

ODA3 INSTITUTE

IMPLEMENTATION GUIDANCE

GAISSF™ v1.0 Implementation Handbook

Operational Architecture, Workflows, Engineering Integration and Evidence

GAISSF-IMP-010 | Public | Final Publication

Issued 29 June 2026 | Updated 05 October 2026

© 2026 ODA3 Pvt Ltd

Document Control

Attribute	Controlled value
Document ID	GAISSF-IMP-010
Title	GAISSF™ v1.0 Implementation Handbook
Purpose	Operational deployment guidance for GAISSF controls and evidence
Primary audience	Security architects, AI engineers, platform teams, DevSecOps, model risk, governance, compliance, internal assurance and independent assessors
Dependencies	GAISSF-NOR-001 through GAISSF-NOR-008; GAISSF-IMP-009, 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 handbook explains implementation patterns. It does not establish or amend GAISSF™ requirements. GAISSF-NOR-001 and GAISSF-NOR-004 remain authoritative. It does not define conformance-tier membership, legal compliance or certification eligibility. 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 decision rights, assurance, legal/regulatory integration, limitations and Notably Absent.
Program or control owner	Use workflows, control records, 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 the handbook as informative context only; test claims against authoritative normative sources and applicable assessment criteria.

Legal and Reliance Notice

© 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 handbook does not constitute legal advice, safety approval, regulatory approval, certification, accreditation or a guarantee of secure or safe operation. It does not create a legal safe harbour, establish a legal standard of care, or determine statutory compliance in any jurisdiction.

Examples are illustrative. Organizations remain responsible for architecture, system safety, privacy, risk acceptance and evidence sufficiency.

Foreword

This handbook translates the GAISSF™ control architecture into implementable operating patterns. It is designed to help practitioners connect governance requirements with system architecture, engineering workflows, control operation, telemetry, evidence and assurance.

1. Purpose, Scope and Use

The handbook covers operational architecture, lifecycle workflows, deployment gates, control ownership, evidence generation, monitoring, exception handling, supplier integration, assurance and implementation patterns for AI systems.

It may be used for greenfield programs, existing AI platforms, third-party AI services, agentic systems, embedded models and physical-AI environments. It shall not be used as a substitute for the exact control statements in GAISSF-NOR-004.

2. Implementation Model

Layer	Purpose	Primary artifacts
Governance	Accountability, policy, risk and decision rights	Charter, RACI, risk register, approvals
Control design	Translate requirements into organizational and technical mechanisms	Control designs, standards, procedures
System architecture	Place controls at trust boundaries and lifecycle stages	Reference architecture, data flows, threat model
Workflow integration	Embed control operation into engineering and business processes	SDLC gates, tickets, approvals, runbooks
Telemetry and evidence	Record control operation and outcomes	Logs, metrics, test reports, evidence index
Assurance	Test design and operating effectiveness	Assessments, samples, findings, retests
Improvement	Correct weaknesses and respond to change	Corrective actions, trend reviews, release impact

3. Reference Operating Architecture

3.1 Core architectural zones

Zone	Components	Key control concerns
User and channel	Web, mobile, API, chat, voice, operator interface	Identity, transparency, misuse prevention, human factors
Application and orchestration	Business logic, prompt chains, agents, tools, memory	Authorization, prompt control, tool permissions, state integrity
Model services	Hosted models, local models, routing, inference endpoints	Model provenance, versioning, robustness, output controls
Data and retrieval	Training data, RAG stores, vector databases, feature stores	Data lineage, poisoning resistance, privacy, retention
Tool and action plane	Plugins, APIs, robotic actions, external systems	Least privilege, transaction controls, human approval, rollback
Platform and infrastructure	Cloud, containers, endpoints, networks, secrets	Segmentation, hardening, monitoring, resilience
Assurance plane	Evaluation, red teaming, test harnesses, released VTS assets where applicable, evidence	Independence, reproducibility, integrity, traceability
Governance plane	Inventory, risk, exceptions, approvals, reporting	Accountability, risk acceptance, change control

3.2 Trust boundaries

- Human-to-AI interaction boundary
- Application-to-model boundary
- Model-to-tool or action boundary
- Internal-to-third-party service boundary
- Production-to-evaluation boundary
- Logical-to-physical actuation boundary
- Data-origin and data-consumption boundary

Each boundary should have identified assets, identities, permitted actions, failure modes, logging, monitoring and recovery mechanisms.

