AKKA

Lightbend Inc, d.b.a Akka

Customer Support Policy

2026-04-13

Version 2

Contents

1.1. Introduction

This Customer Support policy covers Software and products that are deployed, managed, and hosted by Customer in their own environment, as well as those that are hosted or managed by Akka.

The Customer Support policy is designed to ensure that Customer receive prompt, professional, and courteous support. This policy provides an overview of the support and maintenance policies, which are part of the Akka offerings.

1.2. Scope

This policy applies to Customer and applies to all employees and authorized subcontractors who deal with Customer.

Akka's goal is to ensure the success of Customer. Customer may use Akka support to ask questions in addition to reporting bugs. Akka support will guide the use of Akka technologies.

Support does not include code or architectural reviews in-depth, nor does it include writing any application code. For services like these, Customer can engage Akka's professional services team.

1.3. Referenced Policies

1. Disciplinary Policy
2. Incident Management Policy

1.4. Referenced Frameworks and Standards

1. Akka's Internal Assurance Framework

1.5. Product

Our policies around how our products *are supported.*

1.5.1. Product Support Policy

Akka supports all of its products that have not been designated as end-of-life, meaning we will provide support services as described in this policy.

We proactively fix discovered CVEs and bugs only in the latest version, not previous versions.

Customers may request remediation for CVEs on all supported versions. Akka will advise if remediation will be included in an existing version (via a patch version release) or if it will require an upgrade.

1.5.2. New Versions

Whenever a new version of a product is released (including minor patch versions), that version of the product becomes supported. This support is available on that version for a period of two (2) years from the release date of that version, at a minimum.

1.5.3. End-of-Life Notice

In the event we plan to end-of-life a product or module, we will provide a minimum of one (1) year notice.

1.5.4. Product Feature Requests

Akka commits to ensuring a consistent and transparent workflow for evaluating and responding to customer feature requests for all products. It commits to capturing and logging all requests with relevant context and business rationale, which is followed by a prioritization meeting involving key stakeholders to categorize each request as *Accepted and Scheduled* (with an ETA), *Accepted and Backlogged* (acknowledged but unscheduled), *Not Accepted* (with recorded rationale), or *Insufficient Information* Finally, Akka commits to communicating these statuses to the customer and offering funded engagement options for backlogged or reconsidered items.

A documented issue ticket serves as the system of record for all status updates and communications.

1.6. Support Levels

Akka provides different levels of support with varying response time SLOs, as defined below.

1.6.1. Response Times

For customer support for products/services not hosted by Akka, Akka will use commercially reasonable efforts to provide an acknowledgment of a reported Issue to the Customer and respond within the target time frames specified below. Response times define the maximum time to initially respond to the customer's report of an incident, the time for a workaround or patch, and the time for a permanent correction to the incident, if applicable.

While not making a guarantee or warranty, Akka will make commercially reasonable efforts to respond to reports within the timeframes outlined in the table below for each Support level.

To expedite a response, the issue must be opened as a Severity 1 or 2 in the Support Portal making sure that it falls under the definition of Severity 1 or 2 as set forth in Section 1.6.3; these instructions must be followed to expect the noted response time.

Because there are fixed times during which an incident can be reported, the response time shown is not necessarily contiguous. For example, if an incident is reported at 5:00 PM on a Friday afternoon, it may be as late as the following Monday morning before a response is issued.

1.6.2. Support Levels

Akka offers *24/7*, *Developer*, and *Basic* support. 24/7 Support satisfies the requirements of deployed production applications while Developer support assists during the development of the application:

Level	Description	Subscription Type
24/7	24/7 support is geared towards enterprise customers who require around-the-clock support. This option provides customers with 24 hours per day, 7 days per week, and 365 days per year coverage for production outages (Severity 1). 24/7 support is ideal for mission-critical applications. To expedite a response, the issue must be opened as a Severity 1 or 2 in the Support Portal making sure that it falls under the definition of Severity 1 or 2 as set forth in Section 1.6.3.	Enterprise, Serverless-Critical, Serverless-Priority, Bring Your Own Cloud, Self Hosted
Developer	Developer support is for assistance during the development phase of an application. Developer support is not for production systems. Severity 1 and 2 are not applicable to Developer support (as they are only for systems in production)	ISV/OEM, Growth
Basic	Basic support is equivalent to Developer supportassisting during the development phase of an application and not intended for production systems but provided at a lower SLO.	Academic, Dev Subscription, Startup, Serverless-Explorer

