

ODA3 INSTITUTE

IMPLEMENTATION GUIDANCE

GAISSF™ v1.0 Evidence Collection Guide

Artifacts, collection methods, integrity, sampling and assessor readiness

GAISSF-IMP-017 | Public

© ODA3 Pvt Ltd

Document Control

Document ID	GAISSF-IMP-017
Title	GAISSF™ v1.0 Evidence Collection Guide
Doc Type	Implementation guidance — informative
Purpose	A method for identifying, collecting, protecting, evaluating and presenting evidence of GAISSF™ control implementation and operation
Primary Audience	Control owners and operators, AI engineering, MLOps, DevSecOps, governance, compliance, internal audit, evidence custodians and assessors
Dependencies	GAISSF-NOR-001 to GAISSF-NOR-008; GAISSF-IMP-009 to GAISSF-IMP-016, where published and current
Precedence	GAISSF-NOR-001 (Framework Standard) and GAISSF-NOR-004 (Control Catalogue) prevail
Control Baseline	59 controls across nine domains
Status	Final Publication
Publish Date / Review Cycle	Issued 29 June 2026; updated 05 October 2026; review on material change to GAISSF-NOR-001 or GAISSF-NOR-004
Contact	contact@oda3.org
Classification	Public

GAISSF™ v1.0 Evidence Collection Guide

Artifacts, collection methods, integrity, sampling and assessor readiness

Reliance notice: This guide explains how to gather and maintain reliable GAISSF™ evidence. It does not replace the evidence expectations in the normative control records (GAISSF-NOR-004) or the judgement of competent assessors, and it does not create a second control catalogue. Evidence sufficiency depends on scope, risk, profile, control design, operating period and assessor judgement; no artifact type is automatically sufficient. This guide is not legal, regulatory, safety, engineering, certification or audit advice. Certification is not currently offered.

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.

Reader	Recommended use
Legal, privacy or compliance team	Validate jurisdiction-specific obligations, deadlines, retention, disclosure, privilege and regulator-facing requirements.
Independent assessor or reviewer	Use the document as informative context only; test claims against the authoritative normative sources and applicable assessment criteria.

1. Purpose and Scope

This guide defines the evidence lifecycle for GAISSF adoption, assessment, external-assessment readiness and continuing conformance. It covers evidence planning, ownership, collection, metadata, integrity, sampling, automation, chain of custody, privacy, retention, review, export and retirement.

It applies to governance evidence, technical evidence, operating records, supplier evidence, model and data records, security and safety testing, agentic-AI telemetry, physical-AI evidence and management-review artifacts.

2. Evidence Principles

Principle	Operational meaning
Evidence supports a claim	Every artifact should support a specific control, scope, period and assertion.
Operation is stronger than intention	Policies and designs are necessary but rarely sufficient without proof of implementation and recurring operation.
Scope must be explicit	Evidence should identify the system, component, population, supplier, environment and period represented.
Integrity matters	Artifacts should be protected from alteration and attributable to their source.
Failures are evidence	Failed, negative and inconclusive results must be retained and explained.
Provenance must be preserved	The origin, collection method, transformations and custody of evidence should be known.
Evidence should be proportionate	High-risk and high-autonomy systems require stronger, more direct and more frequent evidence.
Privacy and minimization still apply	Evidence collection should not create unnecessary personal, confidential or regulated data exposure.
Reproducibility improves assurance	Technical results should be repeatable where the system permits.

3. Evidence Lifecycle

Stage	Key activities	Output
Plan	Identify control claims, artifact types, owners, periods and collection methods	Evidence plan
Generate	Operate the control or execute the test	Raw source artifacts

Stage	Key activities	Output
Collect	Acquire artifacts using approved methods	Collected evidence
Normalize	Apply naming, metadata, format and redaction rules	Controlled evidence record
Validate	Check scope, completeness, integrity, currency and consistency	Accepted or rejected evidence
Index	Link to control, system, period, owner and repository	Evidence index
Protect	Apply access, integrity, retention and backup controls	Protected repository
Use	Support assessment, review or decision	Evidence package
Refresh	Replace expired, stale or superseded artifacts	Current evidence set
Retire	Archive or dispose according to obligations	Retirement record

