

ODA3 INSTITUTE

GLOSSARY

GAISSF™ v1.0 Glossary

Global AI Safety and Security Framework

GAISSF-NOR-005 | Normative | Final Publication Edition

Published 1 July 2026 | Updated 4 October 2026

© 2026 ODA3 Pvt Ltd

Document Control

Document title	GAISSF™ v1.0 Glossary
Document ID	GAISSF-NOR-005
Version	1.0
Status	Final Publication Edition
Classification	Normative
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
Authoritative framework source	GAISSF-NOR-001, Framework Standard
Control catalogue source	GAISSF-NOR-004, Control Catalogue
Control baseline	59 controls across nine domains
Foundational scope	52 canonical controls in D1-D8
Operational scope	52 D1-D8 controls plus all applicable D9 controls; operating-effectiveness evidence required
Optimized scope	Same applicable control scope as Operational plus continuous monitoring and enhanced assurance
Distribution	Public - docs.oda3.org / official ODA3 publication channels
Updated	4 October 2026

Copyright, Licensing and Legal Notice

Copyright © 2026 ODA3 Pvt Ltd. Published by ODA3 Institute. GAISSF™ is a trademark of ODA3 Pvt Ltd. Use, reproduction, adaptation, and distribution are governed by the licence and legal notices accompanying the official GAISSF release package.

This document defines terminology for GAISSF conformance and assessment. It does not provide legal advice, does not establish regulatory compliance, and does not guarantee that an AI system is secure, safe, lawful, unbiased, accurate, reliable, or free from harmful outcomes.

Precedence and Interpretation

GAISSF-NOR-001 remains the authoritative framework standard. GAISSF-NOR-004 remains the authoritative control catalogue. This glossary governs the meaning of defined terms across the GAISSF v1.0 document set unless a governing document expressly provides a narrower definition for a specific clause or control. In the event of conflict, the more specific normative provision shall prevail.

Table of Contents

1. Purpose

This document establishes a controlled vocabulary for consistent authoring, implementation, assessment, training, automation and cross-framework mapping within the GAISSF ecosystem. It also defines terminology that may be used by a future GAISSF certification scheme if one is separately issued. Definitions are implementation-independent and are intended to support testable and auditable interpretation.

2. Scope

This glossary applies to GAISSF v1.0 normative, implementation, assessment, schema, validation, crosswalk, training and sector-profile artifacts, and to any future certification artifacts only if a GAISSF certification scheme is separately issued. It covers security, safety, governance, evidence, conformance, agentic AI, supply-chain, content, societal harm, regulatory and physical-AI terminology.

3. Normative Language

- **SHALL:** indicates a requirement necessary for conformance.
- **SHALL NOT:** indicates a prohibited action or condition.
- **SHOULD:** indicates a recommended practice for which a justified alternative may exist.
- **SHOULD NOT:** indicates a practice that is generally discouraged, although a justified exception may exist.
- **MAY:** indicates permission or an optional capability.
- **RECOMMENDED:** indicates a preferred but non-mandatory approach.

4. Terminology Rules

- Defined terms shall be interpreted consistently across GAISSF documents, schemas, tests, assessor materials and public claims, and across any future certificates or certification materials only if a GAISSF certification scheme is issued.
- Singular terms include the plural where context permits, and vice versa.
- Examples and notes are informative unless expressly identified as normative.
- A term imported from another framework shall not be presumed equivalent merely because the same label is used.
- Control identifiers, domain identifiers, tier names, and document identifiers shall not be renamed in controlled artifacts.
- Where legal or sector terminology differs by jurisdiction, the applicable law or profile shall be recorded without altering the GAISSF base definition.