1.6.3. Severity Levels and Response Times

Severity	Description	Akka Response	Levels	Initial Response	Work Around	Permanent Correction
1	An Error in the Software which severely affects the overall production performance of the Softwares function or process, such that a production system is non-functional and no procedural workaround exists. *Only applicable to production environments.*	Akka will work continuously on Severity 1 incidents until a workaround or system recovery is successfully implemented and either the incident is closed or the severity is reduced. When required, Akka will provide a patch release to resolve Severity 1 incidents.	24/7	1 hour, any time of day (24 x 7 x 365)	3 hours	Next Release
2	An Error in the Software which materially affects the overall production performance of the Softwares function or process so that the function or process is noticeably impaired from it's previous baseline, but where business operations continue. *Only applicable to production environments.*	Akka will work to provide a resolution to Severity 2 incidents by a reasonable date agreed to between Akka and the Customer. When required Akka will provide a patch release to resolve Severity 2 incidents.	24/7	4 business hours	1 business day	Next Release
3	An Error that does not materially affect the overall performance of a production function or process. This may include a minor issue with limited loss or no loss of functionality or impact on the Customer's operations. Also an Error in a non-production environment which is requested to be reviewed at a higher priority due to it blocking critical development efforts.	Akka will work to provide a resolution to Severity 3 incidents in an Upgrade release.	All Levels	1 business day	Future Release	Future Release
4	An Error encountered in a non-production environment, general usage questions, and documentation Errors.	Akka will work to provide a resolution to Developer incidents in an Upgrade release.	All Levels	1 business day (except 3 business days for Basic level)	Future Release	Future Release

1.6.4. Support Availability

Akka provides support to customers worldwide. Each customer will be designated a regional support center that best matches the customer's time zone. Response times are dictated by the time zone of the customer's designated support center. Support hours are **08:00 to 18:00, Monday through Friday**, within the time zone of the designated regional support center. Daylight savings time changes apply within each center's time zone. Holidays are regional and are itemized below. Akka provides support in the following support centers:

Support Center	Time Zone	Holidays
Australia	Australian Eastern Time (AET)	New Year's Day, Australia Day, Good Friday, Easter Monday, Anzac Day, Queen's Birthday, Labour Day, Christmas Day, Boxing Day.
Central Europe	Central European Time (CET)	New Year's Day, St Berchtold, Good Friday, Easter Monday, Ascension, Whit Monday, Swiss National Day, Federal Fast holiday, Christmas Day.
US East	Eastern Time (EST)	New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, Day after Thanksgiving, and Christmas Day.
US Pacific	Pacific Time (PST)	New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, Day after Thanksgiving, and Christmas Day.

1.6.5. Issue Limits

The number of support issues allowed is unlimited for all classifications.

1.7. Overview

An overview of how we provide support services to our customers.

1.7.1. Policy

Akka is committed to providing the support to Customer. Akka strives to resolve all Customer queries and requests as soon as possible and to keep Customer informed throughout the process.

Akka provides Customer with access to the Support Portal where Customer can submit support cases and review the Akka knowledge base, security alerts, documentation, and other technical content.

Support cases can be submitted by Customer through the Support Portal at https://support.akka.io, through the Akka Console at https://-console.akka.io/support, or by sending an email to support@akka.io. To expedite processing of the support issue, Customer should provide a title, descriptive summary of the problem, error message or symptom descriptions, log messages, time of incident, and a description of how this is affecting Customer's business operations.

All support interactions are conducted in English.

Support cases may be submitted for experimental features, however, the expected response times below do not apply in this case.

