

ODA3 INSTITUTE

EXECUTIVE SUMMARY

GAISSEF™ v1.0 Executive Summary

Global AI Safety and Security Framework

GAISSEF-NOR-002 | Informative | Final Publication Edition

Published 1 July 2026 | Updated 4 October 2026

© 2026 ODA3 Pvt Ltd

Document Control

Item	Value
Document title	GAISSF™ v1.0 Executive Summary
Document ID	GAISSF-NOR-002
Version	1.0
Status	Final Publication Edition
Classification	Informative
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
Authoritative source	GAISSF-NOR-001
Control baseline	59 controls across D1-D9
Foundational scope	52 controls (D1-D8)
Additional controls	7 conditional Physical AI controls (D9)
Supersedes	Earlier 45-control generated draft; withdrawn
Publication date	1 July 2026
Updated	4 October 2026

Copyright, Licensing and Reliance Notice

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute. GAISSF™ is used as the framework identifier. Use, reproduction, adaptation and trademark rights are governed by the applicable GAISSF publication terms and licensing instruments. Certification and credentials are not currently offered; any future rights or claims relating to them require a separately issued scheme or written authorization. This document does not constitute legal advice and does not guarantee security, safety, regulatory compliance, or absence of harmful outcomes.

Precedence Statement

This Executive Summary is informative. It does not establish, amend, replace or override any GAISSF requirement. GAISSF-NOR-001 is the authoritative normative source and prevails where inconsistency exists.

1. Executive Overview

GAISSF is an evidence-based AI safety and security framework comprising 59 controls across nine domains. Its Foundational profile consists of 52 canonical controls in D1-D8. The seven D9 Physical AI controls become additionally mandatory whenever an assessed system can influence or actuate the physical world. GAISSF provides a common structure for governance, technical implementation, evidence, assurance and controlled claims; it does not replace applicable law, sector-specific safety engineering or any separately issued certification scheme.

2. Business Rationale

AI risk is frequently divided across cybersecurity, model risk, data governance, privacy, safety, procurement, legal, compliance and internal audit. GAISSF provides common control identifiers, evidence expectations and assessment procedures so these functions can work from one auditable baseline.

3. Domain Architecture

Domain	Title	Controls	Foundational scope
D1	MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS	9	Yes
D2	RUNTIME SECURITY & ADVERSARIAL DEFENSE	6	Yes
D3	AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY	7	Yes
D4	SUPPLY CHAIN & THIRD-PARTY AI SECURITY	7	Yes
D5	CONTENT SAFETY & OUTPUT INTEGRITY	6	Yes
D6	GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT	7	Yes
D7	HUMAN & SOCIETAL HARMS	5	Yes
D8	REGULATORY ALIGNMENT & COMPLIANCE	5	Yes
D9	PHYSICAL AI SAFETY	7	Conditional — mandatory where Physical AI is in scope

4. What Adoption Requires

Executives must approve scope, ownership, resources, risk appetite, exception authority, residual-risk acceptance and assurance arrangements. Organizations must inventory AI systems, determine applicability for all 59 controls, implement the 52 canonical controls and every applicable D9 control, collect operating evidence, remediate findings and maintain continuing conformance after material change.

5. Conformance and Assessment

Tier	Scope	Executive implication
Foundational	52 canonical controls in D1-D8	Minimum canonical organizational and technical baseline
Operational	52 canonical controls plus all applicable D9 controls and operating-effectiveness evidence	Adds Physical AI controls whenever cyber-physical actuation is in scope
Optimized	Same applicable control scope plus continuous monitoring and sustained higher-assurance evidence	Requires continuous assurance and stronger evidence over time

Certification is not currently offered. GAISSF-NOR-001 defines conformance and assessment requirements; it does not authorize certification, certification marks, accredited status or public claims of certification. If ODA3 later issues a GAISSF certification scheme, any certificate would represent a scoped assessment against the separately issued scheme requirements and evidence. No certificate would guarantee security, safety, legal compliance or absence of harmful outcomes.

6. Evidence and Assurance

Policy documents alone are insufficient. Evidence should demonstrate design, implementation, operation, monitoring and corrective action. Executives should expect traceability from every applicable control to a responsible owner, evidence artifact, test result, exception or remediation record.

7. Executive Decisions

Decision	Required outcome
Assessment boundary	Approved systems, entities, locations, services and dependencies
Conformance target	Foundational, Operational or Optimized
Control ownership	Named accountable and operational owners
Risk authority	Defined exception and residual-risk approval levels
Assurance / future certification intent	Approved assurance scope and public claims; future certification only under a separately issued scheme
Continuing conformance	Monitoring, change triggers, reassessment and remediation governance

8. Benefits and Limitations

Potential benefits include clearer accountability, more consistent technical and governance controls, better audit readiness, stronger evidence discipline and improved coordination. Outcomes depend on scope quality, implementation competence, evidence integrity and sustained operation. GAISSF is not a substitute for law, specialist safety engineering, privacy assessment, sector standards or system-specific testing.

