

ODA3 INSTITUTE

IMPLEMENTATION GUIDANCE

GAISSF™ v1.0 Adoption Guide

Program Establishment, Governance and Implementation Planning

GAISSF-IMP-009 | Public | Final Publication

Issued 29 June 2026 | Updated 05 October 2026

© 2026 ODA3 Pvt Ltd

Document Control

Attribute	Controlled value
Document ID	GAISSF-IMP-009
Title	GAISSF™ v1.0 Adoption Guide
Doc Type	Implementation guidance - informative
Purpose	Guide organizations in establishing a GAISSF adoption program
Primary Audience	Boards, executives, CISOs, AI governance leads, security architects, compliance, risk, legal, internal assurance and program managers
Dependencies	GAISSF-NOR-001 through GAISSF-NOR-008; downstream implementation guides only where published and current
Precedence	GAISSF-NOR-001 governs framework interpretation; GAISSF-NOR-004 governs control records
Control Baseline	59 controls across nine domains; Foundational = 52 D1-D8 controls; D9 additional/conditional where applicable
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

Reliance notice: This guide supports adoption planning. It does not establish, amend or replace GAISSF requirements. GAISSF-NOR-001 and GAISSF-NOR-004 remain authoritative. This guide does not define conformance-tier membership, create certification eligibility, or determine legal compliance. GAISSF certification is not currently offered; any future certification would require a separately issued scheme.

How to Use This Document

Reader	Recommended use
Executive or board reader	Review purpose, decision rights, legal and regulatory integration, limitations and Notably Absent sections.
Program or control owner	Use workflows, templates, gates, evidence fields and escalation criteria as implementation aids.
Engineering or operations team	Translate guidance into system-specific procedures, configurations, runbooks and testable acceptance criteria.
Legal, privacy or compliance team	Validate jurisdiction-specific obligations, deadlines, retention, disclosure, privilege and regulator-facing requirements.
Independent assessor or reviewer	Use this document as informative context only; test claims against authoritative normative sources and applicable assessment criteria.

Copyright, Licensing and Legal Notices

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

GAISSF™ is used as a framework mark. Use of GAISSF™ materials is subject to the GAISSF Ecosystem Licence (GEL) v1.0. Third-party names and marks remain the property of their respective owners.

This guide does not constitute legal, regulatory, safety, engineering, certification or audit advice. It does not create a legal safe harbour, establish a legal standard of care, or determine statutory compliance in any jurisdiction.

Adoption of GAISSF™ does not by itself establish legal compliance, system safety, security, fairness, reliability, or eligibility for any future GAISSF certification scheme.

Foreword

GAISSF adoption is a program of governance, engineering, evidence and assurance - not a document-acquisition exercise. Organizations obtain value when control ownership, operating processes, technical validation and executive risk decisions are integrated into normal business and system lifecycle practices.

1. Purpose and Scope

This guide provides a structured method for planning and establishing a GAISSF adoption program. It covers sponsorship, scope, governance, resourcing, control ownership, gap assessment, evidence architecture, remediation, internal assurance, external-assessment readiness and continuing operation.

The guide applies to enterprise-wide, business-unit, service, platform, product and AI-system adoption. Organizations should tailor the sequence to their size, sector, jurisdiction, deployment model and risk exposure.

2. Adoption Principles

Principle	Adoption meaning
Authoritative-source discipline	Use NOR-001 and the controlled 59-control catalogue as the source of requirements. Do not re-author controls in local language without traceability.
Scope before scoring	Define organizational, system, geographic, lifecycle and supplier boundaries before assessing conformance.
Risk-based but not optional-by-preference	Apply the applicable GAISSF conformance tier exactly as defined in GAISSF-NOR-001 and document justified applicability decisions or exceptions; do not select only convenient controls.
Evidence over assertion	Require operating evidence showing that controls function in the assessed scope.
Cross-functional ownership	Distribute accountability across governance, security, engineering, data, privacy, safety, legal, procurement and audit.
Integration over parallel bureaucracy	Embed GAISSF into existing management systems, development workflows, risk processes and assurance mechanisms.
Continuous operation	Treat adoption as an operating system with monitoring, review and improvement—not a one-time project.