4. Evidence Roles and Responsibilities

Role	Responsibility
Control owner	Defines the claim, approves evidence expectations and accepts gaps
Control operator	Performs recurring activities and generates operating evidence
Evidence custodian	Collects, indexes, protects and maintains artifacts
System owner	Confirms system scope, versions and operational context
Data/model owner	Provides lineage, configuration and evaluation records
Supplier manager	Obtains inherited-control and third-party evidence
Internal assurance	Challenges evidence sufficiency and performs independent tests
Privacy/legal	Reviews collection, retention, disclosure and redaction constraints
Assessment liaison	Coordinates evidence packages, assessor access and public claims
Repository administrator	Maintains access, integrity, backup and audit trails

5. Evidence Classification

Class	Examples	Typical strength
Governance	Charters, approvals, RACI, minutes, risk decisions	Strong for accountability and decision rights
Design	Policies, standards, procedures, architecture, threat models	Shows intended control design
Implementation	Configurations, code, release records, deployment manifests	Shows mechanism exists in scope

Class	Examples	Typical strength
Operating	Logs, tickets, reviews, approvals, recurring tests	Shows control operated during a period
Outcome	Risk reduction, attack prevention, incident containment, safety performance	Shows effectiveness
Assurance	Internal audit, independent testing or external review	Provides challenge and validation
Supplier	Contracts, attestations, audit reports, service records	Supports inherited-control claims
Incident/change	Incident timelines, corrective actions, change and rollback records	Shows response and improvement

6. Evidence Sufficiency Model

Dimension	Questions
Relevance	Does the artifact support the exact control claim?
Scope	Does it cover the assessed systems, users, suppliers, regions and period?
Authenticity	Can the source and creator be verified?
Integrity	Is unauthorized alteration detectable or prevented?
Currency	Does it reflect the current approved implementation?
Completeness	Are failures, exceptions and missing populations visible?
Consistency	Does it agree with other records and the approved baseline?
Reproducibility	Can the result be repeated or independently checked?
Independence	Is appropriate challenge or separation present?
Limitations	Are sampling, opacity and uncertainty recorded?

7. Evidence Planning

An evidence plan should be created before implementation or assessment, not assembled at the last moment.

Planning field	Required content
Control ID	Exact GAISSF control identifier
Claim	What implementation or operating outcome must be demonstrated
Scope	System, component, supplier, environment and population
Artifact types	Preferred and supporting evidence
Source	System, repository, person or supplier
Owner	Responsible generator and custodian
Frequency	Continuous, event-driven, daily, monthly, quarterly or annual

Planning field	Required content
Evidence period	Start and end dates
Collection method	Automated export, API, query, observation, interview or manual record
Integrity method	Hash, signature, immutable storage, repository audit or custody record
Retention	Required retention period and disposal method
Limitations	Known gaps or constraints

8. Collection Methods

Method	Best use	Control considerations
Automated API/export	Logs, configurations, inventory, metrics and tickets	Authenticate source; record query, time and filters
Direct repository capture	Policies, architecture, approvals and versioned documents	Preserve version history and metadata
Database/query extraction	Populations, access, events and control execution	Save query logic and row counts
System observation	Human oversight, physical controls and workflow execution	Record observer, time, conditions and deviations
Interview	Roles, process understanding and control operation	Corroborate with direct evidence
Re-performance	Testing technical or procedural control operation	Use controlled steps and expected outcomes
Screenshot/photo	Visual configuration or physical state	Include context, timestamp and source; avoid using alone
Supplier request	External attestations, reports and service evidence	Record scope, version, period and limitations
Sampling	Large transaction or event populations	Define population, method, sample size and exceptions

9. Evidence Metadata and Naming

Recommended naming pattern: [SYSTEM]-[CONTROL-ID]-[ARTIFACT-TYPE]-[PERIOD/DATE]-[SEQUENCE]-[VERSION].

