

ODA3 INSTITUTE

IMPLEMENTATION GUIDANCE

GAISSF™ v1.0 Operational Handbook

Run-state operations, monitoring, assurance and continuous improvement

GAISSF-IMP-014 | Public

© ODA3 Pvt Ltd

Document Control

Document ID	GAISST-IMP-014
Title	GAISST TM v1.0 Operational Handbook
Doc Type	Implementation guidance — informative
Purpose	A repeatable operating model for monitoring, maintaining and improving GAISST TM controls after deployment
Primary Audience	System owners, security operations, AI operations, MLOps, platform teams, risk, compliance, safety, incident response, internal audit and control owners
Dependencies	GAISST-NOR-001 to GAISST-NOR-008; GAISST-IMP-009 to GAISST-IMP-013, where published and current
Precedence	GAISST-NOR-001 (Framework Standard) and GAISST-NOR-004 (Control Catalogue) prevail
Control Baseline	59 controls across nine domains
Status	Final Publication
Publish Date / Review Cycle	Issued 29 June 2026; updated 05 October 2026; review on material change to GAISST-NOR-001 or GAISST-NOR-004
Contact	contact@oda3.org
Classification	Public

GAISSTTM v1.0 Operational Handbook

Run-state operations, monitoring, assurance and continuous improvement

Reliance notice: This handbook supports run-state operations. It does not replace the normative framework, system-specific runbooks, incident procedures, safety case, legal obligations or approved risk decisions. Operational monitoring reduces uncertainty but cannot prove the absence of unknown threats, emergent behaviour, rare failures or harmful outcomes. This handbook is not legal, regulatory, safety, engineering, certification or audit advice, and does not define conformance-profile membership (see GAISST-NOR-001). Certification is not currently offered.

How to Use This Document

Reader	Recommended use
Executive or board reader	Review purpose, decision rights, legal and regulatory integration, limitations and Notably Absent sections.
Program or control owner	Use workflows, templates, gates, evidence fields and escalation criteria as implementation aids.
Engineering or operations team	Translate guidance into system-specific procedures, configurations, runbooks and testable acceptance criteria.

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

Foreword

Deployment is the beginning of operational assurance, not its conclusion. AI systems, data, suppliers, users, threats and legal obligations change continuously. This handbook defines a practical operating rhythm for control health, monitoring, incident response, evidence maintenance, management review and improvement.

1. Purpose and Scope

This handbook applies to AI systems in pilot, limited-production and general-production states. It covers daily operations, control monitoring, service management, change detection, incidents, exceptions, supplier oversight, evidence refresh, assurance, management review and retirement.

Organizations should tailor the operating model according to system criticality, autonomy, physical consequences, data sensitivity, user population, regulatory exposure and conformance profile.

2. Operational Objectives

Objective	Expected operating outcome
Maintain control effectiveness	Controls continue to operate as designed across the assessed scope.
Detect material change	Model, data, architecture, supplier, user and threat changes trigger review.
Detect degradation and misuse	Behavior, security, safety and service anomalies are identified and triaged.
Preserve evidence	Operating records remain current, attributable, complete and reviewable.
Respond proportionately	Incidents, exceptions and nonconformities receive risk-based treatment.
Sustain accountability	Owners, approvers and escalation routes remain active.
Improve systematically	Incidents, findings, metrics and near misses drive corrective and preventive action.