3. Adoption Outcomes

Outcome	What good looks like	Evidence
Governance established	Executive sponsor, steering body, decision rights and escalation routes are active	Charter, minutes, risk decisions
Scope controlled	In-scope systems, business units, suppliers and locations are enumerated	Scope statement, inventory, architecture diagrams
Controls owned	Each applicable control has accountable and operating owners	RACI, control register
Gaps understood	Design and operating gaps are recorded and prioritized	Gap assessment, risk ratings
Evidence managed	Evidence is indexed, current, traceable and reviewable	Evidence repository and index
Remediation funded	Corrective actions have owners, dates and resources	Approved roadmap, budget, action log
Assurance operating	Internal testing and management review are recurring	Test results, audit reports, review records
External-assessment decision informed	Scope, readiness, cost, public-claim limits and residual risks are understood	Readiness report and executive approval

4. Adoption Lifecycle

Phase	Primary purpose
Phase 0 — Mobilize	Confirm sponsor, mandate, strategic objective and program lead.
Phase 1 — Discover	Inventory AI systems, services, models, data, suppliers and jurisdictions.
Phase 2 — Scope	Define assessment boundary, conformance target and applicable tier.
Phase 3 — Govern	Establish decision rights, control ownership and reporting.

Phase	Primary purpose
Phase 4 — Assess	Perform control-by-control design and operating-effectiveness assessment.
Phase 5 — Remediate	Prioritize and implement corrective actions.
Phase 6 — Evidence	Build assessment-ready evidence packages and traceability.
Phase 7 — Assure	Conduct internal validation, independent review and readiness assessment.
Phase 8 - External assessment and public claims	Pursue independent external assessment where appropriate and control public claims.
Phase 9 — Sustain	Monitor change, threats, performance, exceptions and continued conformance.

5. Phase 0 - Mobilize the Program

5.1 Establish the mandate

- Define the business reason for adoption: assurance, customer requirement, regulatory readiness, risk reduction, market access or internal standardization.
- Name an executive sponsor with authority over scope, funding and cross-functional participation.
- Appoint a program lead responsible for coordination, traceability and reporting.
- Approve a program charter stating objectives, boundaries, assumptions, exclusions and intended assurance or assessment outcome.

5.2 Program charter minimum content

Charter field	Minimum content
Purpose	Why GAISSF is being adopted
Target outcome	Internal conformance, customer assurance, external assessment or staged adoption; any future certification only if a scheme is separately issued
Initial scope	Business units, systems, regions and lifecycle stages
Authority	Sponsor and decision rights
Governance	Steering body and reporting cadence
Resources	Core team, subject-matter support and budget
Milestones	Assessment, remediation, evidence and assurance checkpoints
Dependencies	Legal, procurement, engineering, tooling and supplier constraints
Success criteria	Measurable adoption and readiness outcomes

6. Phase 1 - Discover the Environment

Discovery shall produce an evidence-backed view of the AI estate. The inventory should include internally developed systems, embedded AI functions, third-party services, foundation-model dependencies, agentic components and physical-AI deployments.

Inventory field	Example content
System identifier	Unique name and owner
Purpose and users	Business objective, users and affected persons
Model dependency	Model name, provider, version and deployment type
Data	Training, tuning, retrieval and operational data categories
Interfaces	APIs, tools, agents, plugins, external actions and downstream systems
Deployment	Cloud, on-premises, edge, mobile, embedded or cyber-physical
Criticality	Safety, financial, legal, operational and reputational impact
Jurisdictions	Countries, regions and sector regimes
Suppliers	Model, data, hosting, evaluation and integration providers
Lifecycle status	Design, test, pilot, production, suspended or retired

7. Phase 2 - Define Scope and Conformance Target

7.1 Scope dimensions

- Organizational boundary: legal entities, functions, sites and shared services.

- System boundary: AI components, applications, infrastructure, interfaces and data flows.
- Lifecycle boundary: acquisition, design, training, testing, deployment, monitoring and retirement.
- Geographic boundary: jurisdictions and data-transfer locations.
- Supplier boundary: outsourced services and inherited controls.
- Assessment and public-claim boundary: what is assessed, what is excluded and what may be represented externally. Any future certification boundary would be defined only under a separately issued scheme.

7.2 Conformance target

Target	Use	Adoption implication
Foundational	Initial controlled baseline	Assess the 52 canonical controls in D1-D8. Determine and document D9 applicability wherever Physical AI or cyber-physical actuation is within scope.
Operational	Operating-effectiveness assurance	Use the same applicable control scope as Foundational and demonstrate operating-effectiveness evidence and recurring assurance.
Optimized	Continuous monitoring and enhanced assurance	Use the same applicable control scope as Operational and add continuous monitoring, enhanced assurance and improvement expectations.
Sector profile	Additional sector or jurisdiction obligations	Apply additively where an approved Sector Profile exists; sector guidance is not automatically a conformance profile.