A support issue is closed when either

1. At Customer's request when the issue is considered resolved, or
2. After an extended period where Customer no longer replies to requests for more information or is unable to verify that the issue is resolved.

Akka notifies Customer that a support issue has been closed, and Customer can reopen an issue on request.

1.7.2. Customer Support System

Akka provides a support system that allows users to report suspected defects, complaints, issues, and any other challenge through an appropriate channel.

Reported tickets are addressed by our support staff in a timely manner, as detailed in this policy.

1.8. Support Team Interaction

Our Support Team is focused on rapid response and resolution for operational issues. This section describes how those interactions can be initiated.

1.8.1. Who Should I Contact?

It's important to direct your inquiry to the right team for the fastest resolution.

Scenario	Primary Contact	Description
Urgent/Break-Fix Issues	Akka Support Team	Service degradation, outages, error messages, production system failures, and "how-to" questions.
Proactive/Strategic Guidance	Technical Account Manager (TAM)	Architecture reviews, service adoption roadmaps, strategic planning, feature requests, and escalating high-priority support issues.
Billing/Account Questions	Akka Support Team or Customer Success Team	Invoices, subscription changes, and account management.

1.8.2. Ways to Open a Support Issue with Akka

There are several ways to initiate a support issue with the Akka team. Each support issue is assigned a unique identifier, which can be used to refer to the case in subsequent communications.

Note

A support issue (sometimes also called a support 'case' or 'ticket') is the basic unit that our team work with. In some circumstances an Incident may be created related to a support issue as part of an escalation of high urgency issues, but these are distinct items.

1.8.2.1 Customer Support Portal

In our Support Portal (requires login)

- **Access the Portal**: Log into the Customer Support Portal at https:support.akka.io
- **Provide Critical Information**: The more detail you provide, the faster we can help.
  - **Issue Title**: A brief, descriptive summary of the problem.
  - **Error Message or Symptom Description**: The exact text of any error you are seeing, or a detailed description of the experienced symptom.
  - **Log messages** or other helpful information from our platform.
  - **Time of Incident:** When the issue started, including the time zone.
  - **Impact:** A description of how this is affecting your business operations.

1.8.2.2 Akka Console

In the Akka Console (requires login)

- Access the support form in the Akka console at https://console.akka.io/support
- Provide Critical Information: The more detail you provide, the faster we can help.
  - **Subject:** A brief, descriptive summary of the problem.
  - **CC email:** list other addresses that should receive the support communication, additional to the logged in user.
  - **Project:** If applicable, select a Project from the drop down menu
  - **Error Message or Symptom Description:** The exact text of any error you are seeing, or a detailed description of the experienced symptom.

1.8.2.3 via Email

Sending an email from an address that is part of a registered customer domain will create a support issue in our system.

- Send the email to support@akka.io
- Provide Critical Information: The more detail you provide, the faster we can help.
  - **Subject:** A brief, descriptive summary of the problem.
  - **CC email:** Any addresses on the CC receiver list will also be added to receive the support communication.
  - **Error Message or Symptom Description:** The exact text of any error you are seeing, or a detailed description of the experienced symptom.

1.8.3. How Are Support Issues Closed

A support issue is closed when:

- At the customer's request, when the issue is considered resolved.
- After a long period where the customer no longer replies to requests for more information, or is unable to verify that the issue is resolved.

The customer will always receive a notification that a support issue has been closed, and can always re-open an issue as needed on request.

1.9. Technical Account Manager

For customers who have a Technical Account Manager (TAM) assigned, this section describes their value and how to interact with them most effectively.

1.9.1. How to Schedule Time with Your TAM

- **Direct Email:** Use the contact information provided during your onboarding.
- **Scheduled Meeting:** Your TAM will suggest scheduling a regular meeting so you can discuss your questions and needs.

Note

Do not use your TAM's contact information for initial Break-Fix support issues. Always open a ticket first (as per above) to ensure the fastest resolution path.