4. Control Implementation Record

For each applicable GAISSF control, maintain an implementation record linking the normative statement to operational mechanisms and evidence.

Field	Required implementation content
Control ID	Exact GAISSF control identifier

Field	Required implementation content
Objective	Intended risk outcome
Applicable scope	Systems, components, suppliers and locations
Control owner	Accountable function
Operators	Teams or services executing the control
Mechanisms	Policy, process, configuration and technical safeguards
Trigger	Event or schedule causing operation
Inputs	Data, approvals, configurations or telemetry
Outputs	Decision, block, log, report, test result or evidence
Dependencies	Inherited, shared or supplier controls
Failure mode	How control failure may occur
Detection	Monitoring or testing that identifies failure
Evidence	Artifact IDs and repository locations
Metrics	Coverage, timeliness, effectiveness and exceptions
Assurance method	Inspection, interview, observation, test or re-performance

5. Lifecycle Workflow

Stage	Required workflow activities	Primary evidence
Intake	Register use case, owner, purpose, affected users and initial risk	Intake record, inventory entry
Classification	Assess criticality, autonomy, data sensitivity, sector and jurisdiction	Risk classification, applicability decision
Design	Threat model, architecture, control design and supplier analysis	Architecture, threat model, control plan
Build/configure	Secure development, data controls, model configuration and logging	Code review, configs, lineage, build records
Evaluate	Security, robustness, safety, privacy and performance testing	Evaluation plan and results
Approve	Risk review, exceptions, deployment decision and sign-off	Approval record, risk acceptance
Deploy	Controlled release, rollback, monitoring and incident readiness	Release record, deployment evidence
Operate	Monitoring, review, access control, supplier oversight and user support	Logs, alerts, reviews, tickets
Change	Impact assessment, re-evaluation and approval	Change record, delta test results
Retire	Access removal, data handling, archive and decommission	Retirement checklist, disposal evidence

6. Engineering Workflow Integration

6.1 Backlog and requirements

- Create traceable security and safety requirements linked to control IDs.
- Represent control implementation tasks in the same backlog as product and platform work.
- Define acceptance criteria that include evidence generation.
- Prevent closure where evidence is absent or scope is incomplete.

6.2 CI/CD and MLOps gates

Gate	Example checks	Failure treatment
Source	Secrets, dependencies, policy-as-code, unsafe patterns	Block merge or create exception
Data	Lineage, licence, quality, privacy, poisoning indicators	Quarantine or reject dataset
Model	Provenance, signature, evaluation baseline, known limitations	Reject promotion
Application	Prompt injection, authorization, output filtering, tool controls	Block release
Infrastructure	Hardening, segmentation, identity and logging	Block deployment

Gate	Example checks	Failure treatment
Release	Approval, evidence completeness, rollback and monitoring	Defer production
Post-release	Drift, abuse, incident indicators and control-health telemetry	Alert, contain or roll back