Metadata field	Description
Evidence ID	Unique stable identifier
Control ID	Mapped GAISSF control
System/scope	System, component, supplier or location
Artifact type	Policy, configuration, log, test, review, incident or other
Source	Originating system or person
Collector	Person or service that collected it

Metadata field	Description
Collection time	Date, time and timezone
Evidence period	Period represented
Version	Model, policy, code, data or document version
Integrity value	Hash, signature or repository identifier
Classification	Public, internal, confidential, restricted or regulated
Status	Draft, accepted, rejected, expired, superseded or archived
Limitations	Sampling, opacity, missing fields or known defects

10. Integrity and Chain of Custody

Control	Implementation
Source authentication	Use authenticated APIs, signed exports or trusted repository access
Hashing	Calculate and record a cryptographic hash for collected files where proportionate
Timestamping	Use synchronized systems and record timezone
Read-only preservation	Store original artifacts without editing
Transformation log	Record redaction, format conversion, filtering and aggregation
Access control	Restrict modification and export rights
Audit trail	Retain evidence of upload, access, change and deletion
Custody transfer	Record sender, recipient, date, purpose and integrity verification
Backup	Protect against loss while preserving confidentiality and retention rules

11. Sampling

Sampling is appropriate where populations are too large for complete inspection, but the sampling method must support the control claim.

Sampling element	Required record
Population	Complete defined set from which the sample is drawn
Period	Time window represented
Method	Random, stratified, risk-based, judgemental or systematic
Sample size	Number selected and rationale
Strata	Risk, region, user type, model, supplier or severity groups
Selection logic	Query, random seed or documented judgement
Exceptions	Failures and deviations found
Projection limits	What cannot be inferred from the sample
Follow-up	Expansion or targeted testing triggered by findings

12. Automation and Continuous Evidence

Capability	Implementation guidance
Evidence-as-code	Generate control evidence from infrastructure, policy and configuration pipelines
Continuous control monitoring	Collect signals showing control health and exceptions
Automated manifests	Package model, code, data, prompt and policy versions with releases
API evidence collection	Use scheduled authenticated extraction with logged queries
Immutable event streams	Protect critical security, agentic and safety telemetry
Evidence quality checks	Detect missing fields, stale records, failed jobs and scope gaps
Human review	Retain oversight for interpretation, conflicts and high-impact decisions

13. Privacy, Confidentiality and Redaction

1. Collect only the personal and confidential data necessary to support the control claim.
2. Classify evidence before storage and sharing.
3. Use redaction, tokenization or minimization where raw content is not required.
4. Preserve an unaltered controlled original where lawful and necessary.
5. Document every transformation applied to an assessor copy.
6. Restrict cross-border transfer and third-party disclosure according to applicable obligations.
7. Do not redact information that is necessary to understand a material failure without recording the limitation.

14. Domain Evidence Patterns

14.1 D1 — Model Integrity & Adversarial Robustness

Element	Guidance
Purpose	Demonstrate provenance, integrity, versioning, resilience and controlled modification.
Preferred artifacts	Model registry; dataset lineage; signatures/hashes; training manifests; poisoning tests; adapter and merge records.
Collection method	Export from registries and pipelines; capture signed manifests; preserve test harness and raw results.
Quality checks	Versions align with production; lineage is complete; failed checks retained; source authenticity verified.
Common pitfalls	Screenshots without registry data; missing training-data lineage; silent provider or model changes.

14.2 D2 — Runtime Security & Adversarial Defense

Element	Guidance
Purpose	Demonstrate that prompt injection, jailbreak, multimodal and tool-call attacks are tested and managed.
Preferred artifacts	Threat model; red-team plan; attack corpus; test outputs; mitigations; retest records; monitoring alerts.
Collection method	Run controlled adversarial tests against pinned versions; preserve prompts, parameters, results and environment.
Quality checks	Tests are representative; repeatability is understood; successful attacks are not omitted.
Common pitfalls	Only reporting pass rate; changing model or policy between tests; no evidence of failed scenarios.