GAISSF-NOR-001 governs exact tier definitions and D9 applicability. This implementation guide does not define or alter tier membership.

7.3 Scope statement template

Field	Illustrative entry
Organization	Example enterprise and named business unit
Systems	Named AI services and supporting platforms
Locations	Specified regions and hosting environments
Lifecycle	Development through production operation
Suppliers	Named critical providers and inherited-control boundaries
Tier / sector overlay	Foundational / Operational / Optimized, plus any approved sector overlay
Exclusions	Explicitly justified and approved
Assessment period	Evidence period and cut-off date

8. Phase 3 - Establish Governance

Role	Primary accountability
Board or risk committee	Oversight of material AI risk and assurance
Executive sponsor	Mandate, resources, escalation and residual-risk acceptance
Program steering group	Cross-functional decisions and progress control
Program lead	Plan, dependencies, traceability and reporting
Control owner	Design and accountability for control effectiveness
Control operator	Day-to-day execution and evidence generation
System owner	System risk, lifecycle and supplier decisions
Legal and compliance	Applicable obligations and legal interpretation
Internal audit / assurance	Independent challenge and testing
Assessment liaison	Assessment coordination and controlled public representations

9. Phase 4 - Conduct the Baseline Assessment

Assessment should distinguish control design, implementation, operation and effectiveness. A policy alone does not demonstrate operation.

Rating	Meaning	Typical evidence
Not applicable	Excluded only through controlled applicability rules or approved scope rationale	Applicability decision and approval

Rating	Meaning	Typical evidence
Not implemented	No adequate control design or operation	Gap record
Designed	Control is documented but not fully operating	Policy, procedure, design record
Implemented	Mechanism exists but evidence period is insufficient or inconsistent	Configuration, deployment record
Operating	Control operates consistently in the assessed scope	Logs, tickets, reviews, test outputs
Effective	Control demonstrably reduces the intended risk and passes assurance testing	Outcome metrics, independent validation

9.1 Assessment method

1. Review the exact control statement and objective.
2. Confirm applicability to the defined scope.
3. Identify required control owners and operators.
4. Inspect design documentation and implementation records.
5. Sample operating evidence across the assessment period.
6. Test technical and procedural operation where applicable.
7. Record gaps, risks, dependencies and conflicting evidence.
8. Assign corrective action and target date.

10. Phase 5 - Build the Remediation Roadmap

Priority	Criteria	Expected treatment
P0 — Immediate	Material safety, legal, security or uncontrolled production exposure	Contain, suspend or restrict operation; executive escalation
P1 — Critical	Major control absence affecting assessed conformance or material risk	Funded remediation with executive tracking
P2 — High	Significant design or operating weakness	Time-bound corrective action
P3 — Moderate	Partial implementation or evidence weakness	Planned improvement
P4 — Low	Documentation, efficiency or optimization issue	Normal improvement backlog

10.1 Roadmap fields

- Control ID and finding ID
- Risk statement and affected scope
- Root cause
- Interim containment
- Corrective action
- Accountable owner
- Resources and dependencies
- Target date
- Validation method
- Closure evidence

11. Phase 6 - Establish the Evidence Architecture

Evidence class	Examples	Quality expectation
Governance	Charters, approvals, meeting minutes, risk decisions	Signed, dated and scope-linked
Design	Policies, procedures, architectures, threat models	Controlled version and owner
Technical	Configurations, test outputs, scans, model evaluations	Reproducible and attributable
Operational	Logs, tickets, review records, monitoring outputs	Representative across the evidence period
Supplier	Contracts, attestations, due diligence, service reports	Current and linked to inherited controls
Corrective action	Finding records, fixes, validation and closure approval	Traceable from issue to verified closure

11.1 Evidence index minimum fields

Field	Description
Evidence ID	Unique identifier

Field	Description
Control ID	Mapped GAISSF control
Scope element	System, business unit, supplier or location
Owner	Evidence custodian
Period	Date range represented
Source	System or process of origin
Integrity	Hash, signature or repository control where appropriate
Status	Draft, approved, expired or superseded
Location	Controlled repository path
Limitations	Known gaps, sampling limits or assumptions

12. Phase 7 - Internal Assurance and Readiness

9. Perform a document and traceability review.
10. Re-test high-risk technical controls.
11. Verify the complete Applicable-Control Baseline.
12. Confirm evidence-period sufficiency.
13. Review open exceptions and residual-risk acceptance.
14. Validate that public claims match the assessed scope.
15. Conduct management review and readiness decision.

