AKKA

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

ISO/IEC 23894:2023 — AI Risk Management Guidance

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 23894:2023 — Information Technology — Artificial Intelligence — Guidance on Risk Management. ISO/IEC 23894 is a guidance standard (not a requirements standard) that provides direction on how organizations should manage risks related to AI systems throughout their lifecycle. It complements ISO/IEC 42001 (the AI Management System standard) and ISO 31000 (the general risk management standard), providing AI-specific risk management principles, framework guidance, and process guidance.

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's AI risk management practices are

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

aligned with the principles and guidance of ISO/IEC 23894, and are fully incorporated within the scope of Akka's ISO/IEC 42001-aligned Artificial Intelligence Management System (AIMS).

As a guidance standard, ISO/IEC 23894 does not provide for formal third-party certification. This attestation confirms that Akka's AI risk management practices reflect the standard's guidance.

Scope

This attestation covers Akka's AI risk management practices as applied to:

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

The AI risk management framework applies globally across all Akka operations. All 18 controls mapped to ISO/IEC 23894 have been assessed and implemented. The residual risk across all controls is Medium, reflecting appropriate management through Akka's AIMS controls. This risk level acknowledges the inherent nature of AI risk as an evolving discipline and the coverage provided by complementary ISO/IEC 42001 controls.

Compliance Posture

Controls assessed: 18

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

Controls implemented: 18 (100%)

Controls in progress: 0

Overall risk level: Medium (all controls, covered by ISO/IEC 42001 AIMS)

Geographic scope: Global

All 18 controls aligned to ISO/IEC 23894 are fully implemented. The Medium risk rating reflects the guidance nature of the standard and the fact that residual risk is managed through the broader ISO/IEC 42001 AIMS framework rather than through standalone ISO/IEC 23894-specific controls.

Key Controls and Implementation Evidence

AI Risk Management Framework

Akka has established an AI risk management framework consistent with ISO/IEC 23894 guidance. The framework defines the context for AI risk management, establishes roles and responsibilities, and integrates AI risk considerations into Akka's overall enterprise risk management approach. The framework is documented in Akka's AI Policy and operationalized through the AIMS.

AI Risk Identification

Akka conducts structured AI risk identification as part of its AI risk assessment process. Risk identification considers risks across the full AI system lifecycle — from design and development through deployment, operation, and decommissioning. Risk identification exercises involve cross-functional stakeholders including engineering, product, legal, and security teams. The AI Review Board oversees the risk identification process.

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

AI Risk Analysis and Evaluation

Identified AI risks are analysed to determine likelihood and potential impact, and evaluated against Akka's AI risk criteria. Risk analysis considers technical factors (model accuracy, robustness, reliability), operational factors (deployment context, data quality), and broader factors (societal impact, regulatory exposure, reputational risk). Risk evaluation outcomes inform treatment decisions and are documented in the Agent Registry for each AI system.

AI Risk Treatment

Akka applies risk treatment measures proportionate to evaluated risk levels. Treatment options include risk avoidance (not deploying a system), risk reduction (applying technical or procedural controls), risk sharing (contractual mechanisms, insurance), and risk acceptance (documented decisions with rationale). Treatment plans are reviewed by the AI Review Board and tracked to completion.

Monitoring and Review of AI Risks

AI risks are monitored on an ongoing basis. Key risk indicators are tracked and reviewed by the AI Review Board. Significant changes in AI system behaviour, deployment context, or the external risk landscape trigger reassessment. Annual formal risk reviews are conducted for all AI systems in the Agent Registry.

Communication and Consultation

Akka communicates AI risks appropriately to internal and external stakeholders. Internal communication includes regular reporting to leadership, training for relevant staff, and documentation in the AIMS. External communication includes this attestation and other

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

customer-facing documentation. Akka consults with relevant experts and monitors developments in AI safety and risk management.

Supporting Evidence and Third-Party Assurance

Akka's AI risk management practices are underpinned by the broader governance infrastructure of the ISO/IEC 42001-aligned AIMS, which itself is supported by:

- Google Cloud Platform (GCP): SOC 2 Type II, ISO/IEC 27001 certified infrastructure.
- AWS (Amazon Web Services): SOC 2 Type II, ISO/IEC 27001 certified infrastructure.
- Akka's ISO/IEC 27001-aligned information security management system, which provides foundational risk management practices that are extended to cover AI-specific risks under ISO/IEC 23894.

The integration of ISO/IEC 23894 guidance into Akka's ISO/IEC 42001 AIMS ensures that AI risk management is not siloed but embedded within a comprehensive, auditable management system.

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 23894:2023 as of the date stated above. This attestation is based on internal assessment, documented evidence, and my professional judgment as CISO.

AKKA

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

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 risk management practices evolve.

Michael Nash

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.