

ODA3 INSTITUTE

IMPLEMENTATION GUIDANCE

GAISSF™ v1.0 Frequently Asked Questions

Adoption, implementation, assurance, public claims and operations

GAISSF-IMP-015 | Public

© ODA3 Pvt Ltd

Document Control

Document ID	GAISSF-IMP-015
Title	GAISSF™ v1.0 Frequently Asked Questions
Doc Type	Implementation guidance — informative
Primary Audience	Executives, boards, practitioners, implementers, assessors, legal teams, procurement, suppliers, customers, regulators and the public
Dependencies	GAISSF-NOR-001 to GAISSF-NOR-008; GAISSF-IMP-009 to GAISSF-IMP-014, 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 GAISSF™ update or correction notice, legal change or recurring ambiguity
Contact	contact@oda3.org
Classification	Public

GAISSF™ v1.0 Frequently Asked Questions

Adoption, implementation, assurance, public claims and operations

Reliance notice: This FAQ explains GAISSF™ v1.0 in plain language. It does not amend the normative framework: where an answer conflicts with GAISSF-NOR-001 or GAISSF-NOR-004, those prevail. It is not legal, regulatory, safety, engineering, certification or audit advice, does not create a legal safe harbour or standard of care, and guarantees no compliance, security, safety or market access. Certification is not currently offered.

How to Use This FAQ

The questions are grouped by topic. Readers may use the document as an onboarding reference, a procurement aid, an implementation companion, an assessor briefing or a publication-support resource. Questions involving exact control language, applicability, evidence or conformance should be resolved against GAISSF-NOR-001 and GAISSF-NOR-004.

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.

Reader	Recommended use
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 document as informative context only; test claims against the authoritative normative sources and applicable assessment criteria.

1. Framework Fundamentals

1. What is GAISSF?

GAISSF™ is the Global AI Safety and Security Framework. It is a structured framework for governing, securing, assessing and operating AI systems across the lifecycle, organised into nine domains covering model integrity, runtime and agentic security, supply chain, content safety, governance and human oversight, human and societal harms, regulatory alignment and physical-AI safety.

2. Who publishes GAISSF?

ODA3 Institute publishes GAISSF as the market-facing standards and assurance initiative. ODA3 Pvt Ltd is the legal entity used for copyright, contracting and other formal legal purposes.

3. What is the purpose of GAISSF?

Its purpose is to provide a common, evidence-driven baseline for managing AI security and safety risks. It is designed to support implementation, internal assurance, external assessment, customer assurance and regulatory readiness. Certification is not currently offered.

4. Is GAISSF a law or regulation?

No. GAISSF is a privately developed framework. It may help organizations structure controls and evidence relevant to legal or regulatory obligations, but it does not create law and does not determine whether a legal obligation applies.

5. Is GAISSF a standard?

GAISSF is structured and governed as a standards-based framework. Its normative documents define requirements, controlled terminology, source governance, release status and change history. Whether a particular jurisdiction or regulator formally recognizes it is a separate question.

6. How many controls are in GAISSF v1.0?

GAISSF v1.0 contains 59 controls across nine domains. The control identifiers and exact records are maintained in GAISSF-NOR-001 and GAISSF-NOR-004.

7. What are the nine GAISSF domains?

The nine domains are D1 Model Integrity & Adversarial Robustness (9 controls); D2 Runtime Security & Adversarial Defense (6); D3 Agentic Risk & Autonomous System Security (7); D4 Supply Chain & Third-Party AI Security (7); D5 Content Safety & Output Integrity (6); D6 Governance, Accountability & Human Oversight (7); D7 Human & Societal Harms (5); D8 Regulatory Alignment & Compliance (5); and D9 Physical AI Safety (7). Use these controlled domain names, as defined in GAISSF-NOR-001, for formal references.

8. Does GAISSF apply only to generative AI?

No. It applies to generative AI, predictive models, classical machine learning, agentic systems, embedded AI, decision-support systems, AI-enabled software and physical-AI systems. Applicability depends on the system and risk context.

9. Does GAISSF apply to small organizations?

Yes. Smaller organizations may tailor governance structures, staffing and tooling, but they should not dilute applicable control outcomes. Proportional implementation is acceptable; unsupported omission is not.