12.1 Readiness decision criteria

Decision	Criteria
Proceed	No unresolved major nonconformities; evidence is sufficient; scope is stable
Proceed conditionally	Limited minor issues with approved closure plan and no material misstatement risk
Defer	Evidence period, scope stability or remediation is insufficient
Stop and contain	Material uncontrolled risk or invalid public claim, including any implication of GAISSF certification where none is offered

13. Phase 8 - External Assessment and Public Claims

Organizations pursuing independent external assessment should establish a single controlled interface for assessor requests, evidence transfer, finding management and public claims. GAISSF certification is not currently offered; if a future certification scheme is issued, its additional rules would apply separately.

Preparation area	Required action
Scope	Freeze and approve the assessment boundary and public-claim boundary
Evidence	Provide indexed, current and authenticated evidence
Sampling	Identify populations and support reproducible sampling
Personnel	Make control owners and operators available
Findings	Use controlled correction and corrective-action workflow
Disputes / review	Use the assessment provider's documented review or dispute process
Claims	Approve factual wording, marks and public statements; do not imply certification

14. Phase 9 - Sustain Adoption

Operating mechanism	Minimum activity
Change monitoring	Assess system, supplier, legal and threat changes
Control monitoring	Track failures, exceptions and performance indicators
Management review	Review status, risks, resources and improvement
Internal assurance	Retest controls based on risk and change
Evidence maintenance	Refresh expired and superseded evidence
Training	Maintain role-based competence

Operating mechanism	Minimum activity
Incident learning	Feed incidents and near misses into controls
Release management	Assess GAISSF™ update or correction notices and migration impact

15. Adoption Roadmap

Time horizon	Primary activities	Deliverables
Days 0-30	Mobilize, inventory, initial scope, sponsor and charter	Program charter, inventory, draft scope
Days 31-60	Governance, tier selection and baseline assessment	RACI, Applicable-Control Baseline, gap register
Days 61-90	Prioritized remediation and evidence architecture	Roadmap, evidence index, dashboards
Months 4-6	Implement critical controls and internal assurance	Operating evidence, test results, review records
Months 7-9	Close high-priority gaps and stabilize operation	Corrective-action closure, readiness report
Months 10-12	External assessment or sustained internal conformance	Assessment package and executive public-claim decision

Time horizons are illustrative. Actual duration depends on scope, maturity, evidence availability, supplier dependencies and remediation complexity.

16. Program Metrics

Metric	Interpretation	Caution
Applicable controls with assigned owner	Ownership completeness	Does not prove operation
Controls with current operating evidence	Evidence coverage	Quality matters more than count
Open major findings	Material readiness risk	Track age and exposure
Corrective actions overdue	Execution weakness	Consider dependency causes
Exceptions nearing expiry	Residual-risk exposure	Require review before extension
Systems inventoried	Discovery completeness	Shadow AI may remain
Supplier evidence coverage	Third-party assurance	Attestations may be insufficient
Control retest pass rate	Operational stability	Avoid masking high-impact failures

17. Common Adoption Failure Modes

Failure mode	Why it fails	Corrective response
Treating GAISSF as a checklist	Ignores scope, operation and evidence	Establish control ownership and testing
Starting with certification or an external assurance deadline	Creates evidence scramble and unstable scope; GAISSF certification is not currently offered	Build operating capability and evidence first
Copying control text into policy	Produces paper conformance	Connect requirements to systems and workflows
Using maturity to offset failures	Masks unmet mandatory controls	Separate maturity from conformance
Ignoring suppliers	Leaves inherited risks unassessed	Define supplier boundaries and evidence
Over-scoping the first release	Creates unmanageable remediation	Use a defensible staged scope
Under-scoping interfaces	Excludes material dependencies	Include data flows, tools, agents and external actions
Relying on self-attestation only	Reduces assurance credibility	Use independent challenge based on risk

18. Sector and Jurisdiction Tailoring

Sector and jurisdiction requirements should be treated as additive overlays. The organization should maintain a legal and regulatory obligations register linked to GAISSF controls without claiming automatic equivalence.

- Identify applicable laws, regulators, standards and contractual obligations.
- Record which requirements are fully addressed, partially addressed or outside GAISSF scope.
- Apply approved Sector Profiles and specialist safety or quality standards where required.
- For Physical AI, use GAISSF™ Domain 9 alongside PAI-SF™ v1.0 where applicable; CSX-PAISF-004 is a controlled mapping and does not establish equivalence, evidence sufficiency or automatic conformance.