9. Notably Absent

GAISSF does not provide universal performance thresholds, universal risk-acceptance thresholds, automatic regulatory equivalence, current certification, regulator endorsement, or authorization to use certification marks. Detailed framework mappings require controlled crosswalk artifacts. Any future certification would require a separately issued scheme, assessment rules and claims policy.

Control Index

Control ID	Control title	Domain	Foundational scope
D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS	Yes
D1-CTL-02	MODEL EXTRACTION RESISTANCE	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS	Yes
D1-CTL-03	BEHAVIORAL DRIFT DETECTION	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS	Yes
D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS	Yes
D1-CTL-05	EMBEDDING SPACE ROBUSTNESS	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS	Yes
D1-CTL-06	POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS	Yes
D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS	Yes
D1-CTL-08	MODEL MERGE ATTACK DETECTION	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS	Yes

Control ID	Control title	Domain	Foundational scope
D1-CTL-09	QUANTIZATION BACKDOOR SCREENING	D1: MODEL INTEGRITY & ADVERSARIAL ROBUSTNESS	Yes
D2-CTL-01	DIRECT PROMPT INJECTION PREVENTION	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE	Yes
D2-CTL-02	INDIRECT PROMPT INJECTION PREVENTION	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE	Yes
D2-CTL-03	JAILBREAK RESISTANCE TESTING	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE	Yes
D2-CTL-04	MULTI-MODAL INJECTION DEFENSE	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE	Yes
D2-CTL-05	FUNCTION CALL/TOOL CALL INJECTION PREVENTION	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE	Yes
D2-CTL-06	CROSS-CONTEXT HIJACKING MITIGATION	D2: RUNTIME SECURITY & ADVERSARIAL DEFENSE	Yes
D3-CTL-01	LEAST AGENCY ENFORCEMENT	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY	Yes
D3-CTL-02	INTER-AGENT COMMUNICATION SECURITY	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY	Yes
D3-CTL-03	AGENTIC PROMPT CHAINING DETECTION	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY	Yes
D3-CTL-04	EMBODIED AI SAFETY CONTROLS	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY	Yes
D3-CTL-05	MULTI-AGENT TRUST CHAIN ATTESTATION	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY	Yes
D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY	Yes
D3-CTL-07	SECURE MEMORY LIFECYCLE MANAGEMENT	D3: AGENTIC RISK & AUTONOMOUS SYSTEM SECURITY	Yes
D4-CTL-01	AI BILL OF MATERIALS (AI BOM) MAINTENANCE	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY	Yes
D4-CTL-02	MODEL FILE & ARTIFACT SCANNING	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY	Yes
D4-CTL-03	MODEL HUB & REGISTRY VETTING	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY	Yes
D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY	Yes
D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY	Yes
D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY	Yes
D4-CTL-07	AI SOFTWARE COMPOSITION ANALYSIS (SCA)	D4: SUPPLY CHAIN & THIRD-PARTY AI SECURITY	Yes
D5-CTL-01	HARMFUL CONTENT BLOCKING	D5: CONTENT SAFETY & OUTPUT INTEGRITY	Yes
D5-CTL-02	PII LEAKAGE PREVENTION	D5: CONTENT SAFETY & OUTPUT INTEGRITY	Yes
D5-CTL-03	COPYRIGHT DETECTION	D5: CONTENT SAFETY & OUTPUT INTEGRITY	Yes
D5-CTL-04	AI WATERMARKING ROBUSTNESS	D5: CONTENT SAFETY & OUTPUT INTEGRITY	Yes
D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION	D5: CONTENT SAFETY & OUTPUT INTEGRITY	Yes
D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION	D5: CONTENT SAFETY & OUTPUT INTEGRITY	Yes
D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT	Yes
D6-CTL-02	AUDIT TRAIL COMPLETENESS	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT	Yes
D6-CTL-03	AI MODEL CARD COMPLETENESS	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT	Yes
D6-CTL-04	AI INCIDENT RESPONSE READINESS	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT	Yes
D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT	Yes
D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT	Yes
D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY	D6: GOVERNANCE, ACCOUNTABILITY & HUMAN OVERSIGHT	Yes
D7-CTL-H01	AI-GENERATED PHISHING SIMULATION	D7: HUMAN & SOCIETAL HARMS	Yes
D7-CTL-H02	DEEPFAKE DETECTION TRAINING	D7: HUMAN & SOCIETAL HARMS	Yes
D7-CTL-H03	OUT-OF-BAND AUTHENTICATION	D7: HUMAN & SOCIETAL HARMS	Yes

