

GAISSF™ v1.0

Migration Guide

Transition from Existing Governance, Security and Assurance Frameworks

Global AI Safety and Security Framework

GAISSF-IMP-012 | Public | Final Publication

Issued 29 June 2026 | Updated 05 October 2026

© 2026 ODA3 Pvt Ltd

Document Control

Attribute	Controlled value
Title	GAISSF™ v1.0 Migration Guide
Canonical framework	Global AI Safety and Security Framework
Document ID	GAISSF-IMP-012
Purpose	Provide a structured method for migrating from existing frameworks into the GAISSF™ operating and evidence model
Primary audience	CISOs, AI governance leads, security architects, compliance officers, standards teams, internal audit, program managers, control owners and independent assessors or reviewers
Dependencies	GAISSF-NOR-001 through GAISSF-NOR-008; GAISSF-IMP-009 through GAISSF-IMP-011 where published and current
Precedence	GAISSF-NOR-001 governs framework interpretation; GAISSF-NOR-004 governs control records. Crosswalks inform mapping only and do not override normative requirements.
Control baseline	59 controls across nine domains; Foundational = 52 D1-D8 controls; D9 additional/conditional where Physical AI or cyber-physical actuation is in scope
Status	Final Publication
Issued / Updated	Issued 29 June 2026; updated 05 October 2026
Contact	contact@oda3.org
Distribution	Public - docs.oda3.org / official ODA3 publication channels
Classification	Public

Legal and Reliance Notice

© 2026 ODA3 Pvt Ltd. Published market-facing by ODA3 Institute.

GAISSF™ is the framework mark used for the Global AI Safety and Security Framework. Third-party standards, frameworks, regulations and marks remain the property of their respective owners. Use of GAISSF™ materials is subject to the applicable GAISSF Ecosystem Licence (GEL) and published terms.

References to external frameworks are for identification, transition planning and evidence analysis only. No endorsement, affiliation, equivalence, substitution, certification credit or recognition is implied.

This guide is informative implementation guidance. It does not constitute legal, regulatory, safety, engineering, certification or audit advice; create a legal safe harbour; establish a legal standard of care; determine statutory compliance; or create eligibility for any certification. GAISSF certification is not currently offered; any future certification would require a separately issued scheme.

Foreword

Most organizations adopting GAISSF™ will already operate security, privacy, risk, quality, safety or AI-governance frameworks. Migration should therefore reuse verified capabilities and evidence while identifying GAISSF-specific gaps. It should not duplicate functioning controls or assume that similarly named requirements are equivalent.

1. Purpose and Scope

This guide provides a repeatable method for transitioning from existing frameworks, management systems, control libraries and assurance programs into GAISSF™ v1.0. It covers source-framework inventory, mapping, evidence reuse, gap analysis, control ownership, Applicable-Control Baseline establishment, migration waves, parallel operation, retirement of legacy artifacts and post-migration assessment.

The guide applies to migration from single frameworks and hybrid estates, including ISO/IEC management systems, NIST publications, OWASP and MITRE security resources, CIS Controls, regulatory programs and internal control libraries.

GAISSF-NOR-001 governs conformance-tier interpretation. Foundational comprises the 52 canonical controls in D1-D8. D9 contains seven additional controls that become mandatory where Physical AI or cyber-physical actuation is in scope. Operational and Optimized use the same applicable-control scope with stronger operating-effectiveness evidence, monitoring and assurance expectations.

2. Migration Principles

Principle	Migration meaning
Map intent, not labels	Controls with similar titles may differ in scope, evidence, frequency or assurance depth.

Principle	Migration meaning
Reuse only verified capability	Existing controls and evidence should be reused only after scope, currency and operating effectiveness are confirmed.
Preserve source obligations	Migration to GAISSF™ does not remove legal, contractual, sector or external certification obligations.
Separate mapping from conformance	A mapping indicates relationship; it does not demonstrate implementation, evidence sufficiency or GAISSF™ conformance.
Retain provenance	Every migrated mechanism and evidence artifact should identify its source framework and transformation history.
Resolve gaps explicitly	Partial, unsupported and conflicting requirements should be documented rather than forced into false equivalence.
Avoid duplicate operation	Consolidate overlapping workflows where control outcomes and evidence remain sufficient.
Maintain assurance continuity	Do not retire legacy controls until GAISSF replacements are implemented, evidenced and accepted.