3. Operational Governance Model

Role	Run-state accountability
Executive sponsor	Resolve material risk, funding and scope issues
System owner	Own approved use, service risk and operational acceptance
Control owner	Maintain control design and effectiveness
Control operator	Execute recurring control activities and create evidence

Role	Run-state accountability
AI operations / MLOps	Maintain models, data pipelines, evaluations and deployment state
Security operations	Monitor threats, alerts, abuse and compromise
Safety authority	Oversee hazards, safe state and physical-AI constraints
Data/privacy owner	Maintain data use, retention, rights and leakage controls
Supplier manager	Track provider status, changes, incidents and inherited controls
Internal assurance	Independently test control operation and evidence
Risk authority	Approve exceptions and residual risk within delegated authority

4. Operating Cadence

Cadence	Minimum activities
Continuous	Security telemetry, safety alerts, control-health signals, abuse detection, service availability and physical operating constraints
Per transaction/action	Authorization, policy decision, tool approval, safety gate and evidence capture
Daily	Alert triage, incident review, failed-control follow-up and high-risk exception review
Weekly	Model/data drift review, unresolved alerts, supplier status and deployment changes
Monthly	Control-owner review, evidence expiry, overdue findings, exception status and metric trends
Quarterly	Control attestation, risk review, technical reassessment and management reporting
Semiannual	Scenario exercise, independent assurance and supplier deep review
Annual	Scope confirmation, full profile review, internal audit, management review and release-impact assessment
Event-driven	Incident, major change, legal change, supplier change, new threat or GAISST TM update notice

4.1 Detailed run-state procedures

Procedure	Trigger	Steps	Evidence
Daily control-health review	Start of operating day or continuous shift	Review red/unknown states, assign actions, escalate material issues	Daily review record
Model drift review	Threshold breach or weekly cadence	Validate signal, compare baseline, assess impact, restrict or re-evaluate	Drift investigation
Alert triage	Actionable alert	Acknowledge, classify, investigate, contain, close or escalate	Alert timeline and decision

Procedure	Trigger	Steps	Evidence
Evidence expiry review	Monthly or expiry warning	Identify artifact, assess coverage gap, refresh or exception	Evidence refresh record
Supplier change review	Provider notice or detected change	Assess scope, re-evaluate, update assumptions and approve	Supplier impact record
Management review	Quarterly/annual	Review scope, health, incidents, resources and actions	Approved minutes and decisions

4.2 Shift and on-call handover

- Open critical/high alerts and incidents
- Red/unknown control states
- Temporary restrictions and active exceptions
- Recent model, data, supplier or configuration changes
- Pending evidence preservation or notification
- Named decision owners and next checkpoints

Runbooks should cover detection, containment, preservation, investigation, recovery, validation, communication, legal escalation and recurrence prevention. Shift handover should review new red states, critical alerts, open incidents, active holds, regulatory clocks, degraded controls and pending approvals.

5. Operational Inventory and Baseline

Run-state operations require an authoritative baseline describing what is approved and currently deployed.

Baseline item	Minimum record
System	Name, purpose, owner, users, criticality and lifecycle state
Model	Provider, model/version, configuration and approval status
Data	Sources, classifications, lineage, retention and locations
Prompts/policies	Approved versions and release identifiers
Agents/tools	Capabilities, permissions, limits and sponsoring identity
Infrastructure	Environment, network, secrets, compute and regions
Suppliers	Critical services, contracts, contacts and inherited controls
Control profile	Applicable GAISSF controls and exceptions
Evidence period	Start, end and repository status
Public claims	Approved scope and representations

6. Control-Health Monitoring

Health state	Meaning	Required response
Green	Control operates within approved thresholds	Continue monitoring
Amber	Degradation, evidence weakness or repeated minor failure	Investigate and implement time-bound action
Red	Material failure, missing evidence or control bypass	Contain, escalate and assess nonconformity
Unknown	Telemetry or evidence is unavailable	Treat according to risk; restrict operation where necessary

6.1 Control-health record

Field	Required content
Control ID	Exact GAISST identifier
System/scope	Affected component or population
Signal	Metric, alert, test or observation
Threshold	Approved expected range
State	Green, amber, red or unknown
Owner	Accountable control owner
Action	Investigation, containment or improvement
Evidence	Linked artifact or event
Review date	Next review or expiry

6.2 Worked example: monthly control review

Example: D3 agent tool authorization is rated Amber after two denied actions were not logged. The owner confirms the authorization control still blocked the actions, but the evidence pipeline was incomplete. A seven-day corrective action is opened to repair logging, backfill available records, test alert routing and verify no other tools are affected. The control remains Amber until the retest passes; the evidence record notes the limitation.

