AKKA

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

Attestation of Compliance with EBA Guidelines on ICT and Security Risk Management

Issuer: Akka

Date: 2026-04-23

Subject: Compliance with EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04, updated 2025 to align with DORA)

Introduction

Akka is a provider of an agentic AI SaaS platform whose services are used by European banks, investment firms, and other financial institutions regulated by the European Banking Authority (EBA). The EBA Guidelines on ICT and Security Risk Management set out detailed requirements for the governance, management, and oversight of ICT and security risks at financial institutions, and establish obligations for technology providers supplying critical services to those institutions. Updated in 2025 to align with the Digital Operational Resilience Act (DORA), these guidelines form part of the European financial sector's integrated ICT risk management framework.

All 19 EBA ICT controls tracked by Akka are fully implemented. The risk profile reflects the high regulatory expectations of the financial sector: 10 High, 8 Low, and 1 Medium — with High-risk controls subject to active risk treatment and continuous monitoring.

Scope of Compliance

AKKA

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

1. ICT Governance and Strategy

Akka maintains a robust ICT governance framework integrated with its ISO/IEC 27001:2022-certified ISMS. The framework defines clear governance structures including board-level accountability, CISO leadership, and operational oversight by engineering and security teams. An ICT risk management strategy is documented and reviewed as part of the quarterly ISMS management review. Akka's ICT governance is aligned with the requirements of EBA GL/2019/04 and the DORA framework.

2. ICT Risk Management Framework

Akka maintains a comprehensive ICT risk management framework covering identification, assessment, treatment, and monitoring of ICT risks. ICT risks are tracked in a formal risk register and reviewed quarterly. Risk treatment plans are assigned to accountable owners and progress is monitored. Risk appetite and tolerance levels are defined and reviewed annually. The framework covers all ICT systems, services, and third-party dependencies material to Akka's platform operations.

3. Information Security Controls

Akka implements the following information security controls relevant to EBA ICT requirements:

- Access control: Role-based access controls with mandatory MFA enforced via Okta. Privileged access is subject to additional controls and audit logging.
- Network security: AWS VPC segmentation with security groups, encrypted service-to-service communication, and TLS-protected external traffic.
- Encryption: AES-256 at rest and TLS 1.2+ in transit, with key management via AWS KMS.

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

- Endpoint protection: CrowdStrike Falcon deployed on all endpoints.

- Vulnerability management: Continuous vulnerability scanning via Wiz, with critical findings remediated within defined SLAs.

- Patch management: Documented patch management process with priority-based remediation timelines.

4. ICT-Related Incident Management

Akka maintains a documented ICT incident management process covering detection, classification, escalation, investigation, containment, remediation, and post-incident review. Incident classification criteria align with EBA incident severity thresholds. Financial institution customers are notified of ICT incidents affecting their services in accordance with contractual obligations and, where applicable, DORA reporting timelines. Incident metrics are reviewed as part of management reporting.

5. Business Continuity for ICT Services

Akka maintains business continuity and disaster recovery plans covering all ICT services material to the platform. BCP/DRP documentation includes recovery procedures, recovery time objectives, recovery point objectives, and communication plans. Plans are tested annually through tabletop exercises and technical failover simulations. Akka's multi-region AWS deployment provides resilience against regional infrastructure failures.

6. Third-Party ICT Risk Management

Akka operates a formal third-party risk management programme covering all material ICT suppliers and sub-processors. Supplier assessments evaluate security posture, business continuity, compliance certifications, and contractual obligations. Material ICT suppliers are

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

subject to annual reassessment. Contractual provisions with ICT suppliers align with EBA GL requirements and DORA Article 30 obligations.

7. Data Security and Resilience

All customer data processed on the Akka platform is protected through encryption, access controls, backup, and disaster recovery measures. Data backup procedures ensure RPO objectives are met. Data restoration procedures are tested as part of BCP/DRP exercises. Customer data is logically separated between tenants, preventing cross-customer data access.

8. Change and Project Management

Akka implements a documented change management process covering all changes to platform systems and configurations. Changes are classified by risk level and subject to appropriate review and approval gates. Emergency changes follow an expedited process with post-implementation review. Infrastructure changes are managed through Infrastructure as Code, providing version control and auditability.

DORA Alignment

As the EBA Guidelines have been updated to align with DORA, Akka's compliance programme also encompasses DORA supplier obligations under Title III (ICT Third-Party Risk Management), including Article 30 contractual requirements. Akka maintains a separate DORA attestation covering its full compliance with DORA supplier obligations.

AKKA

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

Supporting Evidence

- ISO/IEC 27001:2022 certification
- SOC 2 Type II report covering security, availability, and confidentiality
- ISO 22301 business continuity management alignment
- AWS security and compliance certifications (ISO 27001, SOC 2, PCI-DSS)
- CrowdStrike Falcon endpoint protection
- Wiz cloud security posture management
- Datadog security monitoring and observability
- Third-party vendor assessment programme
- Annual BCP/DRP test reports

Conclusion

Akka is fully compliant with the EBA Guidelines on ICT and Security Risk Management. All 19 controls are implemented. Akka's ISO 27001-certified security programme, combined with its financial sector-specific ICT risk management and business continuity capabilities, enables its European financial institution customers to meet their EBA and DORA obligations with respect to material third-party ICT providers. This attestation is reviewed annually.

For further information or to request Akka's detailed security documentation, please contact compliance@akka.io.

AKKA

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

Authorized Signatory:

Michael Nash

Chief Information Security Officer

Akka

580 California Street, #1231

San Francisco, CA 94104

michael.nash@akka.io