14.3 D3 — Agentic Risk & Autonomous System Security

Element	Guidance
Purpose	Demonstrate bounded authority, secure delegation, memory controls and containment.
Preferred artifacts	Agent identity records; tool allowlists; approval logs; delegation chains; memory policies; kill-switch tests.
Collection method	Collect plans, tool calls, approvals, state transitions and containment exercises.
Quality checks	Actions are attributable; permissions match approved objectives; replay and bypass tests are included.
Common pitfalls	Shared credentials; missing parent-child identity; logging outputs but not tool actions or approvals.

14.4 D4 — Supply Chain & Third-Party AI Security

Element	Guidance
Purpose	Demonstrate inventory, due diligence, artifact scanning and ongoing supplier control.
Preferred artifacts	AI BOM; supplier assessments; contracts; registry records; scan reports; change notifications; exit plans.
Collection method	Collect from procurement, registries, CI/CD, supplier portals and contract systems.
Quality checks	Scope, edition, period and inherited-control limitations are explicit.
Common pitfalls	Treating a generic certificate as complete evidence; stale supplier records; missing subprocessor visibility.

14.5 D5 — Content Safety & Output Integrity

Element	Guidance
Purpose	Demonstrate harmful-output controls, leakage prevention, copyright and privacy safeguards.

Element	Guidance
Preferred artifacts	Safety evaluations; DLP events; privacy assessments; retention records; leakage tests; user-rights records.
Collection method	Sample representative outputs and events; execute privacy and leakage tests; retain false positives/negatives.
Quality checks	Sensitive content is minimized; populations and thresholds are documented.
Common pitfalls	Using only policy documents; over-redacting failures; no evidence of user or data-subject handling.

14.6 D6 — Governance, Accountability & Human Oversight

Element	Guidance
Purpose	Demonstrate accountability, auditability, incident readiness, lifecycle governance and resilience.
Preferred artifacts	Charters; RACI; minutes; model cards; incident exercises; decommission records; management reviews.
Collection method	Collect from governance, GRC, service management and records repositories.
Quality checks	Decisions, owners and dates are clear; meeting evidence shows action, not attendance only.
Common pitfalls	Unsigned minutes; outdated model cards; no linkage from decisions to actions or controls.

14.7 D7 — Human & Societal Harms

Element	Guidance
Purpose	Demonstrate training, authentication, social-engineering defenses and user-impact controls.
Preferred artifacts	Simulation results; training completion; authentication tests; deepfake exercises; social-engineering incidents.
Collection method	Extract training populations and outcomes; observe exercises; review incident and user-recourse records.
Quality checks	Population coverage and effectiveness are measured; vulnerable groups are considered.
Common pitfalls	Attendance-only evidence; no effectiveness test; missing records for contractors or external users.

14.8 D8 — Regulatory Alignment & Compliance

Element	Guidance
Purpose	Demonstrate structured mapping to applicable obligations and standards.
Preferred artifacts	Legal register; gap assessments; regulatory mappings; reporting procedures; compliance reviews.
Collection method	Collect controlled legal interpretations, crosswalks, approvals and reporting evidence.
Quality checks	Jurisdiction, edition and applicability are current; mapping limitations are explicit.

Element	Guidance
Common pitfalls	Claiming legal compliance from a crosswalk alone; citing obsolete sources; no legal owner.

14.9 D9 — Physical AI Safety

Element	Guidance
Purpose	Demonstrate safe-state behavior, override, command integrity and incident reconstruction.
Preferred artifacts	Hazard analysis; simulation/HIL results; override tests; safety-supervisor logs; sensor calibration; incident telemetry.
Collection method	Observe physical tests; collect synchronized commands, sensor states and safety events; preserve test conditions.
Quality checks	Tests reflect realistic operating envelopes; independent safety paths are verified.
Common pitfalls	Relying only on software screenshots; incomplete timing data; no evidence of emergency-stop independence.

