ODA3 INSTITUTE

ADOPTION GUIDE

The First 30 Days

with GAISSF™

Doc ID: ODA3-2026-08-WHP-COM-009

Classification: Public / Freely Distributable

Executive Summary

This guide offers a suggested implementation spine for the first 30 days after an organization decides to begin applying GAISSF™: from establishing scope through a Day 30 management checkpoint. It is a planning structure, not a required timeline, and Day 30 is a checkpoint for management review — not an attestation, certification, conformance, safety, or regulatory conclusion.

> **METHODOLOGY NOTE**
> This guide is introductory and conceptual. It contains no client outcome data, no proprietary telemetry, and no incident statistics. The 30-day structure is illustrative pacing, not a mandated implementation timeline or assessment methodology.

1. Before You Start

This guide assumes your organization has decided to begin applying GAISSF™ and has identified a candidate AI system or bounded implementation initiative with which to start. It does not assume you have already completed formal scope or profile determination — that work is Week 1's first task, below.

Each week below follows the same structure: objective, activities, working outputs, questions to resolve, evidence to retain, and — deliberately — what that week does not establish, keeping evidence discipline present throughout, not saved for a closing disclaimer.

2. The Implementation Spine

Week 1 — Define Scope and Determine Applicability

Objective: Bound the candidate system and determine, do not casually confirm, the applicable GAISSF™ scope or profile.

- Activities: document the system's boundary — what it does, what data it can access, what actions it can take; determine and document the applicable GAISSF™ scope/profile against the authoritative framework and profile criteria, considering system capability and exposure, architecture and data flow, and assurance ambition. Profile selection must not be based solely on organizational size, convenience, or desired assurance outcome; identify who is accountable for the system's safety and security controls, and how that differs from existing IT/cybersecurity accountability; gather existing governance documentation.
- Working outputs: a documented system boundary, a recorded scope/profile determination with rationale, and a named accountable owner.
- Questions to resolve: are there third-party, embedded, or downstream components not yet in the boundary? does accountability sit with security, governance, engineering, or a shared function?
- Evidence to retain: the boundary documentation, the scope/profile determination and its rationale, and the accountability record.
- What this week does not establish: This week does not establish that the boundary or profile determination is final — both should be revisited if the system changes.

Week 2 — Establish the Applicable-Control Baseline

Objective: Build the applicable-control baseline required for the determined scope.

- Activities: for each applicable requirement, record: applicability and its justification, current implementation status, responsible ownership, available evidence references, exceptions or risk acceptance where applicable, and unresolved questions. Where your organization already uses NIST AI RMF, ISO/IEC 42001, or SOC 2, treat that as a separate, secondary analysis: use the mapping guides' supported correspondence / partial correspondence / gap / unknown categories to record whether existing work may support specific GAISSF™ requirements — this is a

correspondence analysis between frameworks, not the GAISSF™ implementation-status baseline itself.

- Working outputs: an applicable-control baseline record, and — where relevant — a separate framework-correspondence analysis.
- Questions to resolve: for requirements marked implemented, what evidence actually supports that status, versus what is assumed?
- Evidence to retain: the applicable-control baseline and any framework-correspondence analysis performed.
- What this week does not establish: This week does not establish that recorded implementation status is accurate — evidence review in Week 3 examines the support for that recorded status.

Week 3 — Assemble and Screen Evidence

Objective: Assemble evidence for the applicable-control baseline, and screen it for basic quality before relying on it.

- Activities: begin assembling evidence beyond policy statements alone, including relevant governance, configuration, technical, and operational records that may demonstrate implementation and operation; screen candidate evidence for relevance, authenticity, traceability, completeness, currency, and linkage to the system and scope being examined. Evidence existence alone does not establish sufficiency or operating effectiveness. For each gap, determine whether remediation is technical, procedural, governance-related, or mixed.
- Working outputs: an evidence inventory linked to the applicable-control baseline, and a categorized gap list.
- Questions to resolve: where evidence exists, does it demonstrate implementation and operation, or only intent?
- Evidence to retain: the evidence inventory and the underlying artifacts it references.
- What this week does not establish: This week does not establish that assembled evidence is sufficient for any assessment or conformance purpose — only what evidence currently exists and its basic quality characteristics.

> **KEY PRINCIPLE**
> Assurance is demonstrated, not asserted. Evidence should support what is claimed about a control's implementation and operation; the existence of evidence alone does not establish effectiveness or system safety — this applies as much during an initial 30-day implementation period as it does in a mature program.

Week 4 — Establish the Implementation Roadmap

Objective: Consolidate the documented baseline into a prioritized forward plan — not an assessment conclusion.

- Activities: consolidate the applicable-control baseline, available evidence, gaps, exceptions, and unresolved questions; assign owners and rough timelines to priority gaps; establish a recurring review cadence; define what changes — in system capability, exposure, architecture, intended use, or assurance scope — should trigger the scope/profile determination being revisited.
- Working outputs: a short implementation roadmap and a defined reassessment-trigger list.
- Questions to resolve: is the roadmap realistic given the resourcing available?
- Evidence to retain: the roadmap and the reassessment-trigger definition.
- What this week does not establish: This week does not establish that the system meets applicable GAISSF™ requirements, and does not constitute a formal assessment. It produces a management-ready status record, not an assurance conclusion.

3. The Day 30 Baseline

By Day 30, the organization should aim to have documented: bounded system scope; scope/profile determination and rationale; accountable owners; an applicable-control baseline; an evidence inventory with basic quality screening; identified gaps, exceptions, and unknowns; a prioritized roadmap with owners; and reassessment triggers with a next review point.

> **NOTABLY ABSENT**
> These are implementation-management outputs. Their existence does not establish GAISSF™ conformance, certification, control effectiveness, or system safety. Day 30 is a management checkpoint, not an assessment conclusion. This guide does not establish a required implementation timeline or a formal assessment methodology. Thirty days is a suggested planning structure; actual pacing depends on system complexity, resourcing, and organizational context.

4. A Worked Scenario (Hypothetical)

Consider a hypothetical firm piloting an internal AI assistant. In Week 1, the team documents the assistant's data-access boundary, names an accountable owner, and performs the applicable scoping/profile analysis — for purposes of this scenario, documenting Appendix P.1 as the applicable profile. This scenario does not establish general P.1 eligibility for internal assistants or for any particular type of organization; applicability must be determined case by case. In Week 2, they build the applicable-control baseline and find, on separate correspondence analysis, that existing vendor documentation partially supports one access-control requirement but provides no evidence for output review. In Week 3, they screen available evidence and, for this hypothetical system, determine that an appropriate remediation includes a defined human-review control and supporting records — a scenario-specific finding, not a general GAISSF™ requirement. In Week 4, they document remaining gaps in escalation-path definition and schedule a follow-up review in 90 days.

This scenario is illustrative only. It does not describe an ODA3 client, engagement, or outcome.

Next Reading

- GAISSF™ Appendix P.1 SMB Quick-Start Guide
- The 10-Minute Introduction to GAISSF™
- Applying GAISSF™: Worked Scenarios
- Mapping GAISSF to NIST AI RMF / ISO/IEC 42001 / SOC 2