

Attestation of Compliance with ISO 22301:2019 — Business Continuity Management

Issuer: Akka

Date: 2026-04-23

Subject: Compliance with ISO 22301:2019 — Security and Resilience: Business Continuity Management Systems — Requirements

Introduction

Akka is a cloud-native SaaS platform provider whose services support mission-critical enterprise workloads, including agentic AI applications for financial services, healthcare, and other regulated industries. ISO 22301:2019 establishes requirements for a Business Continuity Management System (BCMS) that enables organisations to anticipate, prepare for, respond to, and recover from disruptive incidents. All 10 ISO 22301 controls tracked by Akka are fully implemented.

Akka's business continuity programme is integrated with its ISO/IEC 27001:2022-certified ISMS, ensuring that information security and business continuity objectives are managed in a unified, coherent framework.

Scope of Compliance

1. Business Continuity Policy and Governance

Akka maintains a formal business continuity policy within its ISMS. The policy defines Akka's commitment to maintaining continuity of services, the scope of the BCMS, and the roles and responsibilities for business continuity management. Akka's CISO holds accountability for the BCMS, supported by engineering and operations leadership.

2. Business Impact Analysis

Akka has conducted a Business Impact Analysis (BIA) identifying all critical business processes and technology dependencies, including the Akka platform infrastructure, customer-facing APIs, data stores, and third-party integrations. The BIA defines Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each critical service, which are reviewed annually and updated following material changes to the platform architecture.

3. Risk Assessment for Business Continuity

Business continuity risks are identified and assessed as part of Akka's integrated ISMS risk management process. Disruption scenarios assessed include AWS regional outages, data centre failures, cyber incidents (ransomware, DDoS), key personnel unavailability, and third-party service provider failures. Risk treatment plans address each identified scenario.

4. Business Continuity Strategies and Solutions

Akka's platform is deployed on AWS with multi-region redundancy, automated failover, and elastic scaling. Key continuity strategies include:

- Multi-AZ deployments: All critical services are deployed across multiple AWS Availability Zones within the primary region.

- Cross-region replication: Critical data is replicated to a secondary AWS region to support regional failover.
- Automated backup: Customer data is backed up daily with point-in-time recovery capability.
- Immutable infrastructure: Platform components are deployed via Infrastructure as Code, enabling rapid rebuild from version-controlled configuration.
- Third-party redundancy: Critical third-party dependencies are assessed for their own business continuity capabilities.

5. Incident Response and Crisis Management

Akka maintains documented incident response and crisis management procedures covering the full lifecycle of disruptive incidents: detection, classification, escalation, containment, communication, recovery, and post-incident review. Communication templates and contact trees are maintained for rapid mobilisation. Customer communication procedures are documented with defined timelines and templates.

6. Business Continuity Plans

Akka maintains documented Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs) for all critical services. Plans specify recovery procedures, responsible personnel, escalation paths, and customer communication obligations. Plans are stored in accessible locations (Google Drive with offline copies) and reviewed annually.

7. Continuity Plan Testing and Exercises

Business continuity plans are tested at least annually through tabletop exercises and technical failover simulations. Test results are documented, with findings tracked through Akka's risk

management process. Where tests identify gaps, remediation actions are assigned with defined owners and completion dates.

8. Monitoring, Measurement, and Improvement

Akka continuously monitors platform availability and performance via Datadog, with automated alerting for service degradation or outages. Business continuity metrics including actual RTO/RPO achieved during incidents are tracked and compared against objectives. The BCMS is reviewed as part of Akka's annual ISMS management review, with improvement actions incorporated into the ISMS improvement programme.

Platform Availability Commitments

Akka's platform is designed to achieve high availability for enterprise customers. AWS infrastructure delivers 99.99% availability SLAs for core services. Akka's target platform availability is 99.9% or better, as specified in customer service level agreements.

Supporting Evidence

- ISO/IEC 27001:2022 certification (BCMS integrated with certified ISMS)
- Documented Business Impact Analysis
- Business Continuity Plans and Disaster Recovery Plans

- AWS multi-region and multi-AZ deployment architecture
- Annual BCP/DRP test reports
- Datadog availability monitoring and incident history
- SOC 2 Type II report covering availability trust service criteria

Conclusion

Akka is fully compliant with ISO 22301:2019. All 10 business continuity controls are implemented. Akka's cloud-native architecture, integrated BCMS, and regular continuity testing give enterprise customers confidence that Akka's services will remain available and recoverable in the face of disruptive incidents. This attestation is reviewed annually.

For further information about Akka's business continuity capabilities, please contact compliance@akka.io.

Authorized Signatory:

Michael Nash

Chief Information Security Officer

Akka

580 California Street, #1231

San Francisco, CA 94104

michael.nash@akka.io