7. Domain Implementation Patterns

Domain	Implementation focus	Typical mechanisms
D1 - Model Integrity & Adversarial Robustness	Model provenance, integrity, robustness and change control	Registry/signature verification, lineage, integrity checks, adversarial evaluation, extraction/poisoning monitoring
D2 - Runtime Security & Adversarial Defense	Runtime attack prevention, detection and containment	Prompt-injection/jailbreak defenses, runtime monitoring, segmentation, exploit detection, regression tests
D3 - Agentic Risk & Autonomous System Security	Agency, permissions, delegation, memory and multi-agent controls	Least agency, tool authorization, inter-agent controls, attestation, lifecycle and memory safeguards
D4 - Supply Chain & Third-Party AI Security	Third-party models, components, services and AI supply chain	AI-BOM, artifact scanning, registry vetting, supplier assurance, MCP/service monitoring, SCA
D5 - Content Safety & Output Integrity	Harmful-output, privacy and output-integrity controls	Content filtering, PII leakage prevention, copyright/watermark checks, privacy-by-design controls
D6 - Governance, Accountability & Human Oversight	Accountability, approvals, human oversight and governance records	HITL approvals, audit trails, model cards, incident readiness, continuity and decommissioning
D7 - Human & Societal Harms	Human-impact, manipulation, deepfake and social-engineering risks	Phishing/deepfake defenses, out-of-band authentication, recourse, societal-harm monitoring
D8 - Regulatory Alignment & Compliance	Regulatory, standards and reporting alignment	EU AI Act mapping, ISO/IEC 42001 gap tracking, GPAI documentation, DORA and NIST alignment where applicable
D9 - Physical AI Safety	Cyber-physical safety, control integrity and safe-state behavior	Hazard analysis, command authentication, override/E-stop, HIL/simulation, safe-state and event telemetry

GAISSF-NOR-004 governs the exact control requirements. These patterns are implementation guidance, not replacement control text.

8. Evidence Architecture

8.1 Evidence principles

- Evidence should be generated as a by-product of control operation.
- Evidence should be attributable to a system, control, period and responsible owner.
- Evidence integrity should be protected using repository controls, hashes, signatures or immutable logging where appropriate.
- Evidence should expose limitations, failed tests and exceptions rather than only successful outcomes.

8.2 Evidence package structure

Package element	Content
Manifest	Scope, period, control IDs, owners and artifact list
Control narrative	How the control is implemented and operated
Design evidence	Policies, architecture and configuration standards
Operating evidence	Logs, tickets, approvals and recurring records
Technical evidence	Tests, scans, evaluations and measurements
Exceptions	Approved deviations and residual risk
Findings	Known deficiencies and corrective actions
Integrity record	Hashes, signatures, timestamps or chain of custody
Limitations	Sampling, unavailable data and contextual constraints

8.3 Evidence naming convention

Recommended pattern: [SYSTEM]-[CONTROL-ID]-[EVIDENCE-TYPE]-[YYYYMMDD]-[SEQUENCE]. Example: PAYBOT-D3-CTL-04-CONFIG-20260629-001.

9. Monitoring and Control Health

Metric class	Examples	Use
Coverage	Systems covered, suppliers assessed, controls with current evidence	Detect scope gaps
Operation	Execution frequency, gate pass/fail, review completion	Confirm control operation
Effectiveness	Attack success rate, containment time, leakage rate, override success	Assess risk reduction
Exceptions	Open, expired and repeated exceptions	Track residual risk
Quality	False positive/negative rates, evidence defects, test reproducibility	Improve assurance quality
Change	Model, data, supplier and architecture changes	Trigger reassessment
Incident	Near misses, harmful outputs, misuse, safety events	Drive corrective action

10. Exception and Risk Acceptance Workflow

Step	Action	Required output
1	Identify unmet requirement or control deviation	Exception request
2	Define affected scope and duration	Scope statement
3	Assess risk and compensating controls	Risk analysis
4	Obtain control owner and risk owner review	Review record
5	Approve, reject or require containment	Decision
6	Record expiry and remediation plan	Tracked action
7	Monitor compensating controls	Evidence
8	Close, renew or escalate before expiry	Closure or new decision

11. Supplier and Third-Party Integration

- Map inherited controls and identify where the supplier provides only partial evidence.
- Require contractual notification for material model, data, security or service changes.
- Define incident reporting, audit access, data use, retention and subcontractor requirements.
- Do not treat third-party certifications or attestations as complete substitutes for system-specific evidence.
- Maintain exit, portability and service-continuity plans for critical dependencies.

