AKKA

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

NIST Cybersecurity Framework 2.0 Attestation

Issued by: Akka Technologies, Inc.

Signed by: **Michael Nash**, Chief Information Security Officer (michael.nash@akka.io)

Date: April 20, 2026

Document Status: Active — Subject to Annual Review

Introduction

This document constitutes a formal attestation by Akka Technologies, Inc. ("Akka") of its alignment with the NIST Cybersecurity Framework version 2.0 (NIST CSF 2.0), published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

The NIST Cybersecurity Framework 2.0 is a voluntary framework that provides organisations with guidance for managing and reducing cybersecurity risk. It is structured around six core Functions — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER — each of which represents a high-level cybersecurity outcome. This attestation summarises Akka's current posture against those functions and the controls they encompass.

Scope

This attestation covers the information security management programme operated by Akka Technologies, Inc. in support of its Akka platform — a cloud-hosted SaaS offering and

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

open-source SDK suite for building reactive microservices and distributed systems. The scope includes Akka's corporate systems, cloud infrastructure, software development lifecycle, third-party supplier relationships, and the people, processes, and technologies that support the delivery of Akka's services to its global customer base.

Compliance Posture

Akka has mapped its internal control framework against all 106 controls defined in NIST CSF 2.0. Of those 106 controls:

- 85 controls are fully Implemented
- 21 controls are On Hold, pending prioritisation in Akka's risk treatment backlog

This represents an overall implementation rate of approximately 80%, with the remaining controls acknowledged and scheduled for future implementation based on risk priority. Risk assessments across all controls indicate that 91 controls carry a Low residual risk rating and 15 carry a Medium residual risk rating. No controls carry a High residual risk rating, reflecting the effectiveness of Akka's existing security measures.

Akka's NIST CSF alignment is underpinned by its ISO 27001-aligned Information Security Management System (ISMS) and independently validated SOC 2 Type II report, both of which provide substantive evidence across multiple CSF Functions.

Key Controls and Implementation Highlights

GOVERN

AKKA

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

Akka has established a formal governance structure for cybersecurity, including a documented information security policy, defined roles and responsibilities (including an appointed CISO), and a risk management programme. The ISMS is reviewed annually and updated on a continuous basis. A risk register is maintained, and risk treatment decisions are documented, tracked, and approved through the ISMS governance process. Third-party supplier risk is incorporated into the overall risk management programme.

IDENTIFY

Akka maintains an up-to-date asset inventory covering hardware, software, cloud services, and data assets. Threat and vulnerability assessments are conducted on a regular basis. Business environment context — including regulatory obligations, customer commitments, and contractual requirements — is incorporated into the risk management process. Dependencies on critical third-party providers (cloud infrastructure, identity, monitoring) are tracked and assessed.

PROTECT

Access to Akka systems is governed by a formal access control policy implementing least-privilege principles and role-based access controls. Multi-factor authentication (MFA) is enforced for all corporate systems and cloud infrastructure access. Endpoint security controls, including CrowdStrike Falcon endpoint detection and response, are deployed across all company-managed devices. Data classification and handling procedures are in place, and data is encrypted at rest and in transit. Security awareness training is provided to all employees on joining and annually thereafter. Secure software development lifecycle (SSDLC) practices are embedded in Akka's engineering processes, including static analysis, dependency scanning (FOSSA), and peer code review.

DETECT

AKKA

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

Akka operates continuous security monitoring across its cloud infrastructure and corporate systems. Logging and monitoring are centralised, with alerts configured for anomalous access patterns, infrastructure changes, and potential indicators of compromise. Vulnerability scanning is performed regularly, and findings are tracked through to remediation. Security events are reviewed as part of regular operational processes.

RESPOND

Akka maintains a documented Incident Response Policy and Procedure. The incident response process defines roles, escalation paths, communication procedures (including customer notification obligations), and post-incident review requirements. Tabletop exercises and incident simulations are conducted to validate response readiness. Lessons learned from incidents and near-misses are captured and used to improve controls.

RECOVER

Business continuity and disaster recovery plans are documented and tested. Recovery objectives (RTO/RPO) have been defined for critical services. Backup and restore procedures are regularly tested. The recovery programme is integrated with the incident response process to ensure coordinated response and restoration activities following a security event.

Supporting Evidence

Akka's compliance with NIST CSF 2.0 is supported by the following evidence:

- SOC 2 Type II Report: Akka holds a current SOC 2 Type II report covering the Security, Availability, and Confidentiality Trust Services Criteria. This report provides independent third-party validation of Akka's security controls across multiple CSF Functions.

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

- ISO 27001-Aligned ISMS: Akka operates an Information Security Management System aligned with ISO/IEC 27001:2022. The ISMS provides a structured, risk-based approach to information security governance that maps directly to NIST CSF GOVERN, IDENTIFY, and PROTECT functions.

- Cloud Provider Assurance: Akka's primary cloud infrastructure providers (including Google Cloud Platform) hold their own SOC 2 and ISO 27001 certifications, providing additional assurance at the infrastructure layer.

- Endpoint Security: CrowdStrike Falcon is deployed across all company-managed endpoints, providing continuous threat detection and response capability aligned with DETECT and RESPOND functions.

- FOSSA Software Composition Analysis: Akka uses FOSSA to perform automated software composition analysis and licence compliance scanning, supporting IDENTIFY and PROTECT functions with respect to third-party software components.

Conclusion

Akka Technologies, Inc. is committed to the principles and practices embodied in the NIST Cybersecurity Framework 2.0. With 85 of 106 controls fully implemented, a risk profile showing no High-risk control gaps, and strong supporting evidence from its SOC 2 Type II report and ISO 27001-aligned ISMS, Akka demonstrates a mature and continuously improving cybersecurity posture aligned with this framework.

This attestation is made in good faith based on Akka's current information security programme as of the date of issuance. It is available to customers, prospects, and auditors upon request and is subject to annual review and renewal.

Signed,

Michael Nash

AKKA

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