1.9.2. When to Engage Your TAM

Your TAM is essential for proactive and strategic engagements, including:

- **Roadmap Planning:** Discussing upcoming service consumption and capacity needs.
- **Architecture Reviews:** Scheduling a deep-dive review of your cloud deployment for best practices and cost optimization.
- **Support Escalation:** When a Severity 1 or Severity 2 issue is not progressing according to your expectations, your TAM is the direct path for internal escalation.
- **Quarterly Business Review**: Coordinating a regular review of your performance metrics, support trends, and strategic goals.

1.10. Compliance

For Akka employees, failure to comply with this policy may result in progressive discipline up to and including dismissal. For non-Akka employees and contractors, failure to comply may result in removal of the individual's ability to access and use Akka data and systems. Employers of non-Akka employees will be notified of any violations.

Glossary

EEA States The EU Member States as well as Iceland, Liechtenstein and Norway.. *see* EEA & EU

Agence nationale de la sécurité des systèmes dínformation The French National Agency for the Security of Information Systems. Agence nationale de la sécurité des systèmes dínformation is the National Cybersecurity Certification Authority for France and a leading authority in Common Criteria evaluation and EUCC certification.. *see* EUCC & National Cybersecurity Certification Authority

Bundesamt für Sicherheit in der Informationstechnik The German Federal Office for Information Security. The BSI is the National Cybersecurity Certification Authority for Germany and one of the most active national authorities in Common Criteria evaluation and EUCC certification in Europe.. *see* EUCC & National Cybersecurity Certification Authority

Centro Criptológico Nacional The Spanish National Cryptologic Centre. Centro Criptológico Nacional acts as the National Cybersecurity Certification Authority for Spain under the EUCC scheme and oversees Common Criteria evaluations performed in Spain.. *see* EUCC & National Cybersecurity Certification Authority

Comité français dáccréditation The French national accreditation body responsible for accrediting Conformity Assessment Bodys and other conformity assessment organisations in France, including those operating under EUCC.. *see* Conformity Assessment Body & EUCC

Conformity Assessment Body An accredited organisation authorised by the relevant National Cybersecurity Certification Authority to perform security evaluations and issue evaluation reports under a cybersecurity certification scheme such as EUCC.. *see* EUCC & National Cybersecurity Certification Authority

Development A CC assurance class (designator *ADV*) covering evidence about the design and implementation of the TOE, including functional specification, architectural design, and implementation representation.. *see* CC & TOE

Elliptic Curve Digital Signature Algorithm A digital signature algorithm based on elliptic curve cryptography. Elliptic Curve Digital Signature Algorithm provides equivalent security to Rivest–Shamir–Adleman with shorter key lengths and is widely used for TLS certificates and code signing.. *see* Rivest–Shamir–Adleman & TLS

European Cybersecurity Certification Framework The framework established by the EU Cybersecurity Act for creating European cybersecurity certification schemes. EUCC is the first scheme adopted under the European Cybersecurity Certification Framework.. *see* EUCC

Evaluation Assurance Level A numeric rating (EAL1–EAL7) assigned by a CC evaluation that indicates the depth and rigour of the security examination. Higher Evaluation Assurance Level values demand more comprehensive analysis and testing.. *see* CC

Evaluation Technical Report A confidential document produced by a Conformity Assessment Body summarising the evaluation evidence, methodology, and conclusions. Submitted to the National Cybersecurity Certification Authority as the basis for issuing a CC certificate.. *see* Conformity Assessment Body, CC & National Cybersecurity Certification Authority

Guidance Documents A CC assurance class (designator *AGD*) covering evaluation of the operational and preparative guidance provided to administrators and users of the TOE.. *see* CC & TOE

Impact Analysis Report A document produced during maintenance of a CC certificate that assesses whether a change to the certified TOE affects the validity of the existing certificate and determines what re-evaluation, if any, is required.. *see* CC & TOE

National Competent Authority A national authority within an EU member state designated to oversee cybersecurity matters. In the context of EUCC, the National Competent Authority may also serve as the National Cybersecurity Certification Authority.. *see* EUCC & National Cybersecurity Certification Authority

