18; 8.5; 8.18	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports identity, access, supplier, secure-development and monitoring controls, but does not define least agency, agent trust chains, autonomous-action boundaries or agent-memory protections as GAISSF test outcomes.

GAISSE control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D3-CTL-02 Inter-Agent Communication Security	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 supports identity, access, supplier, secure-development and monitoring controls, but does not define least agency, agent trust chains, autonomous-action boundaries or agent-memory protections as GAISSE test outcomes.
D3-CTL-03 Agentic Prompt Chaining Detection	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 supports identity, access, supplier, secure-development and monitoring controls, but does not define least agency, agent trust chains, autonomous-action boundaries or agent-memory protections as GAISSE test outcomes.

GAISSE control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D3-CTL-04 Embodied AI Safety Controls	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 7.1; 7.2; 7.3; 7.4; 7.5; 7.8; 7.11; 7.13; 8.16	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 supports identity, access, supplier, secure-development and monitoring controls, but does not define least agency, agent trust chains, autonomous-action boundaries or agent-memory protections as GAISSE test outcomes.
D3-CTL-05 Multi-Agent Trust Chain Attestation	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.33; 8.9; 8.24; 8.25; 8.29; 8.31	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 supports identity, access, supplier, secure-development and monitoring controls, but does not define least agency, agent trust chains, autonomous-action boundaries or agent-memory protections as GAISSE test outcomes.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D3-CTL-06 Persistent Memory Exfiltration Prevention	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.12; 5.13; 5.14; 5.15; 5.33; 5.34; 8.10; 8.11; 8.12; 8.15	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports identity, access, supplier, secure-development and monitoring controls, but does not define least agency, agent trust chains, autonomous-action boundaries or agent-memory protections as GAISSF test outcomes.
D3-CTL-07 Secure Memory Lifecycle Management	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.12; 5.13; 5.14; 5.15; 5.33; 5.34; 8.10; 8.11; 8.12; 8.15; 5.11; 7.14; 8.32	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports identity, access, supplier, secure-development and monitoring controls, but does not define least agency, agent trust chains, autonomous-action boundaries or agent-memory protections as GAISSF test outcomes.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D4-CTL-01 AI Bill Of Materials (AI Bom) Maintenance	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.9; 5.11; 5.23; 8.9	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides substantial asset, supplier, cloud, vulnerability and secure-development coverage, but the named AI-specific inventory, model-scanning, registry, MCP or shadow-AI mechanism remains a GAISSF residual.
D4-CTL-02 Model File & Artifact Scanning	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.9; 5.21; 8.4; 8.8; 8.9; 8.25; 8.26; 8.28; 8.29; 8.30; 8.32	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides substantial asset, supplier, cloud, vulnerability and secure-development coverage, but the named AI-specific inventory, model-scanning, registry, MCP or shadow-AI mechanism remains a GAISSF residual.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D4-CTL-03 Model Hub & Registry Vetting	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.19; 5.20; 5.21; 5.22; 5.23; 8.20; 8.21; 8.22	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides substantial asset, supplier, cloud, vulnerability and secure-development coverage, but the named AI-specific inventory, model-scanning, registry, MCP or shadow-AI mechanism remains a GAISSF residual.
D4-CTL-04 MCP Server Behavioral Monitoring	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.22; 8.15; 8.16; 8.17; 5.19; 5.20; 5.21; 5.23; 8.20; 8.21; 8.22	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides substantial asset, supplier, cloud, vulnerability and secure-development coverage, but the named AI-specific inventory, model-scanning, registry, MCP or shadow-AI mechanism remains a GAISSF residual.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D4-CTL-05 Third-Party AI Api Security Assessment	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.19; 5.20; 5.21; 5.22; 5.23; 8.20; 8.21; 8.22	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides substantial asset, supplier, cloud, vulnerability and secure-development coverage, but the named AI-specific inventory, model-scanning, registry, MCP or shadow-AI mechanism remains a GAISSF residual.
D4-CTL-06 Shadow AI Discovery & Governance	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.9; 5.11; 5.23; 8.9	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides substantial asset, supplier, cloud, vulnerability and secure-development coverage, but the named AI-specific inventory, model-scanning, registry, MCP or shadow-AI mechanism remains a GAISSF residual.