10. Can GAISSF be used internationally?

Yes. The framework is designed for cross-jurisdictional use. Organizations must still identify and comply with local legal, regulatory, contractual and sector-specific obligations.

2. Normative Documents and Document Hierarchy

11. Which document is the authoritative source of GAISSF requirements?

GAISSF-NOR-001 is the authoritative normative framework standard. GAISSF-NOR-004 is the detailed control catalogue. Implementation guides explain how to adopt and operate the framework but do not override the normative documents.

12. What is the role of the Executive Summary?

GAISSF-NOR-002 provides a concise executive interpretation. It is intended for leadership, customers, partners and decision-makers who need the purpose, structure and adoption implications without reading every control record.

13. What is the role of the Quick Start Guide?

GAISSF-NOR-003 gives an initial implementation sequence. It helps organizations begin inventory, scope, ownership, gap assessment and evidence collection without treating the quick-start sequence as a substitute for the full framework.

14. What is the role of the Glossary?

GAISSF-NOR-005 controls terminology and abbreviations used across the ecosystem. Formal publications, assessments and certification materials should use those terms consistently.

15. What is the role of the Bibliography?

GAISSF-NOR-006 controls reference identifiers, source classes and citation practices. It improves transparency without claiming endorsement or equivalence with external standards.

16. What is the difference between Release Notes and the Change Log?

Release Notes communicate what changed in a release and what users must do. The Change Log preserves historical traceability, decision records, corrections, supersession and the rationale behind material changes.

17. What is the role of the implementation documents?

The implementation documents translate the normative framework into adoption plans, operating procedures, architecture patterns, deployment gates, migration methods, operational workflows and common answers. They are informative unless a contract or certification scheme gives them additional status.

18. What should happen if two GAISST documents appear inconsistent?

Apply the document hierarchy. GAISST-NOR-001 and the exact control catalogue prevail over implementation guidance. The issue should be recorded through change governance rather than resolved informally.

19. Can organizations rewrite GAISST controls in their own words?

Organizations may create internal control narratives, but they should preserve a direct traceability link to the exact GAISST control identifier and requirement. Internal wording should not silently narrow the original requirement.

20. Are older GAISST drafts valid?

Only if they are explicitly identified as current. Superseded drafts, especially incorrect control-count versions, should not be used for implementation, assessment, certification, tooling or public claims.

3. Profiles, Scope and Applicability

21. What are the GAISST conformance profiles?

GAISSTTM defines three conformance tiers: Foundational, Operational and Optimized. Exact tier definitions and applicability rules are set out in GAISST-NOR-001.

22. How many controls are in the Foundational profile?

The Foundational tier contains the 52 canonical controls in D1-D8. The seven D9 Physical AI Safety controls are additional and become mandatory wherever Physical AI or cyber-physical actuation is within scope. GAISST-NOR-001 governs exact applicability decisions.

23. Do physical-AI controls apply?

Yes, wherever physical AI is in scope. The D9 Physical AI Safety controls apply to systems that perceive, control or materially influence physical environments. Profile membership is defined in GAISST-NOR-001. Where physical AI is in scope, GAISSTTM is used together with PAI-SFTM (see Section 7).

24. What does the Operational profile require?

The Operational tier uses the same applicable control scope as Foundational — the 52 D1-D8 controls plus all applicable D9 controls — and adds operating-effectiveness evidence and recurring assurance expectations.

25. What does the Optimized profile require?

The Optimized tier uses the same applicable control scope as Operational and adds advanced continuous-monitoring, assurance, integration and improvement expectations. It is not simply a higher score; it represents a more mature and continuously evidenced operating model.

26. Can an organization choose only the controls it likes?

No. Applicability should be based on the selected profile, system scope and controlled exceptions process. Convenience, cost or lack of ownership is not a sufficient reason to omit a control.

27. What is a Applicable-Control Baseline?

An Applicable-Control Baseline is the controlled record showing which controls apply, which do not, the reason for each decision, the current implementation status, ownership, evidence and any approved exceptions.

28. How should scope be defined?

Scope should identify legal entities, business units, AI systems, models, data, interfaces, suppliers, users, geographies, lifecycle stages, physical components and the intended assessment boundary. Any future certification boundary would be defined only by a separately issued certification scheme.