3. Migration Relationship Types

Relationship	Meaning	Migration treatment
Full alignment for stated scope	Requirements and evidence expectations appear materially aligned within a defined boundary	May support reuse after verification; retain mapping rationale and limitations
Substantial alignment	Most intent is covered, but some scope, evidence or operation differs	Reuse mechanism; add targeted enhancement
Partial alignment	Only part of the GAISSF objective is addressed	Retain source control and implement missing elements
Dependency	Source control enables GAISSF but does not satisfy it	Link as supporting mechanism
Complementary	Source addresses a related but distinct risk outcome	Operate alongside GAISSF control
Conflict	Source requirement or implementation conflicts with GAISSF or applicable law	Escalate for governance and legal resolution
No mapping	No reliable relationship is identified	Implement GAISSF requirement independently

Relationship labels are analytical aids, not declarations of legal or technical equivalence. A crosswalk or mapping does not establish evidence sufficiency, automatic conformance, mutual recognition or certification credit.

4. Migration Lifecycle

Phase	Primary activity	Output
0 — Mobilize	Define objective, scope, owners and migration governance	Migration charter
1 — Inventory	Catalogue source frameworks, controls, certifications and evidence	Source register
2 — Normalize	Standardize identifiers, terminology, scope and evidence metadata	Normalized source library
3 — Map	Relate source requirements to GAISSF controls	Draft crosswalk
4 — Validate	Review mappings for semantic and evidentiary accuracy	Approved mapping set
5 — Assess	Test migrated mechanisms and evidence against GAISSF	Gap assessment
6 — Design	Define target operating model and remediation	Migration roadmap
7 — Transition	Implement migration waves and parallel operation	Migrated controls
8 — Assure	Perform independent readiness and operating-effectiveness review	Assessment or assurance report
9 — Retire	Archive or retire superseded legacy artifacts	Retirement record
10 — Sustain	Maintain crosswalks, evidence and release impacts	Continuing migration governance

5. Phase 0 - Establish Migration Governance

Role	Migration accountability
Executive sponsor	Approve scope, resources and material risk decisions
Migration lead	Coordinate mapping, transition and reporting
Source-framework owner	Explain current implementation and obligations
GAISSF control owner	Accept migrated mechanisms and evidence
Standards architect	Validate semantic relationships and crosswalk quality
Legal/compliance	Preserve applicable obligations and resolve conflicts
Internal assurance	Challenge evidence reuse and conformance claims before independent review
Assessment liaison	Coordinate effects on assessment scope, evidence representations and any external certification obligations

5.1 Migration charter minimum content

- Migration objective and intended GAISSF™ tier
- Source frameworks and organizational scope
- Systems, regions, suppliers and external certifications affected
- Applicable-Control Baseline decision, including D9 applicability
- Decision rights and mapping approval authority
- Evidence-reuse rules
- Parallel-operation and retirement criteria
- Migration risks and constraints
- Milestones and assessment gates

6. Phase 1 - Inventory the Source Environment

Register field	Required content
Source identifier	Standard, framework, regulation, policy or internal control ID
Edition/version	Controlled version and effective date
Status	Current, superseded, withdrawn or locally modified
Owner	Accountable organizational function
Scope	Systems, entities, locations and processes covered
Requirement text	Controlled summary or licensed reference
Implementation	Policy, workflow, technical mechanism or inherited control
Evidence	Current evidence artifacts and period
Assurance	Audit, test, external certification or review status
Dependencies	Suppliers, shared services and external systems
Constraints	Licence, legal, confidentiality or access limitations

7. Phase 2 - Normalize the Source Library

Normalization creates a consistent basis for comparison. It should preserve original wording and provenance while adding common metadata.