GAISSE control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D4-CTL-07 AI Software Composition Analysis (SCA)	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.9; 5.21; 8.4; 8.8; 8.9; 8.25; 8.26; 8.28; 8.29; 8.30; 8.32	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 provides substantial asset, supplier, cloud, vulnerability and secure-development coverage, but the named AI-specific inventory, model-scanning, registry, MCP or shadow-AI mechanism remains a GAISSE residual.
D5-CTL-01 Harmful Content Blocking	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.31; 5.32; 5.34; 8.12; 8.23; 8.26	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 supports privacy, data leakage, intellectual-property and web-filtering controls, but does not prescribe the named AI content-safety, watermark, copyright-detection or privacy-preserving-ML acceptance criterion.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D5-CTL-02 PII Leakage Prevention	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.12; 5.13; 5.14; 5.15; 5.33; 5.34; 8.10; 8.11; 8.12; 8.15	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports privacy, data leakage, intellectual-property and web-filtering controls, but does not prescribe the named AI content-safety, watermark, copyright-detection or privacy-preserving-ML acceptance criterion.
D5-CTL-03 Copyright Detection	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.31; 5.32; 5.34; 8.12; 8.23; 8.26	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports privacy, data leakage, intellectual-property and web-filtering controls, but does not prescribe the named AI content-safety, watermark, copyright-detection or privacy-preserving-ML acceptance criterion.