7. Monitoring Architecture

Monitoring plane	Signals
Security	Authentication, authorization, exploit attempts, abuse, secrets, dependency and infrastructure events
Model behavior	Output distribution, refusal, harmful-output, robustness and performance changes
Data	Source change, lineage, quality, drift, poisoning indicators, leakage and retention
Agentic activity	Plans, tool calls, delegation, transaction limits, loop behavior and approvals

Monitoring plane	Signals
User and human factors	Complaints, overrides, confusion, recourse, misuse and accessibility
Supplier	Availability, model changes, incidents, contract notifications and assurance reports
Physical safety	Sensor faults, actuation bounds, override, emergency stop, near miss and safe-state events
Control evidence	Missing, stale, incomplete or inconsistent artifacts

7.1 Alert design

1. Define the risk condition represented by each alert.
2. Specify source, threshold, severity, owner and response time.
3. Distinguish informational signals from actionable alerts.
4. Test alert generation, routing, acknowledgement and escalation.
5. Monitor false positives, false negatives and unreviewed alerts.
6. Retain alert decisions and closure evidence.

8. Model and Data Operations

Operational area	Required practices
Model version	Pin approved version; detect provider or package changes
Evaluation baseline	Maintain comparable security, safety and performance tests
Drift	Monitor input, embedding, output, error and outcome distributions
Data source	Review source additions, changes, licence, quality and integrity
Retrieval	Monitor index freshness, unauthorized access and poisoned content
Memory	Review retention, tenant isolation, contamination and deletion
Feedback	Control human and automated feedback used for adaptation
Rollback	Maintain known-good model, data and configuration states

8.1 Re-evaluation triggers

- Model or provider version change
- Material prompt, orchestration or policy change
- New data source or material data distribution change
- New agent, tool or external action
- New jurisdiction, user group or high-impact use
- Incident, near miss or repeated harmful output
- Supplier notification or assurance deterioration
- Material threat-intelligence update

9. Agentic AI Operations

Operational control	Run-state activity
Identity	Track each agent instance and sponsoring principal
Goals	Review approved objective classes and prohibited objectives
Plans	Monitor step count, plan depth, loops and unexpected delegation
Tools	Review allowlists, permissions, parameters and denied actions
Transactions	Monitor value, frequency, destination and approval thresholds
Memory	Review contamination, retention and cross-user leakage
Containment	Test circuit breaker, kill switch and credential revocation
Evidence	Retain plans, tool calls, approvals, state changes and outcomes

10. Physical AI Operations

Area	Run-state requirement
Operational envelope	Monitor speed, load, location, proximity and environmental limits
Sensor health	Track calibration, disagreement, degradation and missing signals
Safety supervisor	Verify independent constraints and blocked-command records
Override	Test accessibility, response time and independent operation
Safe state	Exercise transition and recovery procedures
Maintenance	Control software, model, sensor and actuator changes
Near misses	Capture and investigate events before harm occurs
Incident reconstruction	Preserve synchronized telemetry and command history

11. Operational Runbooks by Domain

Domain	Routine run-state activities
D1 — Model Integrity & Adversarial Robustness	Dataset provenance and poisoning checks, behavioural drift review, model-signing verification, adapter, merge and quantization screening, extraction monitoring
D2 — Runtime Security & Adversarial Defense	Direct and indirect prompt-injection, jailbreak and multimodal attack telemetry; tool-call injection and cross-context hijacking monitoring; regression tests
D3 — Agentic Risk & Autonomous System Security	Least-agency permission review, inter-agent communication security, prompt-chaining detection, multi-agent attestation, memory exfiltration and lifecycle checks
D4 — Supply Chain & Third-Party AI Security	AI-BOM upkeep, model file and artifact scanning, registry vetting, MCP server behavioural monitoring, third-party API review, shadow AI discovery, software composition analysis