National Cybersecurity Certification Authority The national body designated under the EU Cybersecurity Act (Regulation (EU) 2019/881) to supervise cybersecurity certification activities and issue certificates under schemes such as EUCC within a member state.. *see* EUCC

Netherlands National Communications Security Agency The Dutch national authority for communications security, responsible for Common Criteria evaluation oversight and EUCC certification activities in the Netherlands.. *see* EUCC

Organismo di Certificazione della Sicurezza Informatica The Italian Certification Body for Information Security. Organismo di Certificazione della Sicurezza Informatica acts as the National Cybersecurity Certification Authority for Italy under the EUCC scheme.. *see* EUCC & National Cybersecurity Certification Authority

Protection Profile An implementation-independent set of CC security requirements for a category of product, used as a reusable baseline. Vendors may claim Protection Profile compliance within their Security Target.. *see* CC & Security Target

Secure Hash Algorithm A family of cryptographic hash functions standardised by NIST. SHA-256 and SHA-384 (from the SHA-2 family) and SHA-3 variants are approved for use in Akka systems; MD5 and SHA-1 are deprecated.. *see* NIST

Security Assurance Requirement A requirement drawn from CC Part 3 that specifies what the developer and evaluator must produce to demonstrate a given level of assurance. Security Assurance Requirements are composed into Evaluation Assurance Levels.. *see* CC & Evaluation Assurance Level

Security Functional Requirement A requirement drawn from CC Part 2 that specifies the intended security behaviour of the TOE. Security Functional Requirements are stated in the Security Target and verified during the evaluation.. *see* CC, Security Target & TOE

Security Problem Definition The section of a Security Target or Protection Profile that formally describes the threats, organisational security policies, and assumptions that the TOE is designed to address.. *see* Protection Profile, Security Target & TOE

Security Target A document defining the security problem, objectives, and summary of security specifications for a specific TOE. The Security Target is the primary artefact evaluated and certified under CC.. *see* CC & TOE

TOE Summary Specification A section of the Security Target that describes how the TOE satisfies each of its Security Functional Requirements, bridging the security requirements and the implemented product.. *see* Security Functional Requirement, Security Target & TOE

United Kingdom Accreditation Service The sole national accreditation body for the United Kingdom, responsible for accrediting Conformity Assessment Bodys and other conformity assessment organisations. Relevant to EUCC evaluations conducted by UK-based Conformity Assessment Bodys under mutual recognition arrangements.. *see* Conformity Assessment Body & EUCC

Vulnerability Assessment A CC assurance class (designator *AVA*) covering evaluation of the resistance of the TOE to exploitation by an attacker with defined attack potential.. *see* CC & TOE

AAO Akka Automated Operations - a managed platform deployed within a customer VPC that fully automates and supports production-grade, self-clustering and elastic agentic services built with the Akka SDK.. *see* Akka SDK & VPC

AI Risk Management Framework A structured approach to identifying, assessing, and mitigating risks associated with AI systems, as outlined by the NIST.. *see* AI & NIST

AIMS **A**I **M**anagement **S**ystem – a management system for establishing, implementing, maintaining, and continually improving the governance of AI within an organization, as defined by ISO/IEC 42001.. *see* AI

Akka Application An application that is built using the Akka SDK. Akka applications contain APIs, workflows, streaming consumers, timers, and views for querying data. They are packed into Docker images and deployed as microservice instances within an Akka operating environment. Akka applications act as their own in-memory, durable database. They take responsibility for persisting their own state. Akka apps also cluster from within, creating a runtime cluster with other instances that handle balancing traffic, sharding data, and replicating their data to instances running within another region. Akka applications can be replicated between regions in different Akka Application Planes if needed.. *see* Akka Application Plane, Akka SDK & API

Akka Application Plane The runtime environment for hosting Akka applications within one or more regions. The Akka application plane provides compute, storage, and I/O to execute Akka apps. It also provides automation to increase or decrease application instance capacity, observability for monitoring and debugging application behavior, and infrastructure management. The application plane is responsible for ensuring an Akka application meets its SLA by managing the Akka application and the underlying infrastructure. Data in this plane does not leave your VPC nor does it interact with our Akka Federation Plane.. *see* Akka Federation Plane, SLA & VPC