5. Domain Names and Control Baseline

Domain	Official title	Control count	Tier note
D1	Model Integrity & Adversarial Robustness	9	D1-D8: Foundational/Operational/Optimized
D2	Runtime Security & Adversarial Defense	6	D1-D8: Foundational/Operational/Optimized
D3	Agentic Risk & Autonomous System Security	7	D1-D8: Foundational/Operational/Optimized
D4	Supply Chain & Third-Party AI Security	7	D1-D8: Foundational/Operational/Optimized
D5	Content Safety & Output Integrity	6	D1-D8: Foundational/Operational/Optimized
D6	Governance, Accountability & Human Oversight	7	D1-D8: Foundational/Operational/Optimized
D7	Human & Societal Harms	5	D1-D8: Foundational/Operational/Optimized
D8	Regulatory Alignment & Compliance	5	D1-D8: Foundational/Operational/Optimized
D9	Physical AI Safety	7	Additional/conditional at all tiers; mandatory where Physical AI is in scope

Control count verification: $9 + 6 + 7 + 7 + 6 + 7 + 5 + 5 + 7 = 59$ controls. The canonical Foundational scope contains the 52 controls in D1-D8. Operational and Optimized use the same applicable control scope: the 52 D1-D8 controls plus all D9 controls that become mandatory where Physical AI or cyber-physical actuation is in scope. Operational requires operating-effectiveness evidence; Optimized additionally requires continuous monitoring and enhanced assurance.

6. Controlled Definitions

The following definitions are normative for GAISSF v1.0 unless a more specific definition is stated in a governing clause or control. Notes clarify usage but do not create additional requirements.

A

Accountable executive

The senior individual who is answerable for ensuring that GAISSF obligations within an approved scope are governed, resourced, monitored, and escalated.

Usage note: Accountability may be delegated for execution but not transferred without formal governance approval.

Primary references: D6; NOR-001 §§4, 7

Adversarial example

An input intentionally designed or modified to cause an AI system to produce an incorrect, unsafe, or otherwise unintended result.

Usage note: Includes digital, physical, and multimodal perturbations.

Primary references: D1, D2

Adversarial robustness

The ability of an AI system to maintain defined security, safety, and performance properties when exposed to maliciously crafted inputs, manipulations, or operating conditions.

Usage note: Robustness claims require context-specific test evidence.

Primary references: D1

Agentic AI system

An AI system capable of selecting, sequencing, or executing actions toward a goal with a degree of operational autonomy, including use of tools, APIs, memory, or external resources.

Usage note: The term does not imply consciousness or legal agency.

Primary references: D3

AI component

A model, service, agent, data-processing element, prompt layer, retrieval component, tool connector, safety mechanism, or other technical element that contributes to an AI system.

Usage note: Components may be internally developed or supplied by third parties.

Primary references: D1-D5

AI incident

An event involving an AI system that causes, contributes to, or creates a credible risk of security compromise, safety harm, rights impact, material service disruption, regulatory breach, or loss of control.

Usage note: Organizations shall define incident thresholds appropriate to scope and context.

Primary references: D2, D6, D8, D9

AI lifecycle

The stages through which an AI system passes, including conception, design, data acquisition, development, validation, deployment, operation, monitoring, modification, retirement, and disposal.

Usage note: Lifecycle boundaries shall include material third-party dependencies.

Primary references: D1-D9

AI system

An engineered system that uses machine-based inference to generate outputs such as predictions, content, recommendations, decisions, or actions that influence physical or virtual environments.

Usage note: This definition is implementation-independent and includes composite systems.

Primary references: All domains

Applicable control

A GAISSF control determined through scope, risk, tier, and profile analysis to apply to the assessed organization, system, or service.

Usage note: Applicability shall be recorded in the Statement of Applicability.

Primary references: NOR-001 §§5, 7

Assessment boundary

The documented organizational, technical, operational, geographic, legal, and temporal limits within which conformance is evaluated.

Usage note: Excluded dependencies shall be identified and justified.

Primary references: NOR-001 §7

Assessment evidence

Information used by an assessor to determine whether a control is designed, implemented, and operating effectively.

Usage note: Evidence may be documentary, technical, testimonial, observational, or analytical.

Primary references: NOR-001 §6

Assessment procedure

A defined set of examination, interview, observation, testing, and sampling activities used to evaluate a control.

Usage note: Procedures shall be sufficient to support a reproducible conclusion.

Primary references: NOR-004

Assessor

A competent person or team authorized to evaluate GAISSF conformance within a defined assessment scope.

Usage note: Independence requirements depend on the assessment type. Any future GAISSF certification scheme may impose additional independence, competence or accreditation requirements.

