

AIMRS™

Public Glossary

Common language for managing intelligent systems

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-GLS-1.0

© 2026 Cyber Virtues LLC. All rights reserved.

1. Purpose

The AIMRS™ Public Glossary establishes concise, technology-neutral language for executive, practitioner and stakeholder discussions. It distinguishes the operational AI capability from the model, vendor or product and assigns accountability to people and governing bodies - never to AI itself.

2. Core Terms

Term	Public definition
AIMRS™	Artificial Intelligence Management, Risk & Security: the organizational discipline for directing, governing, securing, operating and measuring AI systems that perform or influence work.
AI capability	A managed ability produced through AI models, data, software, tools, infrastructure, people and operating controls to perform or influence work.
AI estate	The total set of AI capabilities used, owned, supplied, embedded, tested or otherwise present within an organization.
AI portfolio	A governed collection of AI investments and capabilities managed together to achieve strategic outcomes.
AI registry	The authoritative system of record for identified AI capabilities, ownership, classification, authorization and lifecycle state.
AI use case	A defined application of AI to a business need, user outcome or operational activity.
AI value case	The documented rationale connecting an AI investment to measurable benefits, costs, risks and strategic objectives.
AI management system	The interacting policies, objectives, roles, processes and resources an organization uses to establish, operate and improve its management of AI.
AI profile	A documented adaptation of the framework for a particular industry, technology, risk context or organizational environment.

3. Workforce and Authority

Term	Public definition
AI workforce	The collection of AI capabilities that perform or materially influence work for an organization.
Blended workforce	A workforce operating model in which people, AI agents, automation and robotics perform coordinated work.
Digital worker	A persistent AI-enabled role configured to perform a defined body of work with assigned ownership, authority, measures and supervision.
Human-AI team	People and AI capabilities intentionally organized to perform interdependent work.
AI agent	An AI capability that can pursue objectives, make plans, use tools or take actions with some degree of autonomy.
Agent identity	The unique, managed identity used to authenticate an AI agent and attribute its access and actions.
Authority boundary	The approved limit on what an AI capability may access, recommend, decide, communicate, transact or control.
Autonomy	The degree to which an AI capability can select or execute actions without immediate human direction.
Human supervision	Ongoing human observation, review, direction and intervention appropriate to an AI capability's authority and impact.
Intervention	An authorized action to pause, restrict, override, isolate or stop an AI capability.

4. Governance, Risk and Assurance

Term	Public definition
Accountable owner	The named person responsible for the value, authority, operation, evidence and lifecycle decisions of an AI capability.
Material AI capability	An AI capability whose failure, misuse or impact could meaningfully affect people, operations, finance, compliance, safety, security or reputation.
Material change	A change that may alter an AI capability's purpose, authority, data, users, impact, risk, performance or operating environment enough to require reassessment.
AI risk	The effect of uncertainty associated with the development, use, operation or impact of AI on objectives.
AI security	Protection of the identities, data, models, tools, infrastructure, actions and evidence that comprise an AI capability.
Evidence	Records or observable facts that support a management, risk, security, performance or conformance claim.
Assurance	A structured evaluation that increases confidence in whether requirements are designed and operating effectively.
Exception	A time-bounded, approved deviation from a requirement with accountable ownership, rationale, safeguards and review.
Safe state	A defined condition that limits harm or unacceptable activity when an AI-enabled capability is interrupted, degraded or uncertain.
Retirement	Controlled removal of an AI capability's authority, access, dependencies and unsupported obligations.

5. Usage Rules

- Spell out Artificial Intelligence Management, Risk & Security on first formal reference to AIMRS™.
- Use AI capability when the managed operational whole is broader than a model or software product.
- Treat authority, autonomy, impact and risk as related but distinct concepts.
- Describe accountability as belonging to a person or governing body, never to AI itself.
- Use shall only in future normative requirements; use should for recommendations and may for permission.

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.