

AIMRS™

Adoption Guide

From executive mandate to an operating AI management capability

PUBLICATION STATUS Official public release. This publication provides high-level AIMRS™ guidance. Controlled scoring keys, control applicability logic, assessment instruments, assurance procedures and practitioner materials are not included.

Originated and stewarded by CyberVirtues

Public Release 1.0 | August 22, 2026

Document ID: AIMRS-PUB-ADP-1.0

© 2026 Cyber Virtues LLC. All rights reserved.

1. Adoption Principle

AIMRS™ adoption begins with context and accountability, not a universal checklist. The objective is a functioning management capability that produces decisions and evidence in proportion to the organization's AI authority, impact and complexity.

ADOPTION PROMISE Start small enough to operate. Expand when scope, autonomy, impact, regulation or organizational complexity requires it.

2. Seven-Phase Adoption Path

Phase	Primary action	Exit condition
1. Mobilize	Name sponsor, leader, scope and objectives.	Accountability and mandate established.
2. Discover	Inventory AI, dependencies, owners and current controls.	Baseline estate sufficiently visible.
3. Assess	Classify material capabilities and review domain maturity.	Priority exposure and gaps agreed.
4. Design	Set target operating model, policies, lifecycle and evidence.	Future-state design approved.
5. Implement	Deploy practices, controls, roles, tooling and training.	Priority outcomes operating.
6. Assure	Test design and operating effectiveness.	Evidence supports management claims.
7. Improve	Measure, learn, remediate and expand scope.	Continual-improvement cycle active.

3. First 90 Days

Window	Leadership focus	Representative outputs
Days 1-15	Mandate and scope	Sponsor, accountable leader, charter, scope and immediate constraints.
Days 16-30	Visibility and materiality	Initial registry, owners, material-use classification and critical issues.
Days 31-45	Operating model	Decision rights, governance cadence, lifecycle gates and exception path.
Days 46-60	Priority controls	Security, authority, supervision, change, incident and intervention practices.
Days 61-75	Evidence and testing	Evidence plan, control tests, performance measures and corrective actions.
Days 76-90	Executive review	Baseline review, residual issues, target maturity and next-quarter roadmap.

4. Minimum Viable Program

- Executive sponsor and accountable AI management leader.
- Authoritative AI registry with assigned capability owners.
- Materiality, impact, risk and authority classification.
- Production authorization and material-change requirements.
- AI security, incident response and emergency intervention capability.
- Defined supervision for human-AI work, agents and consequential automation.
- Performance, value and impact measures appropriate to the capability.
- Evidence retention, exception management and scheduled review.

5. Scaling by Organization Size

Profile	Operating design
Small: 1-99	One executive sponsor, one accountable lead, lean registry, essential lifecycle decisions and quarterly review.
Mid-size: 100-999	Cross-functional forum, portfolio owner network, standard intake and change process, semiannual assurance.
Large: 1,000-4,999	Federated business ownership, central minimums, domain specialists, portfolio reporting and independent challenge.
Enterprise: 5,000+	Multi-entity model, delegated authorities, common evidence requirements, overlays, aggregation and formal assurance planning.

6. Adoption Roles

Role	Accountability
Governing body / executive team	Direction, risk appetite, investment, oversight and challenge.
Executive sponsor	Mandate, resources, escalation and organizational alignment.
AI management leader	Operating model, integration, priorities, reporting and improvement.
Capability owner	Value, authority, operation, evidence and lifecycle decisions for a specific capability.
Security / risk / legal / privacy	Specialist requirements, review, monitoring and challenge.
Workforce and operations leaders	Role design, supervision, adoption, service performance and intervention.
Assurance function	Independent evaluation proportionate to risk and claim significance.

7. Evidence of Adoption

AIMRS™ adoption is demonstrated through operating evidence, not policy publication alone. Evidence may include approved direction, registry records, ownership assignments, authority decisions, risk and impact evaluations, test results, access records, change approvals, incident records, performance measures, exceptions and verified corrective actions.

CLAIM RULE Using AIMRS™ internally does not create certification, endorsement or assessor status. Public conformance claims require an authorized program and defined assurance criteria.

Publication Notice

AIMRS™ (Artificial Intelligence Management, Risk & Security) is developed and stewarded by Cyber Virtues LLC. AIMRS™ and associated names, marks, framework structures and publications are proprietary intellectual property of Cyber Virtues LLC.

Permitted public use

- Download, read, cite and link to the unmodified publication for internal education and evaluation.
- Reference AIMRS™ accurately with attribution to Cyber Virtues LLC and the applicable release number.
- Use the publication to inform internal planning without representing independent certification or authorization.

Restricted use

- Do not modify, rebrand, resell, sublicense or publish derivative standards under the AIMRS™ name without written permission.
- Do not claim AIMRS™ certification, assessor status, conformance or endorsement unless formally authorized through an operational AIMRS™ program.
- Do not reproduce controlled scoring keys, assessment instruments, control logic or practitioner-only materials.

VERSION CONTROL Verify that this is the current public release at cybervirtues.com/ai-framework. References should identify the publication title and Public Release 1.0.