- Escalate conflicts between framework guidance and applicable law.
- Retain legal interpretation outside the control-assessment function.

19. Detailed Program Establishment Model

Workstream	Activities	Deliverables	Gate
Governance	Mandate, charter, sponsor, steering body, decision rights	Charter, RACI, reporting calendar	Sponsor approval
Scope and inventory	Discover systems, data, models, agents, suppliers and jurisdictions	Inventory, boundary, tier, Applicable-Control Baseline	Scope approval
Assessment	Assess design, implementation, operation and effectiveness	Gap register, risk ratings, evidence index	Baseline accepted
Remediation	Prioritize, fund, implement and validate actions	Roadmap, budget, closure evidence	Critical gaps closed
Assurance	Test, sample, challenge and management-review controls	Readiness report, findings, risk decisions	Proceed/defer decision
Sustainment	Operate metrics, incidents, suppliers, evidence and improvement	Operating dashboard and review records	BAU acceptance

20. Resource and Competence Planning

The adoption plan should estimate effort by system count, control applicability, supplier dependence, evidence maturity and remediation complexity. Competence plans should cover AI engineering, cybersecurity, privacy, risk, safety, assurance and relevant sector obligations.

Role family	Minimum competence
Executive and risk	AI risk, accountability, claims and residual-risk decisions
Architecture and engineering	Model, data, agent, platform and secure lifecycle controls
Operations	Monitoring, incident, change and evidence procedures
Assurance	Sampling, technical testing, nonconformity and independence
Legal/compliance	Jurisdiction, contractual and sector obligations

21. Adoption Business Case

- Baseline risk and customer/regulatory drivers
- Cost of current fragmented controls and duplicated assurance
- Expected implementation and operating cost
- Commercial, resilience and trust benefits
- Dependencies, constraints and residual uncertainty
- Decision points for staged funding

22. Stakeholder Engagement Plan

Stakeholder	Engagement need
Board/executives	Material risk, resources and assurance decisions
Product/system owners	Scope, acceptable use and control ownership
Engineering/operations	Mechanisms, evidence and monitoring
Legal/privacy/safety	Applicable obligations and constraints
Procurement/suppliers	Contract, inherited controls and notification
Users/affected persons	Disclosure, feedback, recourse and human factors

23. Sample Adoption Scenario

A mid-size enterprise beginning with an internal generative-AI assistant should first scope the assistant, model provider, retrieval data, user population and supporting cloud services. It should choose the intended conformance tier, assign owners, assess the full applicable

catalogue, contain high-risk data and tool access, build operating evidence over a representative period, and only then decide whether to pursue independent external assessment.

If the system has no Physical AI or cyber-physical actuation in scope, the Foundational baseline is the 52 D1-D8 controls. If Physical AI is introduced, D9 applicability must be determined and documented under GAISSF-NOR-001.

24. 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.

24.1 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 GAISSF certification as legal approval, permission to operate, immunity from enforcement or proof that harm cannot occur.

24.2 Legal and Regulatory Obligations Register

Field	Required content
Obligation identifier	Unique identifier and source citation.
Jurisdiction and authority	Country, state, sector and competent authority.
Applicability rationale	Why the obligation applies or does not apply.
Affected scope	Systems, business activities, locations, suppliers and populations.
Responsible owner	Authorized legal, privacy, compliance or regulatory owner.
Deadline or clock	Reporting, response, review or remediation timing.
Retention and preservation	Applicable schedule, legal hold and disposal constraints.
GAISSF relationship	Relevant controls, evidence and known non-equivalence.
Decision and uncertainty	Interpretation, unresolved issue, exception and approval.
Review trigger	Legal change, material system change, incident or periodic review.

24.3 Board and delegated-committee oversight evidence

- Record information supplied, material risks, unresolved obligations, remediation funding and decision rationale.
- Preserve minutes, dissent, management attestations and escalation of overdue high-risk matters.
- Obtain jurisdiction-specific advice on director, officer and senior-management duties; GAISSF does not define those duties or the legal standard of care.

24.4 Retention governance

Retention periods shall be derived from applicable law, contracts, limitation periods, regulator expectations, litigation holds and business requirements. Generic periods shall not be treated as universally applicable.