Domain	Routine run-state activities
D5 — Content Safety & Output Integrity	Harmful-content blocking, PII leakage, copyright detection, watermarking robustness, privacy-by-design and privacy-preserving ML checks
D6 — Governance, Accountability & Human Oversight	Human-in-the-loop approvals, audit-trail completeness, model cards, incident readiness, decommissioning, vendor governance and continuity
D7 — Human & Societal Harms	Phishing simulation, deepfake detection training, out-of-band authentication, social-engineering incident response and external attack defence
D8 — Regulatory Alignment & Compliance	EU AI Act risk-tier mapping, ISO/IEC 42001 gap tracking, GPAI documentation, DORA incident reporting and NIST SP 800-218A checks, where applicable
D9 — Physical AI Safety	Harm boundaries, safe-state transitions, override and emergency-stop tests, cyber-physical attack detection, environment integrity, actuator command verification, incident evidence

Routine activities are illustrative. The applicable controls and their exact requirements are those in GAISST-NOR-004.

12. Incident and Near-Miss Operations

Stage	Operational action
Detect	Receive alert, report or observed abnormal behavior
Triage	Classify severity, scope, safety, legal and service impact
Contain	Restrict capability, revoke access, isolate, roll back or enter safe state
Preserve	Protect prompts, outputs, state, logs, model/data versions and physical telemetry
Investigate	Reconstruct sequence, cause, control failure and affected parties
Communicate	Notify internal and external stakeholders as required
Recover	Validate safe and secure restoration
Improve	Complete root cause, corrective action and control retest

12.1 AI-specific incident categories

- Prompt injection, model extraction or model compromise
- Data poisoning, unauthorized retrieval or sensitive-data leakage
- Harmful, discriminatory, deceptive or materially incorrect output
- Agent action outside approved authority
- Unapproved model, prompt, data or supplier change
- Loss of human oversight or override capability
- Unsafe physical actuation or safety-envelope breach
- Evidence integrity failure or monitoring blind spot

12.2 Severity and escalation model

Severity	Examples	Response expectation
S1 Critical	Unsafe physical action, major breach, uncontrolled high-impact agent action	Immediate containment, executive/safety authority, incident command
S2 High	Material control failure, sensitive leakage, repeated harmful output	Urgent containment and same-day risk decision
S3 Moderate	Localized degradation, evidence gap, repeated minor failure	Time-bound investigation and corrective action
S4 Low	Documentation or isolated low-impact issue	Normal backlog and trend review

These severity levels are an operational example for triage within a GAISSTTM programme. Where incidents are classified or handled under UAIFTM or AI-IRFTM, those frameworks' severity scales apply.

13. Exception and Residual-Risk Operations

Lifecycle point	Operating requirement
Request	Identify control, scope, reason, duration and compensating measures
Assessment	Evaluate likelihood, impact, affected persons and dependencies
Approval	Use delegated authority appropriate to residual risk
Operation	Monitor compensating controls and risk indicators
Review	Reassess after change, incident or before expiry
Closure	Verify remediation or document new decision
Reporting	Escalate overdue, repeated and high-risk exceptions

14. Supplier Operations

Supplier signal	Operational response
Model or service change	Reassess evaluation baseline, compatibility and control assumptions
Security incident	Assess exposure, activate contractual notification and collect evidence
Availability degradation	Use fallback, controlled degradation or suspension
Assurance expiry	Request updated evidence or increase monitoring
Subprocessor change	Review data, jurisdiction and dependency impact
Contract deviation	Escalate, remediate or execute exit plan
Opaque failure	Record evidence limitation and increase independent testing