Normalization action	Purpose
Standardize identifiers	Prevent duplicate or ambiguous source references
Separate requirement from guidance	Avoid mapping informative text as mandatory
Record scope and applicability	Identify hidden differences between similarly worded controls
Classify evidence type	Distinguish policy, design, operating, technical and assurance evidence
Record frequency	Identify one-time versus recurring obligations
Identify approval authority	Preserve governance and risk decisions
Tag lifecycle stage	Map requirements to acquisition, design, deployment, operation or retirement
Tag domain and threat	Support controlled crosswalk analysis

8. Phase 3 - Build the Crosswalk

8.1 Mapping procedure

1. Read the complete GAISSF™ control objective and requirement.
2. Identify source requirements addressing the same risk outcome.
3. Compare scope, subject, trigger, frequency, evidence and assurance expectations.
4. Assign a relationship type.
5. Document the mapping rationale and limitations.
6. Identify unmapped GAISSF™ elements.
7. Record source evidence proposed for reuse.
8. Submit the mapping for independent review.

8.2 Crosswalk record

Field	Content
GAISSF control ID	Exact identifier from GAISSF-NOR-004
Source framework	Controlled source identifier and edition
Source requirement	Clause, function, category, control or provision
Relationship	Full alignment, substantial, partial, dependency, complementary, conflict or none
Scope conditions	Systems, jurisdictions, Applicable-Control Baseline, tiers and assumptions
Evidence reuse	Artifacts proposed for reuse
GAISSF gap	Missing requirement or evidence element
Migration action	Retain, enhance, replace, add or retire
Reviewer	Independent mapping reviewer
Approval status	Draft, approved, rejected or superseded

9. Phase 4 - Validate Mapping Quality

Validation question	Failure indicator
Does the source requirement address the same objective?	Keyword similarity without common risk outcome
Is the scope materially aligned?	Source applies to IT generally but not models, data, agents or Physical AI
Are mandatory and informative statements separated?	Guidance treated as a requirement
Is the operating frequency adequate?	Annual review mapped to continuous monitoring
Is evidence comparable?	Policy mapped to technical operating evidence
Are exclusions visible?	Source applicability assumptions omitted
Is assurance depth comparable?	Self-attestation treated as independent testing
Are legal obligations preserved?	GAISSF™ mapping used to claim legal compliance

10. Phase 5 - Assess Reusable Controls and Evidence

Existing implementation should be evaluated as if it were a candidate GAISSF™ control mechanism. Source-framework status or external certification alone is not sufficient.

Assessment dimension	Migration test
Design	Does the mechanism address the complete GAISSF requirement?
Scope	Does it cover all in-scope systems, suppliers, users and locations?
Implementation	Is it deployed consistently?
Operation	Is there representative evidence across the required period?
Effectiveness	Does testing show the intended risk outcome?
Currency	Is the evidence current for the deployed model, data and architecture?
Integrity	Is evidence authentic, attributable and protected?
Traceability	Can the mechanism and evidence be linked to the GAISSF control?

10.1 Evidence reuse decision

Decision	Criteria	Treatment
Reuse	Current, scope-aligned and sufficient	Link directly to GAISSF evidence index
Reuse with enhancement	Useful but incomplete	Add missing evidence or mechanism
Reference only	Contextual but insufficient for conformance	Retain as supporting material
Reject	Stale, unverifiable, out of scope or misleading	Generate new evidence

11. Phase 6 - Design the Target Operating Model

Target element	Migration design question
Control ownership	Can existing owners accept GAISSF accountability?
Policies and standards	Can source documents be consolidated without losing obligations?
Workflows	Which reviews, approvals and gates can be reused?
Technical controls	Which mechanisms need extension for AI-specific risks?
Evidence repository	Can existing GRC, evidence or review repositories support GAISSF™ metadata and provenance?
Assurance	Can current review and testing methods assess GAISSF™ design and operating effectiveness?
Metrics	Which source metrics remain valid and which require AI-specific measures?
Exceptions	Can existing risk-acceptance workflows meet GAISSF traceability and expiry needs?