12. Agentic AI Implementation Pattern

Control point	Implementation pattern
Goal and plan	Constrain objectives, plan depth and termination conditions
Tool access	Per-tool authorization, least privilege and allowlists
Memory	Scope, retention, poisoning controls and user separation
Transactions	Human approval or policy gate for consequential actions
Delegation	Identity, limits and traceability for sub-agents
Observation	Record prompts, plans, tool calls, outputs and decisions
Containment	Rate limits, circuit breakers, kill switch and rollback
Evaluation	Scenario tests for manipulation, escalation and unsafe autonomy

13. Physical AI Implementation Pattern

Area	Implementation expectation
Hazard analysis	Identify physical, environmental and human hazards
Safety constraints	Enforce operational envelopes and actuation limits
Human override	Provide reliable, tested and accessible override
Safe state	Define and test fallback behavior

Area	Implementation expectation
Sensing integrity	Validate sensor provenance, calibration and fault handling
Simulation/HIL	Use validated or otherwise appropriately qualified simulation or hardware-in-the-loop where appropriate
Cyber-physical security	Segment control networks and authenticate commands
Incident evidence	Capture telemetry sufficient to reconstruct events

Where Physical AI is in scope, GAISSF™ Domain 9 should be used alongside PAI-SF™ v1.0 as applicable. CSX-PAISF-004 provides controlled mapping; correspondence does not establish equivalence, evidence sufficiency or automatic conformance.

14. Internal Assurance Workflow

Method	Use
Inspection	Review policies, designs, configurations and evidence
Interview	Confirm ownership, competence and actual practice
Observation	Watch control execution or operational workflow
Sampling	Select representative systems, events, users and periods
Re-performance	Repeat tests or control actions
Technical testing	Execute security, robustness, privacy or safety tests
Traceability review	Follow requirement to mechanism to evidence to outcome

15. Implementation Anti-Patterns

Anti-pattern	Risk	Corrective action
Policy-only implementation	No proof of technical or operational control	Add mechanisms and operating evidence
Central dashboard without source integrity	Metrics may be misleading	Validate data lineage and completeness
One-time red team	Rapidly becomes stale	Use change-triggered and periodic testing
Universal model approval	Ignores use-case context	Approve system-and-context combinations
Supplier attestation reliance	Hides inherited gaps	Request system-specific evidence
Logging without review	Creates data, not control operation	Assign alerting and review ownership
Exception without expiry	Normalizes nonconformance	Time-bound and monitor exceptions
Silent failed tests	Overstates assurance	Retain failed and inconclusive results

16. Deployment Readiness Checklist

- ☐ Scope and inventory approved
- ☐ Threat model current
- ☐ Control implementation record complete
- ☐ Applicable requirements traced
- ☐ Critical tests passed
- ☐ Open failures risk-assessed
- ☐ Evidence package complete
- ☐ Monitoring and alerting active
- ☐ Incident runbook tested
- ☐ Rollback and safe-state mechanisms validated
- ☐ Supplier dependencies reviewed
- ☐ Exceptions approved and time-bound
- ☐ Management approval recorded

17. Operating Cadence

Cadence	Activities
Continuous	Security telemetry, control-health monitoring, abuse and safety alerts
Per change	Impact assessment, regression testing, evidence refresh
Monthly	Exception review, overdue findings, supplier changes, metric trends
Quarterly	Control-owner attestation, technical reassessment, management reporting
Semiannual	Cross-functional assurance and scenario exercises
Annual	Full applicable-tier review, scope confirmation, internal audit and GAISSF™ update/correction impact review

18. Control-by-Control Operationalization Method

Design step	Practitioner action
Purpose and risk outcome	State the adverse condition the control is intended to prevent, detect, contain or recover from.
Scope and applicability	Identify systems, models, data, users, agents, suppliers, environments and lifecycle stages.
Control design	Document preventive, detective, corrective and compensating mechanisms.
Operating procedure	Define trigger, inputs, sequence, decisions, outputs, responsible operator and escalation.
Evidence	Specify design, implementation, operating and effectiveness artifacts.
Monitoring	Define health signals, thresholds, alert ownership and review frequency.
Assurance	Define inspection, sampling, technical test, re-performance and independence expectations.
Failure response	Define containment, exception, incident, corrective action and retest.