Akka CLI The CLI for developers, operators, and InfoSec teams to interface with various Akka environments. The Akka CLI provides utilities for building, testing, packing, and deploying Akka applications. It also provides utilities for observability, secrets management, service scaling, and account management.. *see* CLI

Akka SDK SDK with support for programming components, a local debugging console, and a test kit for building, testing, and packing Akka applications.. *see* SDK

ALC-DVS.1.1.1C In the context of the EUCC standard, ALC-DVS.1.1.1C is a specific assurance component within the Common Criteria framework. It falls under the ALC class, specifically the DVS family.. *see* ALC, DVS & EUCC

ALC-DVS.2 A component of the ALC class within the CC framework (EUCC), specifically under the DVS family. This component requires that security measures in place during the development of the TOE are sufficient to protect the TOE and its associated assets. It aims to ensure that the development environment is secure and that the measures are adequate to maintain the confidentiality and integrity of the TOE throughout its development.. *see* ALC, CC, DVS, EUCC & TOE

ANPD **A**utoridade **N**acional de **P**roteção de **D**ados – the Brazilian National Data Protection Authority responsible for enforcing and overseeing compliance with the LGPD.. *see* LGPD

AOC **A**ttestation of **C**ompliance – A formal self-assessment document or report completed by a merchant or service provider to certify compliance with the PCI-DSS, confirming that all applicable requirements have been met.. *see* PCI-DSS

ARN **A**mazon **R**esource **N**ame - A unique identifier for AWS resources used in IAM policies, service configurations, and audit logs to unambiguously reference any resource across the AWS platform.. *see* AWS & IAM

Assets Entities that the owner of the TOE presumably places value upon. In the context of a DSS, assets are information in electronic or other form, information processing facilities and referring processes (incl. access control and alarm systems), development tools and environments, any manifestation of the TOE, and customer code and data provided to produce the TOE. *see* DSS & TOE

Authentic Data In the context of the EU DORA, data from a statutory public register, the dissemination and/or processing of which is subject to statutory requirements and which are disclosed by the customer to third parties in connection with the performance of a contract.. *see* EU DORA

BAA **B**usiness **A**ssociate **A**greement - A contract required under HIPAA between a Covered Entity and a Business Associate that receives, creates, or transmits protected health information on its behalf, establishing each party's obligations for safeguarding that information.. *see* HIPAA

BCR **B**inding **C**orporate **R**ules - An approved data protection policy, under Article 47 of the GDPR, that allows multinational organisations to transfer personal data within their corporate group to entities in countries outside the EEA that do not provide an adequate level of protection.. *see* EEA & GDPR

BIA **B**usiness **I**mpact **A**nalysis – A structured process for identifying critical business functions and processes, quantifying the potential consequences of their disruption, and determining recovery priorities and objectives. See Business Impact Analysis.. *see* Business Impact Analysis

Break-Fix A type of support issue where the customer is reporting a failure or other issue and is expecting the Akka team to stop it from occurring or reoccurring, as opposed to support issues where architecture review, optimization, or other issues are the primary subject of the issue.. 4, 6

BSI Group **B**ritish **S**tandards **I**nstitution Group – A leading global standards body and certification authority that issues ISO/IEC 27001 and other management system certifications.. *see* IEC & ISO

Business Continuity Planning See Business Continuity Planning. *see* Business Continuity Planning

Business Operations General term for the entirety of operations performed by the developer related to the TOE, e.g. "personalization is part of Business Operations.. *see* TOE

BYOD Abbreviation for **B**ring **Y**our **O**wn **D**evice, a corporate IT policy that permits employees to use their personal smartphones, laptops, or tablets to access company data and perform work tasks rather than relying on employer-provided hardware. See personal-device.. *see* IT