24.5 Adoption measures and engagement cadence

Outcome	Illustrative measure
Scope controlled	100% of in-scope systems have approved boundary, owner and jurisdiction record.
Controls owned	100% of applicable controls have accountable and operating owners.
Evidence managed	Target percentage of required evidence is current, attributable and indexed.
Remediation funded	High-risk actions have approved owners, dates and resources.
Oversight active	Material legal and control issues are reported at the approved cadence.

Illustrative engagement: monthly executive risk briefing; biweekly program steering; weekly system-owner implementation review; event-driven legal and regulatory escalation. Cadence shall be tailored to risk.

25. Limitations

- This guide does not enumerate every control requirement.
- It does not replace GAISSF-NOR-001, GAISSF-NOR-004 or the Applicable-Control Baseline.
- It does not establish universal cost, staffing or schedule benchmarks.
- It does not determine legal applicability or certify a system.
- It cannot eliminate sampling, evidence or assessor-judgement limitations.

26. Notably Absent

- No promise of a particular external-assessment outcome or future certification within a fixed period.
- No claim that adoption guarantees security, safety, compliance or market approval.
- No universal requirement to adopt the highest tier.
- No permission to exclude controls for convenience.
- No replacement for sector safety engineering, privacy, quality or cybersecurity obligations.
- No treatment of D9 as universally applicable or universally excluded; applicability follows GAISSF-NOR-001.
- No assertion that weak AI governance automatically creates personal liability or permits corporate-veil piercing.
- No universal retention period.
- No permission to select a tier solely by convenience or a desired public claim.
- No claim that GAISSF establishes fiduciary duties or a legal standard of care.

Annex A - Adoption Readiness Checklist

- ☐ Executive sponsor appointed
- ☐ Program charter approved
- ☐ AI inventory substantially complete
- ☐ Scope statement approved
- ☐ Conformance tier selected
- ☐ Applicable-Control Baseline established
- ☐ Control owners assigned
- ☐ Baseline assessment completed
- ☐ Critical risks contained
- ☐ Remediation roadmap funded
- ☐ Evidence repository operational
- ☐ Internal assurance completed
- ☐ Exceptions and residual risks approved
- ☐ External-assessment and public-claim decision documented
- ☐ Continuing-conformance process active

Annex B - Program Workplan Template

Workstream	Owner	Key outputs	Target date	Status
Governance		Charter, steering committee, reporting		
Scope and inventory		Inventory, boundary, Applicable-Control Baseline		
Control implementation		Control designs and procedures		
Technical validation		Tests, evaluations and monitoring		
Evidence management		Evidence index and repository		
Supplier assurance		Due diligence and inherited-control records		
Remediation		Corrective-action plan and closure		

Workstream	Owner	Key outputs	Target date	Status
Internal assurance		Readiness review and management approval		
External assessment / public claims		Assessment coordination and claims control		

Annex C - Executive Decision Log Template

Decision ID	Decision	Options considered	Rationale	Owner	Date	Evidence

Annex D - Source Traceability and Related Guidance

Guide section	Primary controlled source
Framework requirements	GAISSF-NOR-001
Executive interpretation	GAISSF-NOR-002
Initial implementation sequence	GAISSF-NOR-003
Control records and evidence fields	GAISSF-NOR-004
Terminology	GAISSF-NOR-005
External references	GAISSF-NOR-006
Release and supersession status	GAISSF-NOR-007
Historical decisions and corrections	GAISSF-NOR-008

Related guidance

Related guidance	Document
Operational implementation	GAISSF-IMP-010, where published and current
Evidence collection and preservation	GAISSF-IMP-017, where published and current
Physical-AI security	PAI-SF™ v1.0; CSX-PAISF-004 mapping

Annex E - Publication Record

Date	Change	Status
29 June 2026	Initial Adoption Guide issued for GAISSF™ v1.0.	Final Publication
05 October 2026	Public-publication reconciliation: removed the conflicting profile-scope notice and generic completeness self-assessment; aligned Foundational/Operational/Optimized tier and D9 applicability language to GAISSF-NOR-001; replaced Statement of Applicability with Applicable-Control Baseline; reframed certification as future-scheme only; converted Phase 8 to external assessment and public claims; integrated program-establishment, competence, business-case, stakeholder and legal/regulatory material into the body; added PAI-SF™ mapping boundary; normalized marks, licensing, dependencies and publication controls. No GAISSF™ control was added, removed, renamed or amended.	Updated

GAISSF™ is a framework of ODA3 Institute. Use of GAISSF™ materials is subject to the GAISSF Ecosystem Licence (GEL) v1.0. © 2026 ODA3 Pvt Ltd.