19. Detailed Workflow Library

Workflow	Trigger	Core steps	Evidence
AI intake	New use case or material change	Register, classify, scope, assess, approve	Intake, risk and approval record
Model onboarding	New or changed model	Provenance, licence, security, safety, evaluation, release	Model card, tests, signed release
Data onboarding	New data source	Purpose, rights, lineage, quality, privacy, poisoning checks	Data record and validation
Agent/tool approval	New capability	Identity, permissions, transactions, sandbox, rollback	Tool profile and approval
Exception	Unmet control	Assess, compensate, approve, monitor, expire	Exception record
Incident	Alert or harmful event	Triage, contain, preserve, investigate, recover, improve	Incident and corrective-action evidence

20. Engineering Requirements Specification

Each system should maintain a traceable set of security, safety, privacy and governance requirements derived from applicable GAISSF controls. Requirements should include acceptance criteria, verification method, evidence artifact and responsible owner.

Requirement field	Example
Requirement ID	SYS-SEC-042
GAISSF control	Applicable D-domain control ID
Statement	System shall block unapproved tool calls.
Acceptance criterion	100% of denied test cases blocked and logged.
Verification	Automated test plus manual review.
Evidence	Signed test report and gateway logs.

21. Evidence Engineering

- Generate evidence automatically where feasible but preserve human decisions and limitations.
- Separate source telemetry from interpreted dashboard values.
- Protect evidence write paths and record provenance.
- Retain failed and inconclusive tests.
- Define evidence freshness and expiry.
- Test evidence export before external assessment.

22. Operational Handoffs

Handoff	Required package
Engineering to operations	Approved release, runbooks, monitoring, rollback, known limitations
Operations to incident response	Alert definitions, escalation, evidence sources, containment actions
Control owner to assurance	Implementation narrative, population, evidence index, known gaps
Supplier manager to system owner	Assurance, changes, incidents, dependencies and exit plan

23. Detailed D1-D9 Implementation Checklist

Domain	Design questions	Operating evidence
D1 - Model Integrity & Adversarial Robustness	Are model provenance, integrity, adversarial robustness and change controls operating?	Registry/signature checks, lineage, poisoning/robustness evaluations, extraction monitoring
D2 - Runtime Security & Adversarial Defense	Are runtime attacks, prompt/tool abuse and exploit paths tested and monitored?	Runtime attack telemetry, red-team results, segmentation evidence, regression tests
D3 - Agentic Risk & Autonomous System Security	Are agents, permissions, delegation, memory and multi-agent interactions controlled?	Agent inventories, permissions, tool logs, attestation, memory/lifecycle evidence
D4 - Supply Chain & Third-Party AI Security	Are models, artifacts, registries, suppliers and third-party services controlled?	AI-BOM, artifact scans, supplier evidence, registry/MCP monitoring, SCA results
D5 - Content Safety & Output Integrity	Are harmful-output, privacy, leakage and output-integrity risks controlled?	Content tests, DLP/privacy evidence, watermark/copyright checks, complaints/recourse records
D6 - Governance, Accountability & Human Oversight	Are accountability, approvals, human oversight and governance records operational?	Minutes, approvals, audit trails, model cards, incident/decommissioning records
D7 - Human & Societal Harms	Are manipulation, deepfake, social-engineering and societal harms addressed?	Human-impact reviews, phishing/deepfake tests, recourse and incident evidence
D8 - Regulatory Alignment & Compliance	Are applicable regulatory and standards obligations mapped, maintained and evidenced?	EU AI Act/ISO 42001/GPAI/DORA/NIST records where applicable
D9 - Physical AI Safety	Are physical hazards, actuation limits, override, safe state and cyber-physical integrity independently assured?	Hazard analysis, HIL/simulation, command-authentication, override/safe-state and event telemetry

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 Automated-decision rights and explanation support workflow

1. Authenticate the requester and determine the applicable jurisdiction, legal basis and response deadline.
2. Locate the decision, system, model, data, policy and rule versions.
3. Preserve the decision record and relevant evidence.
4. Retrieve material inputs, factors, sources, rules, human interventions and downstream effects.
5. Generate a context-appropriate explanation or reason-code artifact without misrepresenting model internals.
6. Apply lawful redaction and protection for third-party, privileged, security-sensitive and trade-secret material.
7. Support correction, contestation or human review where required.
8. Record the response, legal basis, limitations, approvals and closure.