29. Can one organization have multiple GAISSE scopes?

Yes. An enterprise may have different product, service, platform, regional or business-unit scopes. Each scope should be explicit and should not be represented as enterprise-wide unless it genuinely is.

30. How are third-party AI services treated?

They remain inside the risk and control model even when the organization cannot inspect the provider's internals. The organization should document inherited controls, contractual protections, evidence limitations, monitoring and fallback or exit arrangements.

31. Are sector profiles replacements for the base framework?

No. Sector, product or jurisdiction profiles should be additive overlays unless the controlled profile explicitly states otherwise.

32. Can a control be marked not applicable?

Yes, but only where the profile and scope support that conclusion. The rationale should be specific, approved, reviewable and reconsidered when the system or operating context changes.

4. Adoption and Program Establishment

33. Where should an organization start?

Start with executive sponsorship, an AI-system inventory, a clear scope, selection of the intended profile, assignment of control owners and a baseline assessment. GAISSE-IMP-009 provides the full adoption method.

34. Who should sponsor adoption?

A senior executive with authority over cross-functional participation, risk acceptance, funding and scope. In larger organizations, board or risk-committee oversight may also be appropriate.

35. Which teams should participate?

Security, AI engineering, MLOps, architecture, data, privacy, legal, compliance, procurement, supplier management, product, safety, operations, internal audit and executive risk owners may all be relevant.

36. How long does adoption take?

There is no universal duration. Time depends on scope, maturity, system criticality, existing controls, evidence history, supplier dependence and remediation complexity. Fixed-duration promises should be treated cautiously.

37. Can GAISSE be adopted in phases?

Yes. A phased approach is recommended where scope is large. The organisation may begin with governance and shared controls, then add AI-engineering, safety and assurance workstreams.

38. Should an organization begin with certification?

Certification is not currently offered. Organizations should first establish stable operations, ownership, evidence and remediation. If a future certification scheme is issued, beginning with a

certificate deadline rather than operational readiness could produce paper compliance and weak control operation.

39. Can existing governance structures be reused?

Yes, where they have adequate scope and authority. Existing risk committees, security operations, internal audit, quality management and privacy governance can be extended rather than duplicated.

40. What are the most common adoption failures?

Typical failures include treating GAISSF as a checklist, copying control text into policy without implementation, under-scoping suppliers and interfaces, relying on self-attestation, collecting evidence only before audit, and confusing maturity with conformance.

5. Implementation and Architecture

41. Does GAISSF require a specific technology stack?

No. GAISSF is technology- and vendor-neutral. The implementation should achieve the required control outcomes and produce sufficient evidence.

42. Is an AI gateway mandatory?

No. An AI gateway is a useful pattern for centralized policy, routing, logging and supplier control, but other architectures may satisfy the same outcomes.

43. Does buying an AI security tool establish conformance?

No. A tool may implement part of a control, but conformance also depends on scope, ownership, configuration, workflow, evidence, testing, monitoring and operating effectiveness.

44. How should trust boundaries be documented?

Document each transition between users, applications, models, tools, data stores, suppliers, assurance services and physical actions. Record assets, identities, permitted flows, controls, telemetry, failure modes and ownership.

45. How should model versions be controlled?

Use a controlled registry or equivalent mechanism that records provider, model name, version, configuration, approval status, evaluation baseline and deployment history.

46. How should prompts and orchestration logic be governed?

Treat them as controlled configuration. Version them, review changes, test them, restrict production modification and link them to release evidence.

47. How should retrieval-augmented generation be secured?

Apply authorization before retrieval, protect tenant isolation, validate source provenance, detect poisoned or malicious content, manage freshness, constrain context and retain source-to-output traceability.

48. How should external model providers be integrated?

Use approved-provider records, data-minimization rules, contractual controls, service monitoring, model-change detection, response validation, fallback arrangements and documented evidence limitations.

49. How should edge or offline AI be handled?

Use signed model packages, secure boot, local policy enforcement, protected local telemetry, authenticated updates, rollback and clearly defined degraded-operation behavior.

50. Where can reference designs be found?

GAISSE-IMP-013 provides complete reference patterns for AI gateways, RAG, agentic AI, private-model platforms, external model services, edge AI and physical-AI systems.