12. Migration from ISO/IEC Management Systems

Organizations with ISO/IEC 27001, ISO/IEC 42001, ISO/IEC 27701 or related management systems can often reuse governance, document control, internal audit, management review, corrective action and risk-management capabilities, subject to edition, scope and evidence verification.

Reusable capability	Typical GAISSF use	Likely migration gap
Context and scope	GAISSF assessment boundary	AI-system, model, agent and supplier granularity
Leadership and policy	D6 - Governance, Accountability & Human Oversight	AI-specific decision rights and system ownership
Risk management	Applicable GAISSF™ risk and assurance mechanisms	Threat, safety, autonomy and harmful-output scenarios
Competence and awareness	Role-based GAISSF capability	AI engineering and independent-assessment competence
Operational control	Applicable D1-D9 implementation	Technical AI-specific mechanisms
Performance evaluation	Monitoring and internal assurance	Control-health and model-behavior evidence
Corrective action	Nonconformity and improvement	Control-specific root cause and retest evidence

13. Migration from NIST AI RMF and NIST CSF

NIST AI RMF and CSF functions can provide governance and risk-outcome structures. Migration requires translating outcomes and profiles into GAISSF™ control-level requirements, evidence and assessment boundaries.

NIST capability	GAISSF transition use	Additional work
Govern/GOVERN	Governance, roles, policy and oversight	Control ownership, assessment scope and evidence records
Map/MAP	Context, inventory, impacts and risk scenarios	Applicable-Control Baseline and system boundary
Measure/MEASURE	Evaluation, metrics and testing	Control-specific evidence and operating-effectiveness criteria
Manage/MANAGE	Risk treatment, prioritization and response	Exception, nonconformity and corrective-action linkage
CSF Govern/Identify	Enterprise security governance and asset context	AI model, data, agent and physical-AI extensions
CSF Protect/Detect/Respond/Recover	Security operating mechanisms	AI-specific threats, harmful outputs and model behavior

14. Migration from OWASP and MITRE Resources

OWASP and MITRE resources are primarily threat, weakness, attack and verification references. They are valuable for applicable GAISSF™ domains and threat mappings but do not by themselves establish a complete governance, evidence or assurance program.

Source use	Migration value	Gap to GAISSF
OWASP LLM/Agentic risks	Threat scenarios, test cases and engineering controls	Governance, evidence periods, risk acceptance and assessment
OWASP ASVS/SAMM	Application-security and maturity practices	Model, data, autonomy, content-safety and physical-AI scope
MITRE ATLAS	Adversary techniques and threat modelling	Control requirements, operating evidence and governance
MITRE ATT&CK	Enterprise attack context	AI-specific model, data and agent behavior

15. Migration from CIS Controls

CIS Controls provide a prioritized cybersecurity baseline. They can support identity, inventory, vulnerability management, logging, configuration, incident response and supplier controls. AI-specific and Physical-AI scope must still be assessed against GAISSF™.

CIS capability	Likely GAISSF support	AI-specific enhancement
Asset and software inventory	System and component inventory	Models, datasets, agents, tools and prompts
Access control	Identity and privilege mechanisms	Tool, model, agent and transaction authorization
Secure configuration	Platform hardening	Model endpoints, orchestration and AI gateways
Audit log management	Security telemetry	Prompts, plans, tool calls, outputs and model decisions
Vulnerability management	Platform and application security	Model and data attack surfaces
Incident response	Containment and recovery	Harmful outputs, model compromise and unsafe autonomy

16. Migration from Regulatory Compliance Programs

Regulatory programs should be preserved as independent obligations. GAISSF™ may organize operational evidence and controls, but it does not determine legal compliance or replace jurisdiction-specific assessments.

- Maintain a controlled legal and regulatory obligations register.
- Map each obligation to GAISSF™ only where the relationship is documented and reviewed.
- Identify requirements outside GAISSF™ scope.
- Preserve regulator-specific records, reporting and retention.
- Do not claim compliance solely because a GAISSF™ control is implemented.

