

ODA3 INSTITUTE

QUICK START GUIDE

GAISSEF™ v1.0 Quick Start Guide

Global AI Safety and Security Framework

GAISSEF-NOR-003 | 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 Quick Start Guide
Document ID	GAISSF-NOR-003
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Supersedes	Earlier 45-control generated draft; withdrawn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 guide provides implementation guidance only. It does not create or modify GAISSF requirements. GAISSF-NOR-001 is the authoritative normative source and prevails where inconsistency exists. GAISSF-NOR-004 is a companion control catalogue where published, but it does not override NOR-001.

1. Rapid Onboarding Sequence

Step	Action
1	Appoint an executive sponsor and implementation lead.
2	Define the organizational, system, data, supplier and deployment boundary.
3	Create an inventory of AI systems and dependencies.
4	Select the target conformance tier.
5	Prepare a 59-control Statement of Applicability.
6	Assess the 52 canonical Foundational controls first.
7	Determine whether physical-world influence, cyber-physical actuation, or safety-relevant autonomous control is within scope. If so, assess all applicable D9 controls as mandatory additions to the selected baseline.
8	Assign control owners and evidence custodians.
9	Perform evidence-based gap assessment and remediation.
10	Conduct an internal readiness review before any independent assessment.

2. Scope Decision

Document legal entities, business units, AI systems, models, datasets, agents, tools, APIs, third parties, interfaces, environments and excluded components. An exclusion should be supported by a risk-based justification and should not remove a dependency that materially affects the assessed system.

3. Select the Conformance Path

Path	Controls / evidence	Use
Foundational	52 canonical controls in D1-D8	Canonical starting baseline; add D9 controls where Physical AI is in scope
Operational	Same applicable control scope as Foundational, plus operating-effectiveness evidence	Demonstrates control operation over an appropriate period and event population
Optimized	Same applicable control scope, plus continuous monitoring and sustained higher-assurance evidence	Higher-assurance sustained operation over time

The seven D9 controls are not part of the canonical 52-control Foundational scope. They become additional mandatory controls whenever Physical AI, robotics, autonomous actuation, operational technology or other cyber-physical effects are within the assessed scope. Operational and Optimized do not automatically expand a non-physical-AI scope to all 59 controls; they apply stronger evidence expectations to the same applicable control scope.

4. Build the Statement of Applicability

Required field	Example
Control ID	D1-CTL-01
Applicability	Applicable
Justification	Training data used within assessed boundary
Implementation status	Implemented / Partially implemented / Not implemented
Evidence reference	EVD-D1-01-001
Owner	Model Security Lead
Exception or risk acceptance	None / reference
Last review	YYYY-MM-DD

5. Evidence Starter Set

Create an evidence index that links each applicable control to policies, system records, configurations, logs, test results, approvals, supplier records, incident records and corrective actions. Preserve original timestamps, signatures, hashes and chain-of-custody information where relevant.

6. First 30/60/90 Days

Period	Priority outcomes
Days 1-30	Sponsor, scope, inventory, tier decision, SoA structure and owners
Days 31-60	Gap assessment, evidence collection, priority remediation and exception governance
Days 61-90	Operating evidence, internal testing, corrective actions and readiness review

7. Common Failure Modes

Common failures include counting policies as operating evidence, omitting supplier dependencies, treating the 52-control Foundational scope as optional sampling, ignoring D9 applicability, using maturity scores to conceal nonconformity, accepting indefinite exceptions, and making public conformance claims broader than the assessed boundary. Certification claims are not currently available and may be made only under any future separately issued scheme.