6. Agentic AI

51. What makes agentic AI different from a normal AI application?

Agentic AI can plan, maintain state, call tools, delegate tasks and take actions over time. That creates additional risks around authority, persistence, transactions, memory, looping, delegation and containment.

52. How should agent permissions be designed?

Permissions should be scoped by identity, objective, tool, action type, resource, transaction value, destination, time and delegation rights.

53. Should agents have shared credentials?

Shared unrestricted credentials should be avoided. Per-agent or per-service identity improves attribution, least privilege, monitoring and revocation.

54. When is human approval required?

Human approval should be required where actions are consequential, irreversible, high-value, safety-relevant, legally significant or outside well-tested automated boundaries.

55. How should agent memory be governed?

Memory should have explicit scope, ownership, retention, separation, integrity checks, deletion, contamination controls and evidence of access and modification.

56. How can runaway agents be contained?

Use step limits, timeouts, rate limits, transaction ceilings, circuit breakers, credential revocation, sandboxing, kill switches and state rollback.

57. What should be logged for an agent?

At minimum, identity, user or sponsoring service, goal, plan steps, tool calls, parameters, approvals, memory changes, outputs, errors, state transitions and containment actions.

58. Does GAISSE permit fully autonomous agents?

GAISSE does not impose a universal prohibition. The permitted level of autonomy should be justified by risk, testing, safety, legal obligations, monitoring and available override or containment.

7. Physical AI and Safety

59. What is physical AI?

Physical AI is AI that perceives, controls or materially influences physical environments, devices, machinery, vehicles, robots or actuators.

60. Does GAISSE replace functional-safety standards?

No. GAISSE complements but does not replace sector-specific functional-safety, machinery, automotive, medical-device or other engineering standards.

61. What is a safe state?

A safe state is a defined condition that limits or prevents harm when normal operation cannot continue. The appropriate safe state depends on the system and environment.

62. Should safety constraints rely on the same AI model?

Where practicable, critical constraints should be enforced by deterministic or independently assured mechanisms rather than relying solely on the learned component being constrained.

63. What is required for human override?

Override should be accessible, reliable, independent where necessary, regularly tested, documented and capable of placing the system into a controlled state.

64. What evidence is expected for physical-AI systems?

Typical evidence includes hazard analysis, operational envelopes, simulation, hardware-in-the-loop tests, sensor and actuator validation, safe-state exercises, override tests, command logs, near-miss records and incident reconstruction data.

65. How should near misses be treated?

Near misses should be recorded and investigated because they reveal control weaknesses before harm occurs. They should feed corrective action and safety-case updates.

66. Could GAISST certification prove a physical system is safe?

No. Certification is not currently offered, and any future certification could only provide evidence of framework conformance within a defined scope. It could not replace product approval, specialist engineering judgement or sector safety certification.

67. How does GAISST relate to PAI-SF?

PAI-SFTM v1.0, the Physical AI Security Framework, is a separate ODA3 Institute framework with more granular physical-AI security controls. For a general AI security programme, GAISSTTM is used together with PAI-SFTM where physical AI is in scope; organisations needing physical-AI coverage only may use PAI-SFTM alone. GAISSTTM Domain 9 is not superseded. The mapping is set out in ODA3-2026-07-CSX-PAISF-004.

8. Evidence, Testing and Assurance

68. What counts as evidence?

Evidence may include policies, architecture, configuration, logs, approvals, test reports, evaluation outputs, tickets, incident records, supplier records, training, metrics, risk decisions and independent-assurance results.

69. Is a policy enough to satisfy a control?

Usually not. A policy shows design intent. Most controls also require implementation, recurring operation and evidence that the mechanism is effective.

70. What makes evidence strong?

Strong evidence is attributable, current, complete, scope-aligned, protected, reproducible where relevant, linked to the exact control and honest about limitations.

71. Can screenshots be used as evidence?

Yes, but screenshots alone are often weak. They should identify the system, date, scope, source and relevant configuration, and should be supported by stronger machine-generated or controlled records where possible.

72. How long should evidence be retained?

Retention depends on legal, contractual, assessment, incident and organizational requirements, and on any future certification requirements if a scheme is later issued. GAISSF does not prescribe one universal retention period.

73. Should failed test results be retained?

Yes. Failed, negative and inconclusive results are important evidence. Removing them can misrepresent assurance and obstruct root-cause analysis.