Primary references: NOR-001 §7

Assurance

Confidence, supported by evidence, that specified requirements have been fulfilled and material risks are being controlled within stated limits.

Usage note: Assurance is not a guarantee of absence of failure or harm.

Primary references: NOR-001 §§6-7

Audit trail

A chronological, integrity-protected record that enables reconstruction of significant decisions, actions, changes, and events.

Usage note: Audit trails shall be attributable and retained according to defined requirements.

Primary references: D2, D3, D6, D8

Autonomy boundary

The explicit limit on decisions, actions, resources, tools, environments, or consequences an agentic or physical AI system is permitted to control without human authorization.

Usage note: Boundaries shall be technically enforceable where feasible.

Primary references: D3, D9

B

Bias

A systematic tendency in data, models, processes, or outcomes that may produce skewed, unfair, or otherwise undesirable effects.

Usage note: Not every statistical difference constitutes prohibited discrimination; context and impact assessment are required.

Primary references: D5, D7

C

Certification

A third-party attestation, under a separately issued GAISSF certification scheme, that specified GAISSF requirements have been fulfilled for a defined scope, tier, profile and period.

Usage note: ODA3 certification is not currently offered. If a GAISSF certification scheme is issued in future, certification would not guarantee security, safety, legality, accuracy or absence of harm.

Primary references: NOR-001 §7

Certification body

An organization authorized to perform conformity assessment and certification activities under a separately issued GAISSF certification scheme.

Usage note: No organization should be described as a GAISSF certification body unless an applicable scheme is active and the authorization is current. Accreditation is separate and shall not be implied unless expressly granted for the relevant scope.

Primary references: NOR-001 §7

Certification scope

The precise organization, AI systems, services, sites, processes, interfaces and exclusions that would be covered by a GAISSF certificate under a separately issued certification scheme.

Usage note: Certification is not currently offered. Under any future scheme, public certification claims shall not exceed the certified scope.

Primary references: NOR-001 §7

Change control

A governed process for requesting, assessing, approving, implementing, verifying, documenting, and reviewing changes.

Usage note: Material AI changes may trigger reassessment.

Primary references: D1-D4, D6, D8

Compensating control

An alternative measure that reduces risk when the primary control cannot be implemented as specified.

Usage note: A compensating control requires documented equivalence analysis and approval; it does not automatically satisfy the original control.

Primary references: NOR-001 §8

Conformance

Fulfilment of all applicable GAISSF requirements for the declared scope, tier, and profiles, subject to approved and valid exceptions.

Usage note: Conformance is distinct from maturity and certification.

Primary references: NOR-001 §§5, 7

Conformance claim

A statement asserting that an organization, system, service, or defined scope fulfils specified GAISSF requirements.

Usage note: Claims shall identify scope, tier, profile, version, and assessment basis.

Primary references: NOR-001 §7

Conformance tier

A defined GAISSF conformance level that specifies the applicable control requirements and the evidence or assurance expectations for an implementation.

Usage note: GAISSF v1.0 uses Foundational, Operational, and Optimized tiers.

Primary references: NOR-001 §7

Continuous monitoring

Ongoing or sufficiently frequent collection and analysis of control, system, threat, and evidence signals to detect material change or degradation.

Usage note: Frequency shall reflect risk and control criticality.

Primary references: Optimized tier; D2, D6, D8

Control

A normative requirement or coordinated measure intended to modify risk and produce an assessable outcome.

Usage note: GAISSF v1.0 contains 59 controls across nine domains.

Primary references: NOR-001; NOR-004

Control objective

The security, safety, governance, or assurance outcome a control is intended to achieve.

Usage note: Objectives guide interpretation but do not replace the normative requirement statement.

Primary references: NOR-004

Control owner

The person or function assigned authority and responsibility for implementation, operation, evidence, and remediation of a control.

Usage note: Ownership shall be documented and current.

Primary references: D6; NOR-003

Corrective action

Action taken to eliminate the cause of a detected nonconformity and prevent recurrence.

Usage note: Correction of an isolated symptom is not necessarily corrective action.

