

AIMRS™ BASELINE

Baseline Quick Start

A simple path to visibility, accountability and prioritized improvement

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-BSL-1.0

© 2026 Cyber Virtues LLC. All rights reserved.

1. Purpose

The AIMRS™ Baseline helps an organization establish a credible starting point without turning AI management into an overwhelming compliance exercise. It answers three questions: What AI do we have? Who is accountable? What must improve first?

BASELINE OUTCOME A defined scope, a sufficiently visible AI estate, named accountability, identified critical gaps and a prioritized improvement plan.

2. Six Baseline Actions

Step	Action	Minimum output
1	Name accountability	Executive sponsor and accountable AI management lead.
2	Define scope	Business units, capabilities, locations and time period included.
3	Discover the estate	Initial registry of AI applications, agents, automation, robotics and embedded AI.
4	Classify material use	Business impact, authority, data sensitivity, reach, reversibility and uncertainty.
5	Review seven domains	Simple current-state judgment for Strategy, Workforce, Governance, Security, Operations, Performance and Lifecycle.
6	Prioritize improvement	Three to five actions with owners, dates and evidence of completion.

3. Minimum Registry Fields

Field	Question
Capability name	What is the AI-enabled capability called?
Purpose	What work or decision does it perform or influence?
Owner	Who remains accountable?
Provider and components	Which vendor, model, platform, data and tools are involved?
Users and affected parties	Who uses it and who may be affected?
Authority	What may it recommend, decide, communicate, transact or control?
Data	What data can it receive, create, retain or disclose?
Lifecycle state	Proposed, testing, approved, operating, suspended or retired?
Materiality	Could failure or misuse create meaningful financial, legal, safety, security, operational or reputational impact?

4. Rapid Domain Review

Domain	Baseline question
Strategy	Is the use tied to an approved objective and acceptable risk?
Workforce	Are human roles, supervision and intervention clear?
Governance	Are ownership, decision rights, policy and exceptions defined?
Security	Are identity, data, tools, vendors and response addressed?
Operations	Can the capability be monitored, supported, interrupted and recovered?
Performance	Are value, quality, cost, behavior and impact measured?
Lifecycle	Are intake, approval, change, suspension and retirement controlled?

5. Prioritization Method

Do not begin by assigning hundreds of checks. Prioritize based on consequence and control weakness. Address any capability with material authority, sensitive data, high reach, difficult reversibility or unclear ownership before lower-impact improvements.

Priority	Use when	Action
Immediate	Unapproved material use, unsafe authority, exposed sensitive data, no accountable owner or no intervention path.	Contain, restrict or suspend; assign leadership; preserve evidence.
Near-term	Material capability has gaps but can operate within temporary boundaries.	Create a dated remediation plan and heightened review.
Planned	Lower-impact capability needs repeatable management improvements.	Add to the operating roadmap and normal governance cadence.
Monitor	Current practices are sufficient for context.	Retain evidence and reassess after material change.

6. Baseline Completion Test

- Scope and exclusions are documented.
- Material AI capabilities are sufficiently visible for leadership decisions.
- Every material capability has a named accountable owner.
- Critical authority, data, security, operational and lifecycle gaps are known.
- Three to five prioritized improvements have owners, target dates and expected evidence.
- A date or event for reassessment is established.

SCORING BOUNDARY This public guide does not include the controlled AIMRS™ assessment instrument, scoring keys, weighting, calibration cases or certification 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.