8. Foundational Control Checklist — 52 Controls

Control ID	Control title	Owner	Status	Evidence reference
D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION			
D1-CTL-02	MODEL EXTRACTION RESISTANCE			
D1-CTL-03	BEHAVIORAL DRIFT DETECTION			
D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION			
D1-CTL-05	EMBEDDING SPACE ROBUSTNESS			
D1-CTL-06	POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING			
D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION			
D1-CTL-08	MODEL MERGE ATTACK DETECTION			
D1-CTL-09	QUANTIZATION BACKDOOR SCREENING			
D2-CTL-01	DIRECT PROMPT INJECTION PREVENTION			
D2-CTL-02	INDIRECT PROMPT INJECTION PREVENTION			
D2-CTL-03	JAILBREAK RESISTANCE TESTING			
D2-CTL-04	MULTI-MODAL INJECTION DEFENSE			

Control ID	Control title	Owner	Status	Evidence reference
D2-CTL-05	FUNCTION CALL/TOOL CALL INJECTION PREVENTION			
D2-CTL-06	CROSS-CONTEXT HIJACKING MITIGATION			
D3-CTL-01	LEAST AGENCY ENFORCEMENT			
D3-CTL-02	INTER-AGENT COMMUNICATION SECURITY			
D3-CTL-03	AGENTIC PROMPT CHAINING DETECTION			
D3-CTL-04	EMBODIED AI SAFETY CONTROLS			
D3-CTL-05	MULTI-AGENT TRUST CHAIN ATTESTATION			
D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION			
D3-CTL-07	SECURE MEMORY LIFECYCLE MANAGEMENT			
D4-CTL-01	AI BILL OF MATERIALS (AI BOM) MAINTENANCE			
D4-CTL-02	MODEL FILE & ARTIFACT SCANNING			
D4-CTL-03	MODEL HUB & REGISTRY VETTING			
D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING			
D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT			
D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE			
D4-CTL-07	AI SOFTWARE COMPOSITION ANALYSIS (SCA)			
D5-CTL-01	HARMFUL CONTENT BLOCKING			
D5-CTL-02	PII LEAKAGE PREVENTION			
D5-CTL-03	COPYRIGHT DETECTION			
D5-CTL-04	AI WATERMARKING ROBUSTNESS			
D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION			
D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION			
D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS			
D6-CTL-02	AUDIT TRAIL COMPLETENESS			
D6-CTL-03	AI MODEL CARD COMPLETENESS			
D6-CTL-04	AI INCIDENT RESPONSE READINESS			
D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING			
D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE			
D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY			
D7-CTL-H01	AI-GENERATED PHISHING SIMULATION			
D7-CTL-H02	DEEPFAKE DETECTION TRAINING			
D7-CTL-H03	OUT-OF-BAND AUTHENTICATION			
D7-CTL-H04	AI SOCIAL ENGINEERING IR			
D7-CTL-H05	AI-ENHANCED EXTERNAL ATTACK DEFENSE			
D8-CTL-01	EU AI ACT RISK TIER MAPPING			
D8-CTL-02	ISO 42001 GAP ANALYSIS			
D8-CTL-03	GPAI TECHNICAL DOCUMENTATION VERIFICATION			

Control ID	Control title	Owner	Status	Evidence reference
D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)			
D8-CTL-05	NIST SP 800-218A COMPLIANCE CHECK			

9. Additional Physical-AI Checklist — 7 Controls

Control ID	Control title	Applicability decision	Status	Evidence reference
D9-CTL-01	PHYSICAL HARM BOUNDARY ENFORCEMENT			
D9-CTL-02	SAFE STATE AND GRACEFUL DEGRADATION			
D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP			
D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION			
D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING			
D9-CTL-06	ACTUATOR COMMAND VERIFICATION			
D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION			

10. Independent Assessment Readiness Gate

Do not proceed to an independent assessment until scope is approved, all applicable controls are represented in the SoA, required evidence is available, tests have been executed, material gaps are closed or explicitly bounded, exceptions are valid and time-bound, and public claims are controlled. Certification is not currently offered. If ODA3 later issues a GAISSF certification scheme, any certification assessment or certification claim must follow that separately issued scheme, its assessment rules and its claims policy.