Primary references: NOR-001 §7

D

Data lineage

Traceable information describing the origin, transformation, movement, use, and disposition of data across the AI lifecycle.

Usage note: Lineage may include provenance, licensing, consent, and quality records.

Primary references: D1, D4, D5

Data poisoning

Deliberate manipulation of training, tuning, evaluation, retrieval, or operational data to influence AI system behavior.

Usage note: Poisoning may target integrity, availability, confidentiality, or downstream behavior.

Primary references: D1, D4

Decommissioning

The controlled retirement of an AI system or component, including removal of access, data disposition, dependency management, record retention, and residual-risk treatment.

Usage note: Deactivation alone may not complete decommissioning.

Primary references: D4, D6, D8

Domain

A coherent grouping of GAISSF controls addressing a related area of AI security, safety, governance, or assurance.

Usage note: GAISSF v1.0 contains nine domains, D1 through D9.

Primary references: NOR-001 §3

Drift

A material change over time in data, model behavior, system context, usage, threats, or performance relative to an approved baseline.

Usage note: Drift can be benign or harmful and may require revalidation.

Primary references: D1, D2, D5

E

Evidence package

An organized set of evidence artifacts, metadata, mappings, attestations, and integrity information submitted for assessment.

Usage note: Evidence packages shall identify scope, period, source, owner, and control linkage.

Primary references: NOR-001 §6

Evidence period

The time interval over which operating evidence is collected and evaluated.

Usage note: The period shall be sufficient to demonstrate sustained operation rather than point-in-time design alone.

Primary references: NOR-001 §§6-7

Exception

A formally approved, time-bounded deviation from an applicable GAISSF requirement.

Usage note: An exception shall include rationale, risk analysis, compensating measures, owner, expiry, and review.

Primary references: NOR-001 §8

Explainability

The extent to which relevant persons can understand factors, logic, or evidence associated with an AI system output or behavior at a level appropriate to their role and risk context.

Usage note: Explainability is context-dependent and is not synonymous with complete model transparency.

Primary references: D6, D7, D8

External dependency

A third-party product, service, dataset, model, API, platform, infrastructure, or operator on which the AI system depends.

Usage note: Dependencies shall be included in supply-chain risk analysis.

Primary references: D4

F

Foundational tier

The GAISSF conformance tier comprising the 52 canonical controls in D1-D8, with the seven D9 controls additionally mandatory whenever physical AI or cyber-physical actuation is within scope.

Usage note: D9 is outside the canonical 52-control baseline but becomes mandatory when physical AI or cyber-physical actuation is within the assessed scope.

Primary references: NOR-001 §7; Annex A

H

Harm

A negative effect on persons, organizations, society, property, the environment, or critical functions.

Usage note: Harm may be physical, psychological, economic, legal, reputational, informational, or rights-related.

Primary references: D5, D7, D9

Human oversight

Governance and operational mechanisms enabling competent persons to supervise, understand, intervene in, override, suspend, or terminate AI system operation as appropriate.

Usage note: Nominal human presence without authority, information, or time to act is not effective oversight.

Primary references: D3, D6, D9

I

Impact assessment

A structured evaluation of potential and actual effects of an AI system on security, safety, rights, stakeholders, operations, and compliance.

Usage note: Assessments shall be proportionate to risk and lifecycle stage.

Primary references: D6-D8

Implementation guidance

Non-normative explanatory material describing possible ways to satisfy a requirement.

Usage note: Alternative implementations may be acceptable when they meet the normative requirement and evidence expectations.

Primary references: NOR-004

Incident response

Coordinated activities to prepare for, detect, analyze, contain, eradicate, recover from, and learn from incidents.

Usage note: AI-specific playbooks may be required for model, data, agent, content, and physical-system events.

Primary references: D2, D3, D6, D9

Inference

The process by which an AI model generates an output from input data or context.

Usage note: Inference may occur locally, remotely, continuously, or through a third-party service.

Primary references: D1-D3

Integrity

The property of accuracy, completeness, consistency, authenticity, and protection from unauthorized modification or destruction.

Usage note: Integrity applies to models, data, code, configurations, logs, evidence, and outputs.