15. Evidence by Artifact Type

15.1 Policy and standard

Element	Guidance
Purpose	Show approved intent and mandatory rules
Preferred artifacts	Controlled document, owner, approval, version, review date
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Approved and current; linked to control
Common pitfalls	Draft or unsigned document presented as operating evidence

15.2 Procedure and runbook

Element	Guidance
Purpose	Show repeatable operating method
Preferred artifacts	Steps, triggers, roles, inputs, outputs, escalation
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Matches actual practice and systems
Common pitfalls	Procedure not used or not updated after change

15.3 Architecture and data flow

Element	Guidance
Purpose	Show control placement and boundaries

Element	Guidance
Preferred artifacts	Current diagram, components, flows, trust zones, owner
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Matches production and inventory
Common pitfalls	High-level diagram omits suppliers or tools

15.4 Configuration export

Element	Guidance
Purpose	Show technical implementation
Preferred artifacts	Authenticated export, version, source, timestamp
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Direct from system; complete relevant fields
Common pitfalls	Manual transcription or cropped screenshot

15.5 Log or event record

Element	Guidance
Purpose	Show control operation
Preferred artifacts	Timestamp, actor, action, result, correlation ID
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Complete period and synchronized time
Common pitfalls	Missing failures or filtered without record

15.6 Test report

Element	Guidance
Purpose	Show validation and effectiveness
Preferred artifacts	Scope, version, method, dataset, results, limitations
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Reproducible and includes failed cases
Common pitfalls	Only executive summary or pass/fail

15.7 Approval record

Element	Guidance
Purpose	Show authorized decision
Preferred artifacts	Decision, scope, approver, date, conditions
Collection method	Collect from the authoritative source and preserve original metadata.

Element	Guidance
Quality checks	Authority and conditions are valid
Common pitfalls	Email fragment without context or approval authority

15.8 Ticket/work item

Element	Guidance
Purpose	Show workflow and remediation
Preferred artifacts	Issue, owner, status, dates, closure evidence
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Complete lifecycle and linked artifacts
Common pitfalls	Closed without validation

15.9 Metric/dashboard

Element	Guidance
Purpose	Show trends and control health
Preferred artifacts	Definition, source, calculation, threshold, period
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Data lineage and exceptions are visible
Common pitfalls	Screenshot without metric definition

15.10 Interview/observation

Element	Guidance
Purpose	Corroborate practice and competence
Preferred artifacts	Participants, questions, observations, time, evidence links
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Supported by direct artifacts
Common pitfalls	Used as sole evidence for technical control

15.11 Supplier evidence

Element	Guidance
Purpose	Support inherited control claim
Preferred artifacts	Provider, scope, period, service, limitations
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Current and applicable to assessed service
Common pitfalls	Generic corporate report unrelated to product

15.12 Physical test record

Element	Guidance
Purpose	Show real-world safety operation
Preferred artifacts	Setup, environment, instrumentation, sequence, result
Collection method	Collect from the authoritative source and preserve original metadata.
Quality checks	Conditions and telemetry are complete
Common pitfalls	No repeatability or missing calibration

16. Evidence Review and Acceptance

Decision	Criteria	Treatment
Accepted	Relevant, current, scope-aligned, authentic, complete and protected	Index and use
Accepted with limitation	Useful but constrained by sampling, opacity or minor gap	Record limitation and supplemental action
Conditionally accepted	Temporary evidence pending stronger artifact or period	Time-bound follow-up
Rejected	Stale, unverifiable, out of scope, altered or insufficient	Replace or regenerate
Escalated	Conflict, possible manipulation or material missing evidence	Independent review or incident process

17. Evidence Conflicts and Gaps

1. Do not choose the artifact that supports the desired conclusion.
2. Reconcile scope, timestamps, versions, definitions and source systems.
3. Preserve conflicting evidence and record the resolution rationale.
4. If the conflict cannot be resolved, state uncertainty and treat the control as not fully evidenced.
5. Material gaps should create findings, exceptions or corrective actions rather than silent assumptions.