GAISSE control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D5-CTL-04 AI Watermarking Robustness	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.31; 5.32; 5.34; 8.12; 8.23; 8.26	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 supports privacy, data leakage, intellectual-property and web-filtering controls, but does not prescribe the named AI content-safety, watermark, copyright-detection or privacy-preserving-ML acceptance criterion.
D5-CTL-05 Privacy-By-Design Verification	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSE validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.12; 5.13; 5.14; 5.15; 5.33; 5.34; 8.10; 8.11; 8.12; 8.15; 8.9; 8.24; 8.25; 8.29; 8.31	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSE pass threshold is established by this crosswalk.	ISO/IEC 27001 supports privacy, data leakage, intellectual-property and web-filtering controls, but does not prescribe the named AI content-safety, watermark, copyright-detection or privacy-preserving-ML acceptance criterion.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D5-CTL-06 Privacy-Preserving MI Validation	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.12; 5.13; 5.14; 5.15; 5.33; 5.34; 8.10; 8.11; 8.12; 8.15	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 supports privacy, data leakage, intellectual-property and web-filtering controls, but does not prescribe the named AI content-safety, watermark, copyright-detection or privacy-preserving-ML acceptance criterion.
D6-CTL-01 Human-In-The-Loop For High-Risk Actions	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.2; 5.3; 5.4; 6.3	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides strong management-system and information-security evidence reuse, but GAISSF retains AI-specific scope, oversight, model documentation, incident, decommissioning and validation operating-effectiveness requirements.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D6-CTL-02 Audit Trail Completeness	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.22; 8.15; 8.16; 8.17	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides strong management-system and information-security evidence reuse, but GAISSF retains AI-specific scope, oversight, model documentation, incident, decommissioning and validation operating-effectiveness requirements.
D6-CTL-03 AI Model Card Completeness	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.33; 5.37; 7.5; 8.15	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides strong management-system and information-security evidence reuse, but GAISSF retains AI-specific scope, oversight, model documentation, incident, decommissioning and validation operating-effectiveness requirements.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D6-CTL-04 AI Incident Response Readiness	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.24; 5.25; 5.26; 5.27; 5.28; 6.8	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides strong management-system and information-security evidence reuse, but GAISSF retains AI-specific scope, oversight, model documentation, incident, decommissioning and validation operating-effectiveness requirements.
D6-CTL-05 Model Deprecation & Decommissioning	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.11; 7.14; 8.10; 8.32	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides strong management-system and information-security evidence reuse, but GAISSF retains AI-specific scope, oversight, model documentation, incident, decommissioning and validation operating-effectiveness requirements.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D6-CTL-06 Third-Party AI Vendor Governance	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.19; 5.20; 5.21; 5.22; 5.23; 8.20; 8.21; 8.22	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides strong management-system and information-security evidence reuse, but GAISSF retains AI-specific scope, oversight, model documentation, incident, decommissioning and validation operating-effectiveness requirements.
D6-CTL-07 AI Resilience & Business Continuity	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.29; 5.30; 7.5; 7.11; 8.13; 8.14	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides strong management-system and information-security evidence reuse, but GAISSF retains AI-specific scope, oversight, model documentation, incident, decommissioning and validation operating-effectiveness requirements.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D7-CTL-H01 AI-Generated Phishing Simulation	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 6.3; 6.8; 8.7; 8.23	Supporting Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides threat intelligence, awareness, authentication and incident controls, but does not prescribe AI-generated phishing, deepfake, social-engineering or AI-enhanced attack scenarios and acceptance criteria.
D7-CTL-H02 Deepfake Detection Training	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 6.3; 6.8; 8.7; 8.23	Supporting Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides threat intelligence, awareness, authentication and incident controls, but does not prescribe AI-generated phishing, deepfake, social-engineering or AI-enhanced attack scenarios and acceptance criteria.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D7-CTL-H03 Out-Of-Band Authentication	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.15; 5.16; 5.17; 5.18; 8.5; 8.18	Strong partial High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides threat intelligence, awareness, authentication and incident controls, but does not prescribe AI-generated phishing, deepfake, social-engineering or AI-enhanced attack scenarios and acceptance criteria.