74. What is operating effectiveness?

Operating effectiveness means the control actually functions consistently in the assessed scope and period, not merely that it is designed or deployed.

75. What is the difference between assessment and certification?

Assessment evaluates conformance or readiness. Certification, if offered under a separately issued scheme, would be a formal decision under defined certification criteria and scope. GAISSF certification is not currently offered.

76. Can evidence from another framework be reused?

Yes, after verifying scope, currency, integrity and coverage. Reuse should not be based only on the fact that evidence was accepted in another audit.

77. Can automation replace assessor judgement?

Automation can improve consistency and coverage, but it cannot fully replace contextual judgement, interviews, design review, physical observation or evaluation of conflicting evidence.

78. What is the role of the Validation Test Specification?

A VTS defines how a control or control outcome should be tested, what inputs are required, what evidence is produced and how results are interpreted. It supports repeatability but does not eliminate professional judgement.

79. How should evidence integrity be protected?

Use controlled repositories, access restrictions, versioning, timestamps, hashes, signatures, immutable logging or chain-of-custody procedures according to risk.

9. Certification and Public Claims

Current position: Certification is not currently offered. The answers below explain how public claims should be framed today and how any future scheme would be expected to operate.

80. Does ODA3 Institute certify GAISSF implementations?

Not currently. Certification is not offered. Certification, accreditation and audit authority is reserved to ODA3 Institute (GEL v1.0 Section 10.5), and any future programme would require separately approved governance, criteria, assessment, appeals, registry and mark-use rules.

81. What would a GAISSF certificate mean?

No GAISSF certificates are currently issued. If a future scheme is established, a certificate should mean only what that scheme states for the named scope, profile, version and period. It should not be represented as a guarantee of safety, security, legality or future performance.

82. Could certification cover an entire enterprise?

Only if a future certified scope genuinely covered the entire enterprise. Otherwise, claims would need to identify the specific product, service, platform, business unit or system.

83. Can an organisation say it is GAISSF compliant?

It may make accurate factual alignment statements, such as "implements GAISSF control X" or "maps to GAISSF D4", which GEL v1.0 Section 10.3 permits. It must not make certification-like or endorsement claims; no certification is currently offered.

84. Can a vendor use the GAISSF name or mark?

Use of the GAISSF™ mark is governed by GEL v1.0 Section 9. Factual identification of the framework is permitted; using the mark in a product, service or domain name, or in a way that implies certification, sponsorship or endorsement, requires written authorisation from ODA3 Institute (Section 9.3).

85. Would GAISSF certification satisfy ISO certification?

No. GAISSF and ISO schemes are separate, and GAISSF certification is not currently offered. Mappings may show relationships, but one should never be represented as a substitute for the other.

86. Would GAISSF certification prove regulatory compliance?

No. Neither conformance nor any future certification could establish legal compliance, which depends on jurisdiction, facts, system use and regulator interpretation.

87. Could a future certification be suspended or withdrawn?

Yes. Any future scheme would define suspension and withdrawal for causes such as material nonconformity, scope misrepresentation, failed surveillance or misuse of marks.

88. What should public claims include?

They should identify the organisation or system, scope, GAISSF™ version, the controls or profile referred to, and relevant limitations. They should not state or imply certification, which is not currently offered.

89. What claims are prohibited?

Claims implying universal safety, zero risk, regulator endorsement, ISO equivalence, whole-enterprise certification from a narrow scope, or guaranteed legal compliance should not be made.

10. Relationship to Other Frameworks

90. How does GAISSF relate to ISO/IEC 42001?

ISO/IEC 42001 provides an AI management-system standard. GAISSF can complement it with detailed security, safety, technical and evidence-oriented controls. Neither should be presented as automatically equivalent to the other.

91. How does GAISSF relate to NIST AI RMF?

NIST AI RMF provides a risk-management structure and outcomes. GAISSF can translate those outcomes into a detailed control, evidence and assurance model.

92. How does GAISSF relate to NIST CSF?

NIST CSF provides broad cybersecurity outcomes. GAISSF extends the operating model into AI-specific model, data, agentic, harmful-output and physical-AI risks.

93. How does GAISSF relate to OWASP guidance?

OWASP resources provide important application, LLM and agentic threat knowledge and test guidance. GAISSF adds governance, lifecycle, evidence, assurance and supplier structures; any future certification scheme would be separately governed.