18. Assessor Readiness

Readiness element	Expected condition
Evidence index	Complete, current and linked to every applicable control
Repository access	Controlled assessor access with confidentiality protections
Evidence package	Manifest, scope, period, versions and limitations included
Populations	Underlying populations available for assessor sampling
Owners	Control owners and operators available for interview
Re-performance	Critical tests can be reproduced or observed

Readiness element	Expected condition
Exceptions	Open deviations, expiry and residual risk are transparent
Failed evidence	Negative and inconclusive results are retained
Change history	Material changes and evidence refresh are traceable

19. Evidence Retention and Disposal

Decision factor	Consideration
Legal/regulatory	Mandatory retention, reporting, litigation hold and deletion rights
External assessment	Assessment cycles and any future certification surveillance (certification is not currently offered)
Incident	Investigation, root cause, liability and lessons learned
Operational	Trend analysis, baselines and regression
Privacy	Minimization, purpose limitation and storage limitation
Supplier	Contractual access and post-termination availability
Physical safety	Longer retention may be needed for hazard and incident records

20. Evidence Quality Metrics

Metric	Purpose	Caution
Controls with accepted evidence	Measure coverage	Does not prove effectiveness
Expired evidence	Detect maintenance gaps	Different artifact classes have different lifecycles
Rejected evidence rate	Detect systemic quality issues	High scrutiny can increase rejection
Automated collection success	Monitor pipeline reliability	Automation can collect incorrect data
Evidence conflict rate	Detect inconsistent systems or definitions	Some conflict is healthy disclosure
Time to fulfill assessor request	Measure readiness and retrieval	Speed should not override privacy or accuracy
Failed tests retained	Measure assurance integrity	Count alone does not show severity

21. Common Evidence Anti-Patterns

Anti-pattern	Why it fails	Corrective practice
Screenshot-only evidence	Weak provenance and limited context	Use direct exports with metadata
Policy equals implementation	Shows intention, not operation	Add configuration and operating records

Anti-pattern	Why it fails	Corrective practice
Cherry-picked success	Misrepresents effectiveness	Retain full population or sampling rationale and failures
Evidence collected only before audit	Does not represent normal operation	Generate continuously through workflows
Uncontrolled shared folder	Weak integrity and access control	Use managed repository and audit trail
Generic supplier certificate	May not cover service, scope or period	Request specific inherited-control evidence
Unrecorded redaction	Breaks provenance and may hide material facts	Preserve original and transformation log
Metric without definition	Cannot be interpreted or reproduced	Record formula, source, threshold and scope

22. 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.

- 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.

22.1 Legal preservation integration

Field	Required content
Trigger and authority	Why preservation applies and who authorized it.
Scope	Custodians, systems, repositories, dates and evidence types.
Hold identifier	Link to the controlled legal-hold or preservation record.
Collection method	Tool, operator, timestamp and transformation.
Chain of custody	Transfer, access, integrity and storage records.
Protection	Privilege, confidentiality, personal data and security markings.
Release	Authorized end date and resumed-disposal decision.

Evidence collection does not by itself create a universal duty to preserve. Preservation obligations depend on applicable law, anticipated proceedings, regulatory instructions, contracts and other facts.

22.2 Regulatory Examination Readiness workflow

1. Identify the authority, legal basis, request scope and deadline.
2. Assign evidence, legal, privacy and technical owners.
3. Map the request to statutory requirements and GAISSF evidence without implying equivalence.
4. Verify completeness, provenance, integrity and known gaps.
5. Apply documented redaction, privilege and confidentiality review.
6. Produce in the required format and secure channel.
7. Record production, supplements, questions and closure.

22.3 Decision-logic and explanation evidence pattern

Evidence item	Illustrative content
Decision identity	Transaction, system, model and policy versions.
Material context	Input, relevant features, retrieved sources and constraints.
Decision basis	Rules, reason codes, factors or explanation artifact appropriate to the system.
Human role	Review, override, appeal and approval.
Outcome	Output, action, downstream effect and correction.
Limitations	Uncertainty, unavailable fields, redactions and rationale.

22.4 Sample evidence package

Control D1-CTL-01 example: claim—"Model X deployed in Production was trained using approved Dataset Y and Code Version Z." Evidence may include the model card, dataset lineage record, training manifest, source commit hash, build attestation, registry record and signed deployment approval. Sufficiency remains scope- and risk-dependent.