Control ID	Control title	Domain	Foundational scope
D7-CTL-H04	AI SOCIAL ENGINEERING IR	D7: HUMAN & SOCIETAL HARMS	Yes
D7-CTL-H05	AI-ENHANCED EXTERNAL ATTACK DEFENSE	D7: HUMAN & SOCIETAL HARMS	Yes
D8-CTL-01	EU AI ACT RISK TIER MAPPING	D8: REGULATORY ALIGNMENT & COMPLIANCE	Yes
D8-CTL-02	ISO 42001 GAP ANALYSIS	D8: REGULATORY ALIGNMENT & COMPLIANCE	Yes
D8-CTL-03	GPAI TECHNICAL DOCUMENTATION VERIFICATION	D8: REGULATORY ALIGNMENT & COMPLIANCE	Yes
D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	D8: REGULATORY ALIGNMENT & COMPLIANCE	Yes
D8-CTL-05	NIST SP 800-218A COMPLIANCE CHECK	D8: REGULATORY ALIGNMENT & COMPLIANCE	Yes
D9-CTL-01	PHYSICAL HARM BOUNDARY ENFORCEMENT	D9: PHYSICAL AI SAFETY	Conditional — mandatory where physical AI is in scope
D9-CTL-02	SAFE STATE AND GRACEFUL DEGRADATION	D9: PHYSICAL AI SAFETY	Conditional — mandatory where physical AI is in scope
D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP	D9: PHYSICAL AI SAFETY	Conditional — mandatory where physical AI is in scope
D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION	D9: PHYSICAL AI SAFETY	Conditional — mandatory where physical AI is in scope
D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	D9: PHYSICAL AI SAFETY	Conditional — mandatory where physical AI is in scope
D9-CTL-06	ACTUATOR COMMAND VERIFICATION	D9: PHYSICAL AI SAFETY	Conditional — mandatory where physical AI is in scope
D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	D9: PHYSICAL AI SAFETY	Conditional — mandatory where physical AI is in scope

Annex A — Executive Source Traceability

Executive topic	Normative source
59-control architecture	GAISSF-NOR-001, Framework Architecture and Control Catalogue
52-control Foundational scope	GAISSF-NOR-001, Conformance and Assessment; Annex A
Conditional D9 controls	GAISSF-NOR-001, D9; Statement of Applicability; Annex A
Evidence requirements	GAISSF-NOR-001, Evidence Requirements
Certification limitations	GAISSF-NOR-001, Conformance and Assessment; Certification launch restriction

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, or treated D9 as universally mandatory or universally excluded, is superseded. D9 applicability must be determined and justified for every assessed scope.

Executive Decision Framework

Executives should treat GAISSF adoption as an enterprise risk and operating-model decision. The essential questions are whether the organization knows where AI is used, understands material consequences, has accountable owners, operates effective controls, can produce evidence and can respond when assumptions fail.

Executive question	Required evidence
What is in scope?	Approved AI inventory, scope statement and supplier map.
Who is accountable?	Named executive, system and control owners.
What can go wrong?	Risk, threat, impact and hazard assessments.
Are controls operating?	Current control-health and assurance evidence.
What remains unresolved?	Exceptions, findings, incidents and residual-risk decisions.
What is claimed externally?	Approved conformance and public-claim register; certification claims only if a future issued scheme authorizes them.

Board and Executive Oversight Agenda

- Material changes in AI scope and risk exposure
- Red or unknown control-health states
- Significant incidents, near misses and harmful outcomes
- Overdue corrective actions and expiring exceptions
- Supplier and regulatory changes
- Conformance and public-claim accuracy; future certification status only if a scheme is issued

- Resources, competence and improvement priorities

Implementation Priorities by Horizon

Horizon	Priority
First 30 days	Sponsor, inventory, scope, high-risk containment and programme charter.
Days 31-90	Profile selection, baseline assessment, ownership, roadmap and evidence repository.
Months 4-6	Critical remediation, technical validation and operating evidence.
Months 7-12	Independent assurance and management review; consider any future certification path only if a GAISSF certification scheme has been launched.
Ongoing	Monitoring, incident learning, supplier oversight and release migration.

Publication Completeness and Intended Use

This publication edition of GAISSF-NOR-002 is designed to stand on its own as executive interpretation and decision support. It summarizes purpose, scope, governance, adoption decisions, evidence expectations, limitations and implementation priorities, but GAISSF-NOR-001 remains the authoritative normative source.

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.

Revision Note — 4 October 2026

Reconciled to the locked GAISSF-NOR-001 v1.0 publication edition. Updated the canonical framework name and mark treatment, preserved the 59-control / 52+D9 architecture, aligned conformance terminology to NOR-001, made the current certification boundary explicit, updated executive decision and oversight wording, corrected source-traceability references, added the update date, and applied the standard ODA3 public cover and page numbering. No normative requirement is created or changed by this informative document.