94. How does GAISSF relate to MITRE ATLAS and ATT&CK?

MITRE resources help identify adversary tactics and techniques. GAISSF uses threat knowledge to support control design and testing but adds normative control and evidence expectations.

95. How does GAISSF relate to CIS Controls?

CIS Controls provide a prioritized cybersecurity baseline. They can support many shared security mechanisms but do not cover the full AI-specific GAISSF scope.

96. Can an organization migrate from these frameworks?

Yes. GAISSF-IMP-012 provides a structured migration method based on inventory, normalization, semantic mapping, evidence reuse, gap assessment, transition waves and legacy-control retirement.

97. Does a crosswalk prove conformance?

No. A crosswalk shows a relationship between requirements. Conformance still requires implementation and evidence in the assessed scope.

11. Operations and Continuous Improvement

98. What happens after deployment?

The organization should operate control-health monitoring, model and data monitoring, incident response, supplier oversight, evidence refresh, exception review, management review and recurring assurance.

99. What is control health?

Control health is the current operating state of a control, commonly expressed as green, amber, red or unknown based on defined signals and thresholds.

100. How should model drift be handled?

Drift should be monitored against approved baselines. Threshold breaches should trigger investigation, re-evaluation, restriction, rollback or risk acceptance as appropriate.

101. What should happen if monitoring fails?

Loss of monitoring should be treated as a control issue. For high-risk systems, the organization may need to restrict capability, pause expansion, fail closed or revert to an observable state.

102. How should exceptions be managed?

Exceptions should identify the control, scope, reason, risk, compensating measures, owner, approver, expiry, monitoring and remediation plan.

103. What is continuous improvement in GAISSF?

It is the systematic use of incidents, test failures, metrics, audit findings, user feedback, supplier issues and threat intelligence to improve control design and operation.

104. How often should management review occur?

The frequency should reflect risk and tier. Quarterly and annual reviews are common, with event-driven review after material incidents, changes, or a GAISSF™ update or correction notice.

105. How should systems be retired?

Retirement should remove access and integrations, manage data, terminate suppliers, archive required evidence, update inventories and claims, and assign residual obligations.

12. Licensing, Copyright and Use

106. Can organizations use GAISSF internally?

Yes. Internal Use is permitted under GEL v1.0 at no cost (Sections 3.3 and 4). Internal Use means use solely within the organisation that produces no deliverable for any external party.

107. Can consultants use GAISSF with clients?

Only with a separate written commercial licence. Consulting, advisory, audit and assessment services, paid training, SaaS integration and client delivery are Commercial Use under GEL v1.0 (Section 3.4) and require a licence from ODA3 Institute (Sections 5.3 and 17).

108. Can the control catalogue be copied into another framework?

Unmodified or modified material may be redistributed non-commercially with attribution, a full licence notice and, for modifications, the mandatory disclaimer (GEL v1.0 Section 5.2). Derivative commercial frameworks are Commercial Use and require a licence.

109. Can GAISSF be used in software?

Software that implements, automates or is substantially derived from GAISSF™ control logic is a derivative work; distributing or deploying it commercially requires a commercial licence (GEL v1.0 Section 3.5). Independently written software that only interfaces with or references GAISSF™ falls under the Section 3.5 carve-out.

110. Can external standards bodies reference GAISSF?

Yes. Anyone may cite and reference GAISSF™ with attribution (GEL v1.0 Section 4). ODA3 Institute may also grant royalty-free licences to recognised standards development organisations where their IPR policies require it (Section 4, SDO carve-out).

111. Does citation imply endorsement?

No. Citation of GAISSF™ by another organisation, or of an external standard by GAISSF™, does not imply endorsement, affiliation or formal recognition. Factual alignment statements are not certification claims (GEL v1.0 Section 10.3).

13. Procurement, Suppliers and Customers

112. Can GAISSF be used in procurement?

Yes. Buyers may use GAISSF controls and profiles to define supplier requirements, due diligence, evidence expectations, contract clauses and ongoing monitoring.

113. Should every supplier be required to certify?

Not necessarily. Requirements should be proportionate to dependency and risk. Suppliers may provide evidence, contractual commitments or independent assurance; GAISSF certification is not currently offered.