Primary references: D1, D2, D4, D5

M

Material change

A change reasonably capable of affecting risk, control effectiveness, assessment scope, conformance conclusions or any future certification scope.

Usage note: Examples include model replacement, new tools, expanded autonomy, new jurisdictions, or significant retraining.

Primary references: NOR-001 §9

Maturity

The degree to which capabilities and processes are established, managed, measured, integrated, and continually improved.

Usage note: High maturity does not cure failure to meet an applicable mandatory control.

Primary references: NOR-001 §7

Metric

A quantitative or qualitative measure used to evaluate control performance, risk, trend, or outcome.

Usage note: Metrics shall be interpreted in context and shall not replace assessment judgment.

Primary references: NOR-004

Model card

A structured record describing an AI model's purpose, characteristics, limitations, intended uses, evaluation results, and governance information.

Usage note: Content and depth shall reflect risk and stakeholder needs.

Primary references: D1, D6, D8

Model extraction

An attack or unauthorized activity intended to reconstruct, replicate, or infer material properties of a model through queries, outputs, or access.

Usage note: Also called model stealing in some sources.

Primary references: D1, D2

Model inversion

An attack or analytical technique that infers sensitive information about training data or model inputs from model access or outputs.

Usage note: Risk depends on data sensitivity and access conditions.

Primary references: D1, D5

N

Nonconformity

Non-fulfilment of an applicable GAISSF requirement.

Usage note: Nonconformities shall be classified and handled according to the applicable assessment rules and, if a future certification scheme is issued, any additional scheme rules.

Primary references: NOR-001 §7

Normative

Prescribing requirements necessary for conformance, typically expressed using SHALL or SHALL NOT.

Usage note: Normative content prevails over informative examples or guidance.

Primary references: NOR-001 §2

O

Operational tier

The GAISSF conformance tier requiring the 52 controls in D1-D8 plus all D9 controls that are applicable because Physical AI or cyber-physical actuation is within scope, together with operating-effectiveness evidence.

Usage note: Operational does not make D9 universally mandatory. D9 remains applicability-driven; the tier adds operating-effectiveness expectations to the applicable control scope.

Primary references: NOR-001 §7; Annex A

Operating effectiveness

The degree to which an implemented control functions consistently as intended over the relevant evidence period.

Usage note: Design and implementation alone do not demonstrate operating effectiveness.

Primary references: NOR-001 §6

Optimized tier

The GAISSF conformance tier using the same applicable control scope as Operational, with continuous monitoring and enhanced evidence, measurement and improvement expectations.

Usage note: Optimized does not mean risk-free or perfect.

Primary references: NOR-001 §7; Annex A

Output integrity

The degree to which AI outputs are protected against unauthorized manipulation and remain attributable, traceable, and consistent with defined safety and security constraints.

Usage note: Output integrity includes provenance and downstream handling where applicable.

Primary references: D5

P

Physical AI

An AI-enabled system capable of sensing, influencing, controlling, or acting within the physical world.

Usage note: Examples include robots, vehicles, industrial control, medical devices, and autonomous machinery.

Primary references: D9

Post-deployment monitoring

Collection and evaluation of information about an AI system after release or deployment to identify drift, incidents, misuse, control degradation, or emerging harm.

Usage note: Monitoring shall reflect the operating context and risk.

Primary references: D1, D2, D5-D9

Prompt injection

An attack or manipulation in which instructions or content are crafted to alter an AI system's intended behavior, override controls, disclose information, or trigger unauthorized actions.

Usage note: Prompt injection may be direct or indirect.

Primary references: D2, D3

Provenance

Information sufficient to establish the origin, custody, transformation, and authenticity of an artifact, dataset, model, output, or evidence item.

Usage note: Provenance supports integrity and accountability but may not prove truthfulness.

Primary references: D1, D4, D5

R

Red teaming

A structured adversarial evaluation designed to identify vulnerabilities, unsafe behavior, control weaknesses, and plausible abuse paths.

Usage note: Red teaming shall be scoped, authorized, risk-managed, and evidence-producing.

Primary references: D1-D3, D5, D7, D9

Residual risk

Risk remaining after controls and other treatments have been applied.