17. Migration from Internal Control Libraries

Internal-library issue	Migration treatment
Duplicate controls	Consolidate only after confirming scope and evidence alignment
Local terminology	Map to GAISSF-NOR-005 terms and retain aliases
Composite controls	Decompose where one internal control maps to multiple GAISSF controls
Overly granular controls	Group for operation while retaining traceability
Unowned controls	Assign accountable and operating owners
Policy-only controls	Add technical and operating mechanisms
Unversioned controls	Place under document and change control
Unverified evidence	Validate integrity, currency and scope before reuse

18. Migration Waves

Wave	Scope	Exit condition
Wave 1 — Governance	Scope, inventory, ownership, risk, exceptions and evidence architecture	Governance operating and Applicable-Control Baseline approved
Wave 2 — Shared security	Identity, logging, secure development, incident response and suppliers	Shared mechanisms verified
Wave 3 — AI engineering	Model, data, adversarial robustness, agents and deployment gates	Technical gaps remediated
Wave 4 — Human and content safety	Transparency, oversight, harmful-output and user recourse	Operational tests passed
Wave 5 — Physical AI	Where applicable: D9 safety, override, safe state, actuation and HIL/simulation	Specialist assurance accepted
Wave 6 — Assessment readiness	Evidence period, internal assurance and corrective action	Readiness decision approved

Migration waves are sequencing aids, not conformance tiers. D9 applicability is determined by system scope, not by migration-wave completion.

19. Parallel Operation and Retirement

Source and GAISSF™ controls may need to operate in parallel until the migrated mechanism is stable and accepted.

Retirement criterion	Required evidence
GAISSF replacement implemented	Approved control implementation record
Operating period completed	Representative operating evidence
Effectiveness validated	Test or assurance result
Obligations preserved	Legal, contractual and external-certification review where applicable
Dependencies migrated	Updated workflows, tooling and ownership
Users trained	Training and communication record
Rollback available	Archived source control and recovery plan
Retirement approved	Named decision authority and date

20. Migration Risks and Controls

Migration risk	Control response
False equivalence	Independent semantic review and relationship classification
Evidence over-reuse	Revalidate scope, currency, integrity and effectiveness
Obligation loss	Legal and external-certification dependency review where applicable
Control gap during transition	Parallel operation and explicit cutover gates
Duplicate bureaucracy	Consolidate workflows after assurance acceptance
Mapping drift	Version-controlled crosswalks and release impact review
Owner confusion	Single target ownership model and RACI
Premature retirement	Formal retirement criteria and approval

21. Migration Metrics

Metric	Purpose	Caution
GAISSF controls with approved mappings	Measure crosswalk progress	Mapping is not conformance
Controls with reusable evidence	Estimate migration leverage	Quality and scope determine usability
Partial or no-map controls	Identify remediation demand	Do not force mappings to improve percentages
Legacy controls retired	Track simplification	Retirement must preserve obligations
Migration findings overdue	Track execution risk	Prioritize by impact
Evidence rejected during assurance	Measure reuse quality	Investigate systemic causes
Crosswalk version currency	Detect mapping drift	Review after external-source changes

22. Migration Work Packages

Work package	Activities	Deliverable
Source governance	Confirm edition, ownership, status and obligations	Approved source register
Semantic mapping	Compare objective, scope, trigger, evidence and assurance	Controlled crosswalk
Evidence qualification	Test currency, integrity, scope and effectiveness	Reuse decision register
Gap remediation	Implement missing GAISSF-specific mechanisms	Migration roadmap and closure
Parallel operation	Run source and target controls until acceptance	Cutover evidence
Retirement	Preserve obligations, archive and remove duplication	Retirement record

23. Mapping Confidence and Review

Confidence	Criteria	Treatment
High	Same objective, scope, frequency and evidence; independently reviewed	May support reuse subject to operating test
Medium	Substantial overlap with documented differences	Enhance and retest
Low	Keyword or contextual relationship only	Reference only; not evidence of conformance
Rejected	Misleading, obsolete or incompatible	Do not use

Confidence describes the strength of a mapping rationale. It does not establish equivalence, evidence sufficiency or conformance.