114. What should customers ask for?

Customers should ask for exact scope, version, the applicable controls, evidence period, known limitations, supplier dependencies and incident-notification commitments.

115. What should suppliers avoid claiming?

Suppliers must not claim to be "GAISSE certified": no GAISSE certification is currently offered. Factual alignment statements should identify scope, version and the controls referred to.

116. How should inherited controls be documented?

Identify the provider, control outcome, evidence, contractual basis, limitations, monitoring, fallback and the responsibility retained by the customer.

117. Can supplier certifications be accepted as sufficient?

They may reduce effort, but should not automatically replace system-specific evidence, especially where integration, data use, configuration or customer operation changes the risk.

14. Common Misunderstandings

118. Is GAISSE just a checklist?

No. The controls require governance, architecture, operation, evidence, testing, assurance and improvement. A completed checklist without evidence is not conformance.

119. Does a higher maturity level excuse missing controls?

No. Maturity and conformance are different. Advanced monitoring cannot compensate for an unmet mandatory control unless an approved exception process permits a temporary deviation.

120. Is the Foundational profile only for low-risk AI?

Not necessarily. It is an adoption profile, not a declaration that the system is low risk. High-risk systems may require all controls and additional sector obligations.

121. Does passing a red-team exercise prove security?

No. Red teaming samples known scenarios and methods. It cannot prove the absence of unknown or low-frequency attacks.

122. Does transparency require revealing trade secrets?

Not automatically. Transparency should be meaningful and proportionate while respecting security, privacy, intellectual property and legal constraints.

123. Does human oversight always make an AI system safe?

No. Oversight can fail because of poor interface design, automation bias, insufficient authority, time pressure, lack of competence or unavailable evidence.

124. Can an organization outsource GAISSE accountability?

Activities may be outsourced, but accountability for the organization's system, users, obligations and risk generally remains with the organization.

125. Does zero incidents mean controls are effective?

Not necessarily. Incidents may be rare, under-detected or under-reported. Effectiveness should be evaluated using multiple evidence sources.

126. Is continuous monitoring required for every profile?

Monitoring is required according to applicable controls and risk. The Optimized profile adds more advanced and integrated continuous-monitoring expectations.

127. Can GAISSE eliminate AI risk?

No. It provides a structured way to reduce, detect, govern and evidence risk. Residual uncertainty and risk remain.

15. Escalation and Further Interpretation

128. Where should a technical implementation question be resolved?

Start with GAISSF-NOR-004, then consult GAISSF-IMP-010, IMP-011, IMP-013 and IMP-014. Document architecture decisions and unresolved assumptions.

129. Where should a profile or scope question be resolved?

Use GAISSF-NOR-001, the controlled profile register and the Applicable-Control Baseline. Escalate material ambiguity through framework governance.

130. Where should a certification claim question be resolved?

Use GEL v1.0 (Sections 9 and 10), the trademark policy and the public-claims guidance in this FAQ. Certification is not currently offered, so no certificate-specific decision applies.

131. How should an error in GAISSF documentation be reported?

Record the affected document, clause or control, the suspected defect, evidence, impact and proposed correction. Submit it through the controlled change or issue process.

132. How are new FAQ questions added?

Questions should be evaluated for recurrence, materiality and whether they reveal a normative ambiguity. Informative clarification may be added to the FAQ; requirement changes must follow formal change governance.

133. What should users do when the FAQ is silent?

Return to the normative requirements, document the interpretation used, identify assumptions, obtain appropriate legal or specialist advice where needed, and preserve the decision for review.

16. Legal, Regulatory and Public-Claim Questions

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

134. Does GAISSF create a legal safe harbour?

No. GAISSF does not establish statutory compliance, regulatory approval, immunity from enforcement, permission to operate or a defence to civil liability.

135. Does GAISST establish the legal standard of care?

No. A legal standard of care is determined by applicable law and facts. GAISST may be considered as one source of practice evidence, but conformance neither defines nor conclusively satisfies the legal standard.

136. Could certification prevent negligence claims or statutory fines?

No. Certification is not currently offered, and any future certification would be scoped and evidence-based. It could not prevent enforcement, litigation, contractual claims or findings about conduct inside or outside the assessed scope.