Usage note: Residual risk shall be evaluated and accepted only by authorized persons within defined authority.

Primary references: NOR-001 §8

Risk acceptance

A documented decision by an authorized risk owner to retain a defined residual risk for a stated period and scope.

Usage note: Acceptance does not remove accountability or monitoring duties.

Primary references: NOR-001 §8

Risk owner

The person with authority and accountability to make decisions concerning a specified risk.

Usage note: The risk owner may differ from the control owner.

Primary references: D6; NOR-001 §8

S

Safety case

A structured, evidence-supported argument that a system is acceptably safe for a defined use and environment.

Usage note: A safety case may be required by sector or profile but is not universally prescribed for every GAISSF scope.

Primary references: D9

Sampling

Selection of a subset of populations, records, systems, transactions, time periods, or evidence items for assessment.

Usage note: Sampling shall be risk-based, representative, documented, and sufficient to support conclusions.

Primary references: NOR-001 §7

Sector Profile

A separately issued, approved set of additional, tailored or clarified requirements and evidence expectations for a particular sector, technology, use case or risk context.

Usage note: Where issued, Sector Profiles are additive and shall not weaken base requirements. Sector guidance documents are not automatically Sector Profiles.

Primary references: NOR-001 §7

Statement of Applicability (SoA)

The controlled record identifying the GAISSF controls applicable to a defined scope, together with implementation status, justification, ownership, evidence, exceptions, and profile requirements.

Usage note: The SoA is a central conformance and assessment artifact and may support a future certification process only if a separate GAISSF certification scheme is issued.

Primary references: NOR-001 §5

Supply chain

The network of organizations, people, processes, technologies, data, models, services, and infrastructure involved in creating, delivering, operating, or supporting an AI system.

Usage note: Supply-chain scope includes upstream and downstream dependencies.

Primary references: D4

System boundary

The documented technical and operational limit separating an AI system from its environment and external dependencies.

Usage note: Boundaries shall include interfaces, trust zones, data flows, and control responsibility.

Primary references: D1-D4

T

Threat

A circumstance, actor, event, or condition with the potential to exploit a vulnerability or otherwise cause harm.

Usage note: Threat identification shall account for malicious and non-malicious causes.

Primary references: All domains

Threat model

A structured representation of assets, actors, trust boundaries, attack paths, hazards, assumptions, and mitigations relevant to a system.

Usage note: Threat models shall be maintained when material changes occur.

Primary references: D1-D4, D9

Third party

An external organization or individual that supplies, operates, supports, assesses, or otherwise materially affects an in-scope AI system.

Usage note: Contracting does not transfer the organization's accountability for applicable controls.

Primary references: D4, D6

Tool use

The capability of an AI system or agent to invoke software, APIs, devices, databases, or services to perform actions beyond text generation.

Usage note: Tool permissions shall follow least privilege and autonomy boundaries.

Primary references: D3

Traceability

The ability to follow the history, application, location, decision basis, and control linkage of an item or event.

Usage note: Traceability shall be sufficient for assessment and incident reconstruction.

Primary references: D1-D8

V

Validation

Confirmation, through objective evidence, that requirements for a specific intended use or application have been fulfilled.

Usage note: Validation is distinct from verification.

Primary references: D1, D5, D9

Verification

Confirmation, through objective evidence, that specified requirements have been fulfilled.

Usage note: Verification asks whether the system was built or configured correctly against specifications.

Primary references: D1, D4, D9

Vulnerability

A weakness in design, implementation, configuration, operation, governance, or dependency that may be exploited or contribute to harm.

Usage note: Vulnerabilities may be technical or procedural.

Primary references: All domains

W

Withdrawal

Formal removal or invalidation of an authorized conformance claim or, under a separately issued future scheme, a certification.

Usage note: Withdrawal of a conformance claim may result from unresolved material nonconformity, misrepresentation or scope failure. Any future certification withdrawal would follow the separately issued scheme rules.