15. Evidence Operations

Activity	Operational requirement
Capture	Generate evidence as part of normal control operation
Index	Link artifact to control, system, period, owner and source
Protect	Use repository access, integrity and retention controls
Review	Check completeness, consistency, currency and limitations
Refresh	Replace expired or superseded evidence
Preserve failures	Retain negative, failed and inconclusive results
Export	Use controlled packages for audit or external assessment
Dispose	Follow legal, privacy and records requirements

15.1 Evidence freshness classes

Class	Typical evidence	Refresh trigger
Static design	Approved architecture, policy or standard	Material change or scheduled review
Periodic operating	Monthly/quarterly review or test	Next scheduled cycle
Continuous	Logs, alerts and telemetry	Ongoing retention and integrity monitoring
Event-driven	Incident, exception or change evidence	Each relevant event
Supplier	Attestation, report or contract evidence	Expiry, supplier change or incident

16. Change and Configuration Operations

1. Maintain an approved baseline for model, data, prompts, tools, policies and infrastructure.
2. Detect configuration drift and unauthorized changes.
3. Assess GAISSF control and evidence impact before material change.
4. Use tested rollback or safe-state capability.
5. Refresh affected evidence after deployment.
6. Update inventory, risk, the Applicable-Control Baseline and public claims where necessary.

17. Operational Metrics and Indicators

Metric class	Examples	Interpretation caution
Control coverage	Controls with current evidence and active monitoring	Coverage does not equal effectiveness
Control health	Green/amber/red/unknown distribution	Aggregate views can hide high-impact failures

Metric class	Examples	Interpretation caution
Security	Attack detections, abuse, unauthorized actions and containment time	Normalize by use and exposure
Safety	Near misses, overrides, blocked commands and safe-state events	Low counts may reflect under-detection
Model behavior	Drift, refusal, harmful-output and performance changes	Thresholds are context dependent
Operations	Availability, latency, error and recovery	Service quality is not safety assurance
Exceptions	Open, expired, repeated and high-risk exceptions	Track risk and age, not only count
Evidence	Expired, missing, rejected and unverifiable artifacts	Artifact volume is not evidence quality

17.1 KPI, KRI and KCI catalogue

Type	Examples	Use
KPI	Review completion, remediation throughput, evidence refresh timeliness	Process performance
KRI	Critical incidents, harmful-output rate, high-risk exceptions, unsafe-command attempts	Risk exposure
KCI	Blocked unauthorized actions, test pass rate, control-health green state, override success	Control effectiveness

18. Management Review

Review input	Management question
Scope and inventory	Does the approved scope still reflect actual operation?
Control health	Which controls are degraded, unknown or repeatedly failing?
Incidents and near misses	What changed in risk and what corrective action is needed?
Metrics	Are trends meaningful and thresholds still appropriate?
Exceptions	Are residual risks still acceptable and within authority?
Suppliers	Have inherited assumptions, services or assurance changed?
Resources	Are staffing, tooling and competence sufficient?
Improvement	Are corrective actions effective and recurring issues reduced?
Public claims	Does continuing operation remain within approved scope and public claims?

19. Continuous Improvement

Continuous improvement should be evidence-driven and linked to risk outcomes.

Input	Improvement action
Incident or near miss	Root cause, corrective action and control redesign
Failed test	Fix, retest and expand regression coverage
Metric degradation	Investigate causes and adjust control or threshold
User complaint	Review human factors, disclosure, recourse and misuse controls
Supplier issue	Strengthen contract, monitoring, redundancy or exit
Audit finding	Correct systemic cause and verify closure
Threat intelligence	Update scenarios, detection and technical controls
GAISST TM update or correction notice	Perform impact assessment and migration planning

19.1 Corrective-action quality criteria

- Addresses root cause rather than only the visible symptom
- Has an accountable owner and target date
- Includes interim containment where needed
- Defines validation and closure evidence
- Assesses recurrence across other systems and controls
- Updates procedures, training and monitoring where appropriate

19.2 Closed-loop improvement

Improvement should operate as a closed loop: identify signal, assess systemic cause, prioritize by risk, implement change, validate effectiveness, update documentation and monitoring, and review for recurrence across other systems.