24. Hybrid Framework Example

An organization operating ISO/IEC 27001, NIST AI RMF and OWASP LLM guidance may reuse management-system governance, enterprise risk workflows and security test cases. It must still establish one GAISSF™ Applicable-Control Baseline, a control-ownership model, a system-specific evidence index, agentic and Physical-AI treatment where applicable, and GAISSF-specific assessment records.

25. Assessment Transition Controls

- Do not represent an existing external certification as GAISSF™ certification.
- Confirm whether the source assessment or certification scope matches the GAISSF™ boundary.
- Preserve certificate and audit-report licence restrictions where applicable.
- Identify evidence that can be considered by the independent assessor or reviewer.
- Control public statements during parallel-framework and external-certification periods.
- GAISSF certification is not currently offered; any future certification would require a separately issued scheme and cannot be inferred from migration completion.

26. Migration Validation and Completion

- All 52 D1-D8 controls have an approved migration disposition.
- D9 applicability has been explicitly determined; all applicable D9 controls have an approved migration disposition.
- The Applicable-Control Baseline is fully enumerated.
- Mappings are independently reviewed and version controlled.
- Reusable mechanisms and evidence have passed GAISSF™ assessment.
- Unmapped and partial gaps have corrective actions.
- Legacy obligations and external certifications remain traceable.
- Parallel-operation and retirement decisions are documented.
- Internal assurance has verified target-state operation.
- Public claims have been reviewed; any future certification claim or mark use is separately authorized.
- Continuing crosswalk maintenance is assigned.

27. Legal and Regulatory Integration

GAISSF™ provides an operational security, safety, governance and evidence framework. It does not determine which laws apply, establish statutory compliance, create a legal safe harbour, define a legal standard of care, replace competent legal advice, or guarantee that evidence collected for GAISSF™ purposes will satisfy a regulator, court or other authority. Organizations should maintain a jurisdiction-specific legal and regulatory obligations register and map applicable obligations to their GAISSF™ scope, controls, evidence, reporting processes and decision authorities.

27.1 Legal and regulatory interface requirements

- Identify applicable jurisdictions, regulators, sector rules, contractual duties and internal legal authorities before relying on this guide.
- Maintain a controlled obligations register, reporting-clock register, retention schedule, legal-hold process and conflicts-of-obligation procedure.
- Treat statutory, regulatory and contractual analysis as a parallel workstream to GAISSF™ implementation and assurance.
- Record the legal basis, responsible owner, scope, decision, evidence, deadline and review date for each material obligation.
- Do not represent GAISSF™ conformance, maturity or any future certification as legal approval, permission to operate, immunity from enforcement or proof that harm cannot occur.

27.2 Migration-specific regulatory gap analysis

1. Identify applicable legal, regulatory, contractual and sector obligations.
2. Determine what the source framework actually covers.
3. Record partial, unsupported and conflicting relationships.
4. Assess operational and evidentiary gaps independently of framework mapping.
5. Obtain authorized legal, privacy or compliance review.
6. Track remediation outside the migration-completion claim.

Framework mapping shall not be treated as a safe harbour, legal equivalence or proof of statutory compliance.

28. Legacy Model and Data Legal Review

Review area	Questions
Provenance and licensing	Are source, licence, permitted use and downstream restrictions documented?
Privacy and consent	Is there a valid basis, notice, consent or other authority for processing?
Sensitive populations	Are children's, biometric, health or other protected data involved?
Supplier terms	Do model or dataset terms permit migration, reuse and evidence retention?
Deletion and opt-out	Can statutory, contractual and data-subject requests be executed?
Uncertainty	Is unresolved provenance clearly recorded and risk accepted by authorized owners?