Primary references: NOR-001 §7

7. Abbreviations and Acronyms

Abbreviation	Meaning
AI	Artificial Intelligence
AIA	AI Impact Assessment
AIMS	Artificial Intelligence Management System
API	Application Programming Interface
CAB	Conformity Assessment Body
CAPA	Corrective and Preventive Action
CIS	Center for Internet Security
CI/CD	Continuous Integration / Continuous Delivery
CISO	Chief Information Security Officer
DPA	Data Processing Agreement or Data Protection Authority, according to context
DPIA	Data Protection Impact Assessment
GAISSF	Global AI Safety and Security Framework
GEL	GAISSF Ecosystem Licence
GPAI	General-Purpose AI
HIL	Hardware-in-the-Loop
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LLM	Large Language Model
ML	Machine Learning
MITRE ATLAS	Adversarial Threat Landscape for Artificial-Intelligence Systems
NIST	National Institute of Standards and Technology
OWASP	Open Worldwide Application Security Project
PII	Personally Identifiable Information
RACI	Responsible, Accountable, Consulted, Informed
RAG	Retrieval-Augmented Generation
RMF	Risk Management Framework
SBOM	Software Bill of Materials
SoA	Statement of Applicability
SLA	Service-Level Agreement

Abbreviation	Meaning
SOP	Standard Operating Procedure
VTS	Validation Test Specification
XAI	Explainable Artificial Intelligence
ZTA	Zero Trust Architecture

8. Controlled Identifiers

Identifier pattern	Meaning	Example
GAISSF-NOR-###	Normative or controlled GAISSF publication identifier	GAISSF-NOR-005
D#-CTL-##	Domain and control identifier	D3-CTL-04
VTS-...	Validation Test Specification identifier	As defined in the controlled VTS register
Profile identifier	Approved sector or implementation profile identifier	As defined in the profile publication

9. Prohibited or Ambiguous Usage

Expression	GAISSF usage rule
Certified AI	Shall not be used as a GAISSF claim while GAISSF certification is not currently offered. If a future GAISSF certification scheme is issued, any certification claim shall identify the precise certified scope, certificate holder, tier, profile, version, certification body and validity period.
GAISSF compliant	Should be replaced by a precise conformance claim identifying scope, tier, version, profiles, and assessment basis.
Safe AI	Shall not be treated as an absolute claim. Safety is context-dependent, and neither conformance nor any future certification guarantees absence of harm.
Secure AI	Shall not imply immunity from vulnerabilities, incidents, misuse, or emerging threats.
Accredited	Shall not be used unless accreditation exists and the accreditor, scope, and standard are accurately stated.
Equivalent to ISO/NIST/OWASP/MITRE/CIS	Shall not be claimed solely because a mapping or crosswalk exists.
Full compliance	Shall not be used without identifying the exact law, requirement set, scope, date, and competent determination.

10. Terminology Governance

- New or revised terms shall be proposed through the GAISSF change-management process.
- A terminology change that alters control meaning, scope, evidence, assessment or any future certification interpretation shall be treated as a normative change.
- Editorial changes shall not alter obligations or conformance outcomes.
- Schemas, VTS artifacts, assessor guidance, training, and crosswalks shall be checked for terminology impact before release.
- Deprecated terms shall remain traceable to their replacements for at least the supported version lifecycle.
- Translation shall preserve normative meaning; where ambiguity exists, the English-language controlled release shall prevail unless ODA3 Institute publishes an equally authoritative language edition.

11. Framework Limitations and Notably Absent

This glossary standardizes language; it does not independently establish technical controls, legal conclusions, sector-specific risk thresholds, universal safety criteria, model-performance benchmarks, regulatory equivalence or a certification programme. Definitions do not convert examples into requirements. Certification is not currently offered; any future certification would be governed by a separately issued scheme and bounded assessment scope.

Notably absent: a claim that common terminology guarantees common implementation; a universal definition of acceptable risk; a presumption that mapped external terms are legally or technically equivalent; a guarantee that every jurisdiction uses the same meaning; and a claim that terminology alone demonstrates control effectiveness.

Annex A — Term-to-Documents Reference Matrix

This informative matrix identifies the principal document families in which terminology is used. It is not exhaustive.