Improvement stage	Required output
Identify	Incident, finding, metric trend, complaint or threat signal
Analyze	Root cause and affected population
Plan	Corrective and preventive action with owner/date
Implement	Controlled change and updated evidence
Validate	Retest and effectiveness decision
Institutionalize	Procedure, training, monitoring and cross-system update

20. Operational Assurance

Method	Use
Control-owner attestation	Confirm ownership and known changes

Method	Use
Evidence review	Verify currency, scope and integrity
Technical retest	Confirm continuing operation of critical mechanisms
Scenario exercise	Test incident, rollback, override and safe state
Sampling	Review representative users, events, suppliers and periods
Independent audit	Challenge design and operating effectiveness
External assessment	Obtain external assurance where applicable (certification is not currently offered)

21. Service Degradation, Suspension and Retirement

State	Operational treatment
Degraded	Restrict capability, inform users and increase oversight
Suspended	Disable affected function while preserving evidence and safe state
Withdrawn	Remove access, revoke integrations and stop new processing
Retired	Decommission system, close suppliers, manage data and archive evidence

21.1 Retirement checklist

- ☐ Users and integrations identified
- ☐ Processing and physical actions stopped
- ☐ Credentials, tools and supplier access revoked
- ☐ Data retained, returned or disposed appropriately
- ☐ Models, prompts and configurations archived where required
- ☐ Evidence and incident records preserved
- ☐ Public claims and inventories updated
- ☐ Residual obligations assigned

22. Operational Anti-Patterns

Anti-pattern	Risk	Corrective practice
Dashboard-only assurance	Metrics may lack source integrity or control context	Link signals to controls, owners and evidence
Alert accumulation	Critical events are lost in noise	Tune, prioritize and measure review completion
Model drift without decision criteria	Change is detected but unmanaged	Define thresholds and approved responses
Permanent exception	Nonconformance becomes normalized	Use expiry, review and remediation

Anti-pattern	Risk	Corrective practice
Supplier status assumed	Inherited controls silently degrade	Monitor notifications, incidents and assurance
Evidence refreshed only before audit	Run-state failures remain invisible	Maintain evidence continuously
Incident closure without retest	Control failure may persist	Require validated corrective action
Retirement without data and access closure	Residual exposure remains	Use controlled decommissioning

23. Legal and Regulatory Integration

GAISSF provides an operational security, safety, governance and evidence framework. It does not determine which laws apply, establish statutory compliance, create a legal safe harbour, define a legal standard of care, replace competent legal advice, or guarantee that evidence collected for GAISSF purposes will satisfy a regulator, court or other authority. Organizations should maintain a jurisdiction-specific legal and regulatory obligations register and map applicable obligations to their GAISSF scope, controls, evidence, reporting processes and decision authorities.

- Identify applicable jurisdictions, regulators, sector rules, contractual duties and internal legal authorities before relying on this guide.
- Maintain a controlled obligations register, reporting-clock register, retention schedule, legal-hold process and conflicts-of-obligation procedure.
- Treat statutory, regulatory and contractual analysis as a parallel workstream to GAISSF implementation and assurance.
- Record the legal basis, responsible owner, scope, decision, evidence, deadline and review date for each material obligation.
- Do not represent GAISSF conformance, maturity, or any future GAISSF certification as legal approval, permission to operate, immunity from enforcement or proof that harm cannot occur.

23.1 Statutory reporting and legal-response track

1. Open a legal and regulatory assessment in parallel with technical containment.
2. Identify each potentially applicable reporting regime and start its clock register.
3. Preserve facts supporting materiality, risk, harm and notification decisions.
4. Coordinate initial, supplemental and final reports with authorized legal and regulatory owners.
5. Document the basis for notification or non-notification and subsequent changes.