22.5 Redaction decision record

Field	Content
Artifact and location	Evidence identifier and exact portion affected.
Reason	Legal privilege, personal data, security sensitivity, third-party confidentiality or irrelevance.
Authority	Policy, legal basis and approver.
Method	Mask, remove, substitute or controlled unredacted copy.
Impact	Whether the redaction affects the control claim or reviewability.
Verification	Reviewer and date.

23. Limitations

- No universal evidence package is sufficient for every system or control.
- Supplier opacity may prevent direct evidence and require alternative assurance.
- Automated evidence collection can reproduce incorrect configuration or incomplete scope.
- Sampling cannot prove the absence of rare failures outside the sample.
- Privacy, safety and legal constraints may limit evidence sharing even when evidence exists.

24. Notably Absent

- No rule that a certificate or policy automatically satisfies a GAISSF control.
- No permission to omit failed, negative or inconclusive evidence.
- No fixed evidence-retention period for all organizations.
- No universal sample size or testing frequency.
- No assumption that screenshots alone establish technical operation.
- No requirement to collect unnecessary personal or confidential data.
- No assertion that GAISSF VTSS are regulator-mandated tests.
- No universal duty-to-preserve trigger from ordinary evidence collection.
- No per-control checklist that supersedes NOR-004 or creates a second control catalogue.

Annex A — Evidence Plan Template

Field	Entry
Control ID	
Claim	
Scope	
Artifact types	
Source	
Generator	
Custodian	
Frequency	
Evidence period	
Collection method	
Integrity method	
Retention	
Limitations	
Reviewer	

Annex B — Evidence Index Template

Evidence ID	Control	System	Type	Period	Source	Owner	Integrity	Status	Location

Annex C — Chain-of-Custody Record

Evidence ID	From	To	Date/time	Purpose	Hash/signature	Transformation	Accepted by

Annex D — Sampling Record

Field	Entry
Control ID	
Population	
Period	
Sampling method	
Sample size	
Strata	
Selection logic	
Exceptions	
Projection limits	
Reviewer	

Annex E — Evidence Acceptance Checklist

- ☐ Artifact supports the exact control claim
- ☐ Scope and period are explicit
- ☐ Source and collector are attributable

- ☐ Version matches the assessed implementation
- ☐ Integrity is protected or verified
- ☐ Failures and exceptions are included
- ☐ Sampling is documented where used
- ☐ Privacy and confidentiality are addressed
- ☐ Limitations are recorded
- ☐ Repository location and retention are assigned

Annex F — Source Traceability

Evidence subject	Controlled source
Normative requirements and evidence fields	GAISST-NOR-001 and GAISST-NOR-004
Terminology	GAISST-NOR-005
Source references	GAISST-NOR-006
Release and change status	GAISST-NOR-007 and GAISST-NOR-008
Adoption planning	GAISST-IMP-009, where published and current
Implementation workflows	GAISST-IMP-010, where published and current
Deployment records	GAISST-IMP-011, where published and current
Migration and evidence reuse	GAISST-IMP-012, where published and current
Reference architecture and telemetry	GAISST-IMP-013, where published and current
Operational evidence maintenance	GAISST-IMP-014, where published and current
Interpretation and issue resolution	GAISST-IMP-015 and GAISST-IMP-016, where published and current

Related guidance	Document
Exact evidence expectations	GAISST-NOR-004
Evidence operations	GAISST-IMP-014, where published and current
Preservation-aware troubleshooting	GAISST-IMP-016, where published and current

Annex G — Publication Record

Date	Change
29 June 2026	Initial evidence collection guide for GAISST TM v1.0.

Date	Change
05 October 2026	Corrected domain names in Section 14 to GAISSF-NOR-001; aligned certification references to the current position (not offered); moved legal and regulatory integration, preservation, examination-readiness, decision-logic, sample-package and redaction guidance into the body; clarified independent-assessor terminology, future-certification legal wording and implementation-guide dependency status. No GAISSF™ control was added, removed, renamed or amended.

GAISSF™ is a framework of ODA3 Institute, referenced under the GAISSF Ecosystem Licence (GEL) v1.0. | GAISSF Ecosystem developed by ODA3 Institute, licensed under GEL v1.0. | © 2026 ODA3 Pvt Ltd