Annex A — Complete 59-Control Reference

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
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

Control ID	Control title	Domain	Foundational scope
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	DEEPPAKE DETECTION TRAINING	D7: HUMAN & SOCIETAL HARMS	Yes
D7-CTL-H03	OUT-OF-BAND AUTHENTICATION	D7: HUMAN & SOCIETAL HARMS	Yes
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	No — apply where physical AI is in scope
D9-CTL-02	SAFE STATE AND GRACEFUL DEGRADATION	D9: PHYSICAL AI SAFETY	No — apply where physical AI is in scope
D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP	D9: PHYSICAL AI SAFETY	No — apply where physical AI is in scope
D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION	D9: PHYSICAL AI SAFETY	No — apply where physical AI is in scope
D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	D9: PHYSICAL AI SAFETY	No — apply where physical AI is in scope
D9-CTL-06	ACTUATOR COMMAND VERIFICATION	D9: PHYSICAL AI SAFETY	No — apply where physical AI is in scope
D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	D9: PHYSICAL AI SAFETY	No — apply where physical AI is in scope

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

Complete Quick-Start Sequence

Step	Action	Output
1	Appoint sponsor and program lead	Approved mandate and charter
2	Create AI inventory	System, model, data, agent and supplier register
3	Define scope	Approved organizational and system boundary
4	Select conformance profile	Version-controlled profile and SoA
5	Assign owners	RACI and control-owner register
6	Assess all applicable controls	Gap and risk register
7	Contain critical exposure	Interim safeguards and executive decisions
8	Build remediation roadmap	Funded plan with owners and dates
9	Establish evidence repository	Evidence index and retention rules
10	Operate and monitor	Control-health dashboard and incidents
11	Perform internal assurance	Readiness report and corrective actions
12	Decide independent assessment path	Approved external-assessment plan; future certification only if a scheme is issued

First Assessment Workshop

- Bring system, security, data, legal, risk, privacy, safety, procurement and operations representatives.
- Review scope before discussing scores.
- Use exact control text and evidence requirements from the authoritative normative source.
- Record disagreements and assumptions rather than forcing consensus.
- End with owners, actions, dates and escalation decisions.

Minimum Viable Evidence Pack

Evidence class	Minimum examples
Governance	Charter, scope, inventory, RACI and risk decisions
Architecture	Data flows, trust boundaries, model and supplier dependencies
Technical	Configurations, evaluation results, scans, logs and release records
Operational	Tickets, reviews, incidents, access records and monitoring
Assurance	Test plan, samples, findings, corrective actions and management review

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.

Publication Completeness and Intended Use

This publication edition of GAISSF-NOR-003 is designed to stand on its own for its stated role: rapid but complete onboarding and initial adoption sequence. It includes scope, operating guidance, evidence expectations, 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. GAISSF-NOR-001 remains the authoritative normative source. Other GAISSF companion documents remain part of the controlled document system only to the extent they are published and current.

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, escalation and reusable records.
Traceability	Preserves the distinction between normative requirements, implementation guidance and examples.
Limitations	States what the guide does not establish or guarantee.
Maintenance	Includes review triggers, change control and publication status.

Evidence-State and Reassessment Rules

Configuration, policy, architecture and deployment records demonstrate design or implementation. They do not, by themselves, demonstrate sustained operating effectiveness. Period-of-operation evidence shall cover a duration and event population appropriate to the control, risk, deployment stage and assessment objective; no universal 30-day threshold applies to every control.

Material changes to the assessed system, model, data, prompts, tools, privileges, deployment context, suppliers, interfaces, intended use or physical-actuation capability shall trigger documented impact analysis. Where applicability, risk, implementation or evidence requirements may have changed, the affected Statement of Applicability entries shall be reassessed.

Revision Note — 4 October 2026

Reconciled to the locked GAISSF-NOR-001 v1.0 publication edition. Corrected the canonical framework name and mark treatment; preserved the 59-control / 52+D9 architecture; corrected Operational and Optimized scope so D9 remains applicability-driven rather than universally mandatory; changed certification-readiness language to independent-assessment readiness with the current certification boundary stated explicitly; made NOR-001 the sole authoritative source; retained NOR-004 only as a companion where published; updated the Quick-Start sequence, public-claim wording, cover and page numbering. No normative requirement is created or changed by this informative guide.