D7-CTL-H04 AI Social Engineering IR	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 6.3; 6.8; 8.7; 8.23	Supporting Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides threat intelligence, awareness, authentication and incident controls, but does not prescribe AI-generated phishing, deepfake, social-engineering or AI-enhanced attack scenarios and acceptance criteria.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D7-CTL-H05 AI-Enhanced External Attack Defense	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29	Supporting Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 provides threat intelligence, awareness, authentication and incident controls, but does not prescribe AI-generated phishing, deepfake, social-engineering or AI-enhanced attack scenarios and acceptance criteria.
D8-CTL-01 Eu AI Act Risk Tier Mapping	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 4.2; 5.31; 5.35; 5.36; 7.5; 9.2; 9.3; 4.1; 4.3	Contextual High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 does not establish conformity with the external AI law, standard or sector regime named by this control; separate authoritative interpretation and evidence remain required.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D8-CTL-02 Iso 42001 Gap Analysis	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 4.2; 5.31; 5.35; 5.36; 7.5; 9.2; 9.3; 4.1; 4.3	Contextual High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 does not establish conformity with the external AI law, standard or sector regime named by this control; separate authoritative interpretation and evidence remain required.
D8-CTL-03 Gpai Technical Documentation Verification	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.33; 8.9; 8.24; 8.25; 8.29; 8.31; 4.2; 5.31; 5.35; 5.36; 7.5; 9.2; 9.3; 5.37; 8.15	Contextual High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 does not establish conformity with the external AI law, standard or sector regime named by this control; separate authoritative interpretation and evidence remain required.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D8-CTL-04 Dora Ict Incident Reporting (Financial Sector)	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.24; 5.25; 5.26; 5.27; 5.28; 6.8; 4.2; 5.31; 5.35; 5.36; 7.5; 9.2; 9.3	Contextual High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 does not establish conformity with the external AI law, standard or sector regime named by this control; separate authoritative interpretation and evidence remain required.
D8-CTL-05 Nist Sp 800-218A Compliance Check	Use an independently controlled validation method appropriate to the control, system boundary, threat model and assurance objective. Where a GAISSF validation asset is published, current and applicable, it may be used as one method.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 4.2; 5.31; 5.35; 5.36; 7.5; 9.2; 9.3	Contextual High	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 does not establish conformity with the external AI law, standard or sector regime named by this control; separate authoritative interpretation and evidence remain required.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D9-CTL-01 Physical Harm Boundary Enforcement	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. No universal SIL/DAL or certification level is implied.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 7.1; 7.2; 7.3; 7.4; 7.5; 7.8; 7.11; 7.13; 8.16	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information and physical security, continuity and monitoring, but does not replace functional-safety engineering or prescribe the GAISSF physical-AI mechanism and acceptance criteria.
D9-CTL-02 Safe State And Graceful Degradation	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. No universal SIL/DAL or certification level is implied.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.29; 5.30; 7.5; 7.11; 8.13; 8.14	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information and physical security, continuity and monitoring, but does not replace functional-safety engineering or prescribe the GAISSF physical-AI mechanism and acceptance criteria.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D9-CTL-03 Human Override And Emergency Stop	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. No universal SIL/DAL or certification level is implied.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.9; 5.21; 8.4; 8.8; 8.9; 8.25; 8.26; 8.28; 8.29; 8.30; 8.32; 5.2; 5.3; 5.4; 6.3	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information and physical security, continuity and monitoring, but does not replace functional-safety engineering or prescribe the GAISSF physical-AI mechanism and acceptance criteria.
D9-CTL-04 Cyber-Physical Attack Detection	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. No universal SIL/DAL or certification level is implied.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.7; 8.7; 8.8; 8.16; 8.20; 8.23; 8.29; 7.1; 7.2; 7.3; 7.4; 7.5; 7.8; 7.11; 7.13	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information and physical security, continuity and monitoring, but does not replace functional-safety engineering or prescribe the GAISSF physical-AI mechanism and acceptance criteria.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D9-CTL-05 Physical Environment Integrity Monitoring	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. No universal SIL/DAL or certification level is implied.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.22; 8.15; 8.16; 8.17; 5.33; 8.9; 8.24; 8.25; 8.29; 8.31; 7.1; 7.2; 7.3; 7.4; 7.5; 7.8; 7.11; 7.13	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information and physical security, continuity and monitoring, but does not replace functional-safety engineering or prescribe the GAISSF physical-AI mechanism and acceptance criteria.
D9-CTL-06 Actuator Command Verification	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. No universal SIL/DAL or certification level is implied.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.33; 8.9; 8.24; 8.25; 8.29; 8.31; 7.1; 7.2; 7.3; 7.4; 7.5; 7.8; 7.11; 7.13; 8.16	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information and physical security, continuity and monitoring, but does not replace functional-safety engineering or prescribe the GAISSF physical-AI mechanism and acceptance criteria.