137. What is AI washing in the GAISST context?

AI washing includes inaccurate, exaggerated or insufficiently qualified claims about AI capability, autonomy, safety, security, compliance or certification. Public statements should identify the assessed entity, systems, GAISST™ version, applicable tier or controls, period, exclusions and limitations.

138. What happens when a GAISST control conflicts with law?

The organization should document the conflict, obtain competent legal review, restrict or redesign the activity where necessary, record the approved treatment and avoid claiming conformance for an unmet mandatory requirement unless the applicable scheme expressly permits that treatment. Conflicting laws or extraterritorial obligations may require suspension or withdrawal from an activity or jurisdiction.

139. Can a high-risk system select the Foundational profile merely because it is easier?

No. Convenience does not override the controlled profile definitions in GAISST-NOR-001, applicability decisions, contractual duties or legal requirements.

Annex A — Quick Reference by Audience

Audience	Start with	Then consult
Board/executive	NOR-002 Executive Summary	IMP-009 Adoption Guide and IMP-014 Operational Handbook
Program lead	IMP-009 Adoption Guide	IMP-010, IMP-011 and IMP-014
Architect	IMP-013 Reference Architecture	NOR-004 and IMP-010
Engineer/MLOps	IMP-010 Implementation Handbook	IMP-011, IMP-013 and IMP-014
Independent assessor/reviewer	NOR-001 and NOR-004	NOR-005, NOR-006 and evidence records
Legal/compliance	NOR-001, NOR-005 and NOR-006	IMP-012 and applicable laws
Procurement	NOR-004 and IMP-012	Supplier evidence and contractual terms
Operations/SOC	IMP-014 Operational Handbook	IMP-011 and incident procedures
Customer/public	NOR-002 and IMP-015	Scope, evidence limitations and public claims

Annex B — FAQ Maintenance Record

Field	Required content
FAQ ID	Unique question identifier
Question	Approved wording
Answer	Controlled response
Source documents	Normative and implementation references
Owner	Responsible subject-matter owner
Status	Draft, approved, superseded or withdrawn
Review trigger	GAISSE™ update or correction notice, legal change, recurring ambiguity or incident
Last reviewed	Date and reviewer

Annex C — Notably Absent

- No legal opinion or jurisdiction-specific compliance determination.
- No guarantee of certification, security, safety, reliability or market acceptance.
- No formal equivalence with ISO, NIST, OWASP, MITRE, CIS or any regulation.
- No permission to use GAISSE marks beyond applicable trademark and certification rules.
- No universal control implementation, threshold, evidence period or rollout duration.
- No replacement for sector-specific safety, quality, privacy, cybersecurity or product approval requirements.
- No market approval or permission-to-operate guarantee.
- No immunity from consumer-protection enforcement.
- No claim that mandatory local law always resolves every cross-border conflict without further analysis.
- No definition of conformance-profile membership; GAISSE-NOR-001 controls.
- No current certification programme.

Annex D — Source Traceability

FAQ subject	Controlled source
Framework and requirements	GAISSE-NOR-001 and GAISSE-NOR-004
Executive interpretation	GAISSE-NOR-002
Initial adoption	GAISSE-NOR-003 and GAISSE-IMP-009, where published and current
Terminology	GAISSE-NOR-005
External references	GAISSE-NOR-006
Release and historical status	GAISSE-NOR-007 and GAISSE-NOR-008

FAQ subject	Controlled source
Implementation and evidence	GAISST-IMP-010, where published and current
Deployment	GAISST-IMP-011, where published and current
Migration	GAISST-IMP-012, where published and current
Architecture	GAISST-IMP-013, where published and current
Operations	GAISST-IMP-014, where published and current

Annex E — Publication Record

Date	Change
29 June 2026	Initial full FAQ for GAISST TM v1.0.
05 October 2026	Corrected the framework name and canonical D1-D9 domain names; aligned the three conformance tiers and D9 applicability to GAISST-NOR-001; aligned certification answers to the current position (not offered); grounded licensing answers in GEL v1.0; replaced Statement of Applicability with Applicable-Control Baseline; added the PAI-SF TM relationship; moved legal and public-claim questions into the body; normalized independent-assessor terminology, update-notice wording, future-certification legal language and implementation-guide dependency status. No GAISST TM control was added, removed, renamed or amended.

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