Document	Primary terminology role	Precedence
GAISSF-NOR-001	Framework requirements, governance, evidence, conformance, assessment and future-certification boundary	Authoritative framework standard

Document	Primary terminology role	Precedence
GAISSF-NOR-002	Executive interpretation and adoption context	Informative; NOR-001 prevails
GAISSF-NOR-003	Implementation sequencing, examples, and starter templates	Informative; NOR-001 prevails; NOR-004 is the control companion where relevant
GAISSF-NOR-004	Normative control records and control-specific terminology	Normative control catalogue; NOR-001 prevails on framework interpretation
GAISSF-NOR-005	Controlled definitions and abbreviations	Terminology authority unless a more specific normative provision applies

Annex B — Change Record

Version	Date	Change	Approval status
1.0	1 July 2026	Initial GAISSF v1.0 controlled glossary aligned to the 59-control baseline and NOR-001 through NOR-004.	Final Publication Edition
1.0	4 October 2026	Reconciled to locked NOR-001 through NOR-004: canonical name/mark treatment, applicability-driven D9 at all tiers, current certification boundary, corrected GEL expansion, terminology precedence, and removal of stale certification assumptions.	Final Publication Edition - updated

Controlled Profile Reconciliation Notice

The Foundational profile comprises the 52 canonical controls in D1-D8. The seven D9 controls are additional mandatory controls whenever physical AI or cyber-physical actuation is within the assessed scope.

Any earlier wording that described the Foundational profile as spanning all nine domains, treated D9 as universally mandatory or universally excluded, or defined Operational/Optimized as automatically requiring all 59 controls is superseded. D9 applicability shall be determined and justified for every assessed scope.

Terminology Interpretation Rules

- Use the defined singular and plural consistently.
- Do not substitute marketing terms for controlled conformance terms.
- Where an external source uses a different meaning, identify that source-specific meaning.
- New terms require definition, owner, rationale and impact review.

Term Governance Workflow

Stage	Action
Propose	Submit term, definition, context and affected documents.
Review	Check technical, legal and cross-document consistency.
Approve	Assign authority and effective version.
Publish	Update glossary and affected artifacts.
Retire	Mark deprecated aliases and migration guidance.

Revision Note - 4 October 2026

Reconciled to the locked GAISSF-NOR-001 through NOR-004 publication baseline. Corrected the canonical framework name and mark treatment; corrected Operational and Optimized scope so D9 remains applicability-driven; made certification terminology explicitly future-scheme terminology because certification is not currently offered; corrected the GEL expansion; clarified NOR-001/NOR-004 precedence; removed stale registered-mark and certification assumptions; added the update date, standard ODA3 cover and page numbering. No control requirement is created or changed by this glossary update.

Publication Completeness and Intended Use

This publication edition of GAISSF-NOR-005 is designed to stand on its own for its stated role: controlled terminology and abbreviation authority. It includes purpose, scope, governance, operating guidance, evidence terminology, limitations, decision criteria and reusable records appropriate to that role.

Completeness does not mean that the document replaces the normative control statements, applicable law, sector-specific engineering, organizational procedures or professional judgement. Cross-referenced GAISSF documents remain part of the controlled document system.

Completeness dimension	Treatment in this edition
Normative alignment	Reconciled to the authoritative 59-control baseline and controlled profile structure.
Operational usability	Includes roles, workflows, gates, evidence, metrics, escalation and examples where relevant.
Traceability	Identifies dependencies and preserves the distinction between requirements, guidance and examples.
Limitations	States what the document does not establish or guarantee.
Maintenance	Includes review triggers, change control and publication status.

Controlled Evidence Terminology

Design evidence: documentation showing intended control design, including policies, standards, architectures, procedures, and approved specifications.

Implementation evidence: documentation or observation showing that a designed control has been deployed or configured.

Operating-effectiveness evidence: period-of-time or event-population evidence showing that an implemented control operated as intended, including exceptions and failure treatment.

Evidence source: the origin of evidence, such as internally generated, supplier-provided, independently produced, observed, re-performed, technically tested, or simulated.

Source tier: a classification used by GAISSF-NOR-006 for the authority and proximity of cited references. Source tier does not rate assessment-evidence sufficiency, reliability, or operating effectiveness. GAISSF v1.0 does not establish a second T1-T4 assessment-evidence scale.