CCM **C**loud **C**ontrols **M**atrix – a cybersecurity control framework developed by the CSA that provides security controls mapped to leading industry standards for cloud environments.. *see* CSA

CD **C**ontinuous **D**eployment - The automated release of software builds that have passed all automated quality and security gates to production or a staging environment, typically as the final stage of a CI/CD pipeline.. *see* CI

CLD Cloud-specific control prefix used in ISO/IEC 27017 to designate controls applicable specifically to cloud service customers and providers (e.g., CLD.12.4.1 for monitoring of cloud services).. *see* IEC & ISO

CNAPP **C**loud-**N**ative **A**pplication **P**rotection **P**latform – An integrated security platform that combines CSPM, workload protection, and software composition analysis capabilities to secure cloud-native applications from development through runtime.. *see* CSPM

Confidence In Akka's ISMS, the confidence level assigned to a control following an internal audit, reflecting whether evidence was found that the Implementation Details are being followed in practice. Rated High, Medium, or Low.. *see* ISMS

Consent Consent of the Data Subject means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.. *see* Data Subject

Consumer In the context of the CCPA, A natural person who is a California resident.. *see* CCPA

CPA **C**ertified **P**ublic **A**ccountant - A licensed accounting professional qualified to perform independent audits; CPA firms conduct SOC 2 Type II attestation audits of service organisation controls.. *see* SOC

Critical or Important Function In the context of the EU DORA, a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.. *see* EU DORA

CSA **C**loud **S**ecurity **A**lliance – a non-profit organisation that promotes best practices for secure cloud computing and publishes guidance and frameworks including the CCM and the STAR certification programme.. *see* CCM & STAR

CSF The NIST Cyber Security Framework (v2.0). *see* NIST

CVE Common Vulnerabilities and Exposures: A unique, standardized ID for a publicly disclosed software security vulnerability, acting as a universal dictionary entry to facilitate data sharing.. 1

Data Subject Request A request made by an individual or an individual's legal representative to request Akka to do something which falls under one of the rights granted to EU-based individuals by the GDPR.. *see* EU & GDPR

Data Subjects See Data Subject.. *see* Data Subject

Deployer Any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity. *see* AI

Development environment Environment in which the TOE is developed; development includes the production of the TOE.. *see* TOE

DORA The EU Digital Operational Resilience Act, or DORA Regulation. *see* DORA Regulation & EU

DORA CO DORA **C**ontractural **O**bligations - specific contractural obligations required to be in place by the EU DORA for regulated industries and their ICT suppliers.. *see* DORA, EU DORA & ICT

DR **D**isaster **R**ecovery is a set of policies, tools, and procedures used to regain access and functionality to IT infrastructure following a catastrophic event. While HA focuses on surviving small hardware failures, DR is the "Plan B" for major disasterssuch as fires, floods, cyberattacks (like ransomware), or massive regional power outages.. *see* HA & IT

DRP **D**isaster **R**ecovery **P**lan – a documented set of procedures to recover and restore IT systems, data, and operations following a disruptive event.. *see* IT

DSAR **D**ata **S**ubject **A**ccess **R**equest - A request by an individual under data protection law (e.g. GDPR) to obtain a copy of the personal data an organisation holds about them, along with information about how it is processed.. *see* GDPR

DSD Development Security Documentation, in the context of the EU CRA. *see* EU CRA

DSS Development Security System, in the context of the EU CRA. *see* EU CRA

EBA **E**uropean **B**anking **A**uthority – the EU regulatory body responsible for maintaining financial stability and ensuring the integrity of the European banking sector through binding technical standards and guidelines.. *see* EU

EBS **E**lastic **B**lock **S**tore - An AWS block storage service providing persistent, high-performance storage volumes for use with EC2 instances, supporting encryption at rest and point-in-time snapshots.. *see* AWS & EC2

EC2 **E**lastic **C**ompute **C**loud - An AWS service providing scalable virtual machine capacity in the cloud, used to run application workloads, container nodes, and managed services.. *see* AWS