23.2 Legal hold and preservation override

Step	Control
Trigger	Pending or reasonably anticipated litigation, examination, investigation or formal preservation instruction.
Scope	Systems, custodians, repositories, dates and evidence categories.
Override	Suspend routine deletion, rotation, auto-termination and disposal.
Collection	Use authorized methods and preserve chain of custody.

Step	Control
Monitoring	Record acknowledgements, exceptions and preservation failures.
Release	Resume disposal only after documented authorized release.

23.3 Regional telemetry architecture

- Classify telemetry before collection.
- Keep sensitive telemetry regionally where required or approved.
- Use minimized, pseudonymized or aggregated cross-region feeds.
- Control support access, replication, retention and incident transfer.
- Document regional blind spots and compensating controls.

24. Limitations

- Operational metrics cannot capture every failure mode or emerging risk.
- Monitoring may be constrained by privacy, supplier opacity, system design or physical conditions.
- Thresholds require system-specific validation and may change over time.
- Absence of alerts does not establish absence of compromise or harm.
- Continuous monitoring does not eliminate the need for periodic independent assurance.

25. Notably Absent

- No universal operational threshold for every AI system.
- No assumption that service availability demonstrates security or safety.
- No permission to suppress failed, negative or inconclusive evidence.
- No automatic acceptance of supplier attestations as complete assurance.
- No guarantee that monitoring will detect every novel attack or emergent behavior.
- No substitution for sector-specific safety, quality, privacy or incident obligations.
- No universal reporting clock for every incident.
- No assumption that centralized telemetry is legally permissible in every region.
- No universal operational metric threshold; thresholds are risk- and context-specific.

Annex A — Daily Operations Checklist

- ☐ Critical alerts reviewed
- ☐ Red and unknown control-health states assigned
- ☐ Incidents and near misses triaged
- ☐ Unauthorized changes investigated
- ☐ High-risk agent and physical actions reviewed

- ☐ Supplier notifications checked
- ☐ Evidence pipeline operating
- ☐ Escalations completed

Annex B — Monthly Control Review Template

Field	Entry
Control ID	
System/scope	
Owner	
Health state	
Operating evidence	
Metrics	
Incidents/findings	
Exceptions	
Changes	
Actions	
Next review	

Annex C — Operational Dashboard Template

Indicator	Current	Threshold	Trend	Owner	Action
Control health					
Open incidents					
Expired evidence					
Open exceptions					
Model/data drift					
Supplier risk					
Safety events					

Annex D — Management Review Record

Review area	Finding	Decision	Owner	Due date	Evidence
Scope					

Review area	Finding	Decision	Owner	Due date	Evidence
Control health					
Incidents					
Exceptions					
Suppliers					
Resources					
Improvement					

Annex E — Source Traceability

Operational subject	Controlled source
Normative requirements	GAISSF-NOR-001
Control records	GAISSF-NOR-004
Terminology	GAISSF-NOR-005
Release and change history	GAISSF-NOR-007 and GAISSF-NOR-008
Adoption model	GAISSF-IMP-009 (where published and current)
Implementation workflows and evidence	GAISSF-IMP-010 (where published and current)
Deployment and handover	GAISSF-IMP-011 (where published and current)
Migration and evidence reuse	GAISSF-IMP-012 (where published and current)
Reference designs and telemetry	GAISSF-IMP-013 (where published and current)

Related guidance	Document
Troubleshooting	GAISSF-IMP-016
Evidence preservation	GAISSF-IMP-017
Continuous improvement	GAISSF-IMP-018

Annex F — Publication Record

Date	Change
29 June 2026	Initial operational handbook for GAISSF™ v1.0.
05 October 2026	Corrected D1-D9 runbooks; removed the conflicting profile notice; aligned certification, baseline, structure and severity wording; normalized assessor terminology; made legal certification wording future-conditional; qualified IMP-009 to IMP-013 dependencies. No GAISSF™ control changed.

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