24.3 Audit-trail capability requirements

Capability	Minimum expectation
Time integrity	Authoritative time source, drift monitoring and recorded timezone.
Attribution	Actor, service, model, tool and transaction identity.
Tamper evidence	Integrity controls proportionate to risk, including hashing or signing where appropriate.
Version linkage	Model, prompt, policy, data, code and configuration versions.
Reviewability	Searchable export, preserved context and documented telemetry gaps.
Preservation	Retention enforcement, legal-hold override and chain of custody.
Access control	Least privilege, separation of duties and access logging.

24.4 Agentic legal-policy gates

Before consequential tool execution, architectures should support configurable deny, allow, require-human-approval, restrict-data, substitute-route, log-and-escalate and safe-state outcomes for applicable sanctions, export-control, geographic, licensing, court-order, transaction-limit and regulated-product constraints.

24.5 Implementation Toolchain Capability Model

Service	Minimum capabilities
Evidence repository	Access control, metadata, integrity verification, retention, legal hold and export.
CI/CD and MLOps gate	Artifact identity, policy checks, test evidence, approvals and rollback linkage.
Decision record service	Transaction correlation, version linkage, explanation artifact and human-review record.
Policy decision point	Auditable legal, security and business constraints with reviewable outcomes
Monitoring platform	Regional routing, alerting, evidence preservation and control-health reporting.

25. Limitations

- This handbook does not provide the exact implementation for every technology stack.
- Examples do not establish assessment evidence sufficiency or any future certification evidence sufficiency.
- System-specific safety, legal and sector engineering remain necessary.
- Monitoring metrics may not be comparable across systems without normalization.
- Control operation cannot eliminate unknown threats or model uncertainty.

26. Notably Absent

- No assumption that a tool purchase constitutes control implementation.
- No guarantee that automated testing establishes conformance.
- No universal architecture mandated for all AI systems.
- No substitution for independent safety engineering in physical AI.
- No permission to omit failed, negative or inconclusive evidence.
- No claim that every control can be fully automated.
- No universal right-to-explanation claim.
- No representation that an audit trail is legally sufficient in every proceeding.

- No universal requirement for sanctions or export screening where those regimes do not apply.
- No endorsement of named vendors or tools.

Annex A - Control Implementation Record Template

Field	Entry
Control ID	
System/scope	
Owner	
Objective	
Mechanisms	
Workflow trigger	
Inputs	
Outputs	
Dependencies	
Failure modes	
Monitoring	
Evidence IDs	
Metrics	
Exceptions	
Assurance result	

Annex B - Evidence Index Template

Evidence ID	Control ID	System	Type	Period	Owner	Integrity	Location	Status

Annex C - Workflow-to-Control Traceability Template

Workflow stage	Activity	Control IDs	System owner	Evidence	Failure treatment

Annex D - Source Traceability and Related Guidance

Handbook subject	Controlled source
Normative requirements	GAISSF-NOR-001
Control records	GAISSF-NOR-004
Terminology	GAISSF-NOR-005
References	GAISSF-NOR-006
Release status	GAISSF-NOR-007
Historical decisions	GAISSF-NOR-008
Adoption program	GAISSF-IMP-009, where published and current

Related guidance	Document
Deployment gates	GAISSF-IMP-011, where published and current
Architecture patterns	GAISSF-IMP-013, where published and current
Evidence collection	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 Implementation Handbook issued for GAISSF™ v1.0.	Final Publication
05 October 2026	Public-publication reconciliation: corrected D1-D9 taxonomy; removed the conflicting profile-scope notice and generic completeness self-assessment; integrated control-operationalization, workflow, requirements, evidence-engineering, handoff, detailed-domain and legal/regulatory material into the body; bounded VTS to released assets; aligned certification/current-state language, PAI-SF mapping, marks, GEL, dependencies and publication controls. No GAISSF™ control was added, removed, renamed or amended.	Updated