29. Portability, Concentration and Exit Controls

- Test data, model, configuration and evidence export.
- Assess substitute providers and concentration dependencies.
- Define termination assistance, deletion verification and continuity arrangements.
- Preserve legacy evidence until the replacement has operated through an accepted assurance cycle and retention obligations permit disposal.

30. Physical AI and PAI-SF™ Boundary

Where Physical AI or cyber-physical actuation is in scope, GAISSF™ Domain 9 applies in addition to the D1-D8 baseline. PAI-SF™ v1.0 should be used alongside GAISSF™ D9 where applicable to physical/kinetic system risks.

CSX-PAISF-004 is mapping only. Correspondence does not establish equivalence, evidence sufficiency, automatic conformance or certification status.

31. Worked Mapping Rule

A source requirement may be classified as “substantial alignment” only where intent is mostly covered and the remaining scope, evidence, frequency or assurance gap is explicitly stated. Worked examples are illustrative, version-specific and do not establish formal equivalence.

32. Limitations

- This guide does not provide a definitive clause-by-clause crosswalk.
- External frameworks and regulations may change after publication.
- Mappings depend on edition, organizational implementation and assessed scope.
- Evidence accepted under one scheme may not be sufficient under another.
- External certification or accreditation bodies may impose additional migration requirements.
- Migration completion does not establish legal compliance, evidence sufficiency for another scheme, or eligibility for any future GAISSF™ certification.

33. Notably Absent

- No claim of formal equivalence or mutual recognition.
- No automatic certification credit for existing certifications.
- No assurance that one source control maps to exactly one GAISSF™ control.
- No permission to discard source obligations after migration.
- No requirement to replace functioning controls solely to adopt GAISSF™.
- No promise that migration reduces audit or assessment effort or cost.
- No ISO, NIST or other framework safe harbour.
- No requirement that legal counsel personally signs every migration record; review authority is risk-based.
- No permission to retire a legacy control merely because a mapping exists.
- No representation that an ODA3 certification service or certification mark is currently available.

Annex A - Source Framework Register Template

Field	Entry
Source identifier	
Title	
Edition/version	
Status	
Owner	
Scope	
Certification/assurance status	
Evidence repository	
Dependencies	
Constraints	

Annex B - Crosswalk Record Template

GAISSF ID	Source ref.	Relationship	Scope	Evidence	Gap	Action	Status

Annex C - Evidence Reuse Assessment Template

Evidence ID	Source framework	GAISSF control	Scope match	Currency	Integrity	Decision	Reviewer

Evidence ID	Source framework	GAISSF control	Scope match	Currency	Integrity	Decision	Reviewer

Annex D - Legacy Control Retirement Record

Field	Entry
Legacy control ID	
Source framework	
GAISSF replacement	
Obligations preserved	
Operating evidence	
Assurance result	
Dependencies updated	
Approval	
Retirement date	

Annex E - Source Traceability

Migration-guide subject	Controlled source
Normative framework	GAISSF-NOR-001
Control records	GAISSF-NOR-004
Terminology	GAISSF-NOR-005
External references	GAISSF-NOR-006
Release status	GAISSF-NOR-007
Historical decisions	GAISSF-NOR-008
Adoption program	GAISSF-IMP-009 - where published and current
Operational implementation	GAISSF-IMP-010 - where published and current
Deployment and cutover	GAISSF-IMP-011 - where published and current
Physical AI companion	PAI-SF™ v1.0 - where applicable and current
GAISSF / PAI-SF mapping	CSX-PAISF-004 - mapping only; no equivalence, evidence-sufficiency or automatic-conformance effect

Annex F - Publication Record

Version	Date	Change	Status
1.0	29 June 2026	Initial Migration Guide for GAISSF™ v1.0	Final Publication
1.0	05 October 2026	Reconciled profile/D9 applicability, Applicable-Control Baseline, assessment/certification terminology, crosswalk boundaries, R2 placement, canonical domains, PAI-SF™ relationship, dependencies, GEL and publication metadata; no GAISSF™ control was added, removed, renamed or amended.	Updated