

# ISO/IEC 42001:2023 Artificial Intelligence Management System

Compliance Attestation

**Issuing Organization:** Akka Technologies, Inc.

**Issued By:** Michael Nash, Chief Information Security Officer

**Contact:** michael.nash@akka.io

**Date of Attestation:** April 20, 2026

**Review Cycle:** Annual

**Attestation Status:** Active

## Introduction

This attestation is issued by Akka Technologies, Inc. ("Akka") to confirm alignment with ISO/IEC 42001:2023 — the international standard for Artificial Intelligence Management Systems (AIMS). ISO/IEC 42001 is the first international standard establishing requirements for an AI management system, analogous in structure and intent to ISO/IEC 27001 for information security. It specifies requirements for establishing, implementing, maintaining, and continually improving an AIMS within the context of an organization that develops, provides, or uses AI systems.

Akka develops and operates the Akka platform — a reactive microservices and distributed systems toolkit available as both SaaS and open-source SDKs — and incorporates AI capabilities into its platform and internal operations. Akka recognizes the responsibilities that

accompany AI development and deployment, and has invested significantly in building governance structures aligned with ISO/IEC 42001.

Akka does not yet hold formal third-party ISO/IEC 42001 certification. This attestation represents Akka's self-assessment and internal confirmation that its practices align with all requirements of the standard. Akka intends to pursue formal third-party certification as the standard's certification ecosystem matures.

## Scope

This attestation covers Akka's Artificial Intelligence Management System (AIMS) as applied to:

- AI systems embedded in or offered through the Akka platform (SaaS)
- Internal AI tooling and automation used in Akka's operations
- AI capabilities integrated into Akka's software development lifecycle
- Third-party AI services and APIs incorporated into Akka's products or processes

The AIMS applies globally across all Akka operations. All 98 controls defined under ISO/IEC 42001 have been assessed and implemented. The risk posture across all controls is Low, reflecting the maturity of Akka's AI governance program following comprehensive internal review and remediation.

## Compliance Posture

Controls assessed: 98

Controls implemented: 98 (100%)

Controls in progress: 0

Controls not applicable: 0

Overall risk level: Low (all controls)

Geographic scope: Global

Akka's AIMS has achieved a fully implemented posture across all 98 controls, with every control assessed at Low residual risk. This represents the highest possible compliance posture under the standard and reflects the depth and maturity of Akka's AI governance investment.

## Key Controls and Implementation Evidence

### AI Policy and Strategic Direction

Akka has established a formal AI Policy that defines the organization's approach to the responsible development, deployment, and use of AI systems. The policy articulates AI objectives aligned with Akka's business strategy and ethical commitments, establishes accountability structures, and communicates expectations to all personnel who interact with AI systems. AI objectives are reviewed at least annually and tracked as part of the AIMS continual improvement process.

### AI Review Board

Akka has constituted a formal AI Review Board with a documented charter. The Board is responsible for reviewing and approving new AI system deployments, assessing AI-related

risks, monitoring compliance with the AI Policy, and providing oversight of the AIMS. The AI Review Board convenes on a scheduled basis and maintains records of all decisions and approvals. No AI system is deployed in production without Board review and formal sign-off.

## Agent Registry

Akka maintains a comprehensive Agent Registry — a structured inventory of all AI systems and autonomous agents deployed within the organization or offered to customers. For each registered AI system, the registry records the system's purpose, deployment context, data inputs and outputs, owning team, risk classification, approval status, and review history. The Agent Registry is a foundational control enabling effective AI governance, incident response, and continual improvement.

## AI Risk Assessment Process

Akka has implemented a formal AI risk assessment process aligned with ISO/IEC 42001 requirements. Risk assessments are conducted for all AI systems prior to deployment and periodically thereafter. The process evaluates risks across multiple dimensions including accuracy and reliability, security and adversarial robustness, privacy, fairness and bias, safety, transparency, and societal impact. Risk assessments are documented, reviewed by the AI Review Board, and used to determine required controls and mitigations.

## Interested Party Requirements Management

Akka has identified and documented the requirements of interested parties relevant to the AIMS, including customers, employees, regulators, and the public. Interested party requirements are reviewed periodically and inform the AI Policy, AI objectives, and AIMS scope. Customer contractual requirements relating to AI are tracked and addressed through Akka's contract management process.

## AI Incident Response

Akka has established AI-specific incident response procedures covering detection, reporting, investigation, and remediation of AI-related incidents. These include incidents involving AI system failures, unexpected outputs, bias or fairness concerns, and security events targeting AI systems. AI incident response is integrated with Akka's broader information security incident management program and is exercised regularly.

## Continual Improvement

Akka's AIMS incorporates a structured continual improvement process following the Plan-Do-Check-Act (PDCA) model. Internal audits of the AIMS are conducted on a scheduled basis. Management reviews are held to assess AIMS performance, review audit findings, evaluate changes in context, and set improvement objectives. Nonconformities are documented, root-cause analysed, and corrected. Improvement actions are tracked to completion.

## AIMS Scope Document

Akka has produced and maintains a formal AIMS Scope Document that defines the boundaries and applicability of the management system, including the organizational units, AI systems, and activities covered. The scope is reviewed at least annually and updated to reflect changes in Akka's AI landscape.

## Supporting Evidence and Third-Party Assurance

While ISO/IEC 42001 does not require third-party certification of cloud infrastructure providers, Akka's AI systems operate on cloud infrastructure that is independently audited. The following third-party assurances support Akka's overall AI governance posture:

- Google Cloud Platform (GCP): SOC 2 Type II, ISO/IEC 27001 certified. Akka's primary cloud infrastructure provider for AI workloads.
- AWS (Amazon Web Services): SOC 2 Type II, ISO/IEC 27001 certified. Used for supplementary AI infrastructure.
- Akka's own information security program is aligned with ISO/IEC 27001, providing a strong foundation for AI-specific controls.

Internal governance documentation available to qualified parties under NDA includes: AI Policy, AI Review Board Charter, Agent Registry (summary), AI Risk Assessment methodology, AI Incident Response procedures, and AIMS Scope Document.

## Attestation and Signature

I, Michael Nash, Chief Information Security Officer of Akka Technologies, Inc., attest that the information contained in this document accurately represents Akka's alignment with ISO/IEC 42001:2023 as of the date stated above. This attestation is based on internal assessment, documented evidence, and my professional judgment as CISO.

This attestation is made in good faith and to the best of my knowledge. It does not constitute a guarantee of absolute compliance or an invitation to audit without prior agreement. Akka reserves the right to update this attestation as its AI management system evolves.

**Michael Nash**



Akka.io | info@akka.io | 1-877-989-7372  
580 California St, #1231 San Francisco, CA 94104

**Chief Information Security Officer**

**Akka Technologies, Inc.**

**michael.nash@akka.io**

**April 20, 2026**

This attestation is available on request and is subject to annual review. For questions or to request supporting documentation, please contact michael.nash@akka.io.