GAISSF control	Validation method / evidence expectation	ISO/IEC 27001 locations	Relationship / confidence	Evidence potentially reusable	Additional validation / assurance	Residual / notably absent
D9-CTL-07 Physical Incident Evidence Preservation	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable. No universal SIL/DAL or certification level is implied.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; 9.1; 5.24; 5.25; 5.26; 5.27; 5.28; 6.8; 7.1; 7.2; 7.3; 7.4; 7.5; 7.8; 7.11; 7.13; 8.16	Partial Medium	ISMS scope and context; information-security risk assessment and treatment; Statement of Applicability; Annex A implementation records; supplier, access, logging, incident, continuity, privacy, secure-development, audit, management-review and corrective-action evidence applicable to the cited locations.	Qualify ISO/IEC 27001 evidence for matching scope, system, period, provenance, relevance and operating effectiveness. Define implementation-specific acceptance criteria, sample size, test conditions and limitations; no universal numeric GAISSF pass threshold is established by this crosswalk.	ISO/IEC 27001 addresses information and physical security, continuity and monitoring, but does not replace functional-safety engineering or prescribe the GAISSF physical-AI mechanism and acceptance criteria.

8. Reverse Traceability Summary

ISO location	Primary subject	GAISSF reuse / limitation
Clauses 4-5	Context, scope, leadership, policy and roles	Strong reuse for D6/D8 governance and control ownership. Mapping correspondence does not establish evidence sufficiency, GAISSF conformance, or operating effectiveness.
Clause 6	Information-security risk assessment, treatment, SoA and objectives	Cross-domain evidence reuse; additional GAISSF controls are expressly possible under 6.1.3. Mapping correspondence does not establish evidence sufficiency, GAISSF conformance, or operating effectiveness.
Clauses 7-8	Resources, competence, communications, documentation and operation	Supports implementation records; does not replace AI-specific validation. Mapping correspondence does not establish evidence sufficiency, GAISSF conformance, or operating effectiveness.
Clauses 9-10	Monitoring, audit, management review and corrective action	Strong assurance reuse across all domains. Mapping correspondence does not establish evidence sufficiency, GAISSF conformance, or operating effectiveness.
A.5 Organizational	Policy, assets, suppliers, incidents, continuity, compliance, privacy and procedures	Broad support for D4-D8 and governance aspects of all domains. Mapping correspondence does not establish evidence sufficiency, GAISSF conformance, or operating effectiveness.
A.6 People	Screening, terms, awareness, confidentiality, remote work and reporting	Supports D6/D7; AI-specific exercises remain residual. Mapping correspondence does not establish evidence sufficiency, GAISSF conformance, or operating effectiveness.
A.7 Physical	Physical perimeter, monitoring, environment, equipment and media	Supports D9 infrastructure security but not functional safety. Mapping correspondence does not establish evidence sufficiency, GAISSF conformance, or operating effectiveness.
A.8 Technological	Access, authentication, malware, vulnerabilities, configuration, DLP, logging, monitoring, cryptography, networks and secure development	Strong technical-security support for D1-D5, but AI-specific attack models and thresholds remain residual. Mapping correspondence does not establish evidence sufficiency, GAISSF conformance, or operating effectiveness.

9. Amendment and ISO/IEC 27002 Status

ISO currently lists ISO/IEC 27001:2022, Edition 3 (2022-10), as published and identifies ISO/IEC 27001:2022/Amd 1:2024, Climate action changes, as a published amendment. The source package states that the 2022 base text was verified against a licensed copy. The amendment text was not supplied in the package, so this update records its public status and does not claim independent full-text amendment verification.

10. Validation and Assurance Handling

- All 59 GAISSF controls retain traceability to the ISO/IEC 27001 locations used by the source package and to an implementation-specific validation expectation. This public crosswalk does not depend on held/internal GAISSF VTS identifiers, repository paths, benchmark suites or test harnesses.
- ISO/IEC 27001 evidence may reduce documentary duplication where scope, provenance, currency, completeness and relevance are sufficient, but it does not waive GAISSF technical validation or independent assessment.
- Demo fixtures, mock outputs and unsigned or untraceable records are not sufficient evidence of operating effectiveness or independent assurance.
- Inherited evidence, compensating controls and validation substitutions require documented rationale and independent assessor or reviewer consideration. GAISSF certification is not currently offered.

11. Source Register and Publication Rules

Source	Treatment
ISO/IEC 27001:2022, Edition 3	Primary external baseline. Source package states licensed full text was used for original verification; do not redistribute protected text.
ISO/IEC 27001:2022/Amd 1:2024	Published amendment: Climate action changes. Public status rechecked 5 Oct 2026; amendment text was not included in the supplied package for independent full-text verification.
ISO/IEC 27002:2022	Supplementary implementation guidance only; not treated as part of the verified mapping baseline unless separately verified.
GAISSF-NOR-001 / NOR-004 v1.0	Current GAISSF framework/control baseline. Applicable-Control Baseline = 52 D1-D8 + applicable D9.
GAISSF validation assets	Not a public dependency. Use only where published, current and applicable.
PAI-SF™ / CSX-PAISF-004	Use alongside D9 where Physical AI is in scope; CSX-PAISF-004 is mapping only, not equivalence or automatic conformance.

- Retain GAISSF-CRO-020 as an informative, version-controlled ****Draft for Publication**** until independent crosswalk review and explicit publication approval are complete.
- Do not reproduce the supplied ISO/IEC PDF or substantial ISO text.
- Do not claim that ISO/IEC 27001 certification establishes GAISSF conformity or AI safety.
- Publish the explanatory document together with the XLSX and JSON registers.
- Trigger review upon a material revision to GAISSF, ISO/IEC 27001, ISO/IEC 27001:2022/Amd 1:2024, the relevant evidence base, or the crosswalk methodology.