ECS Amazon **E**lastic **C**ontainer **S**ervice – an AWS managed container orchestration service for deploying, managing, and scaling containerized applications.. *see* AWS

EIOPA **E**uropean **I**nsurance and **O**ccupational **P**ensions **A**uthority – One of the three EU financial supervisory authorities responsible for regulating and supervising the insurance and occupational pension sectors, and jointly overseeing the designation of critical ICT third-party service providers under DORA.. *see* DORA, EU & ICT

EKS Amazon's **E**lastic **K**ubernetes **S**ervice - A managed service that automates the deployment, scaling, and management of **K**ubernetes control planes and infrastructure on AWS.. *see* AWS

end-of-life End-of-Life means a vendor has formally declared that a particular version of a product, application, operating system, or technology will no longer be supported, developed, or sold.. 1

ESMA **E**uropean **S**ecurities and **M**arkets **A**uthority – One of the three EU financial supervisory authorities responsible for regulating and supervising securities markets, and jointly overseeing the designation of critical ICT third-party service providers under DORA.. *see* DORA, EU & ICT

ETA **E**stimated **T**ime of **A**rrival - in the context of software development or services, an estimate of the time by which the noted change or feature will be completed.. 2

EU CRA EU **C**yber **R**esiliency **A**ct: The goal of the CRA is to protect consumers and strengthen the EU's overall level of resilience. This means reducing the risks for all users of digital products, whether private individuals or public entities (corporations, hospitals, banks, utilities, postal services and so on). The CRA is mandatory, and compliance is required for CE Marking of regulated products, as well as for distribution in the European market. The CRA includes some strict, coercive measures such as heavy fines.. *see* CE Marking & EU

EU DORA See DORA. *see* DORA

EU GDPR Specifically the EU version of the GDPR.. *see* EU & GDPR

EUCC **E**uropean **U**nion **C**ommon **C**riteria, a standard for evaluating the security of information technology products and systems, ensuring they meet defined security requirements and specifications. The EUCC framework is derived from the SOG-IS Common Criteria which in turn is based on the ISO/IEC 15408-1 Common Criteria standard for Information Technology Security Evaluation. However, the SOG-IS adds an additional layer of mutual recognition among European countries. This means that a product evaluated and certified in one member state under SOG-IS is recognized by other member states, reducing the need for multiple evaluations.. *see* IEC & ISO

GPG **G**NU **P**rivacy **G**uard - A free, open-source implementation of the OpenPGP standard for encrypting and digitally signing data, widely used for signing software release artefacts and verifying their integrity.. *see* OpenPGP

gRPC gRPC - An open-source remote procedure call framework using HTTP/2 transport and Protocol Buffers serialisation, enabling efficient, strongly typed, language-agnostic communication between services.. *see* HTTP

High Security Area Area where TOE related data or material classified critical or very critical is accessible, and Security Control areas (access control and intrusion detection) where applicable.. *see* TOE

ICT Asset In the context of the EU DORA, a software or hardware asset in the network and information systems used by the financial entity.. *see* EU DORA

ICT Risk In the context of the EU DORA, any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.. *see* EU DORA

ICT Services In the context of the EU DORA, digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.. *see* EU DORA & ICT

ICT Third-Party Risk An ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements.. *see* ICT

ICT Third-Party Service Provider Any company (whether independent or part of a financial group) providing ICT Services to financial entities. *see* ICT Services

ICT-Related Incident In the context of the EU DORA, a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity.. *see* EU DORA

ICTS **I**nformation and **C**ommunication **T**echnology **S**ecurity – The practice of protecting ICT systems, networks, and data from threats, ensuring the confidentiality, integrity, resilience, and availability of digital infrastructure.. *see* ICT

Incident An unplanned interruption or reduction in quality of service or breach of our Cloud Services SLA Policy, or any event that requires an immediate and time-sensitive response in order to avoid security or availability issues for our customers.. 4

IS Incident An IS incident. A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.. *see* IS

ISO/IEC 27701 Security techniques Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management Requirements and Guidelines. *see* IEC & ISO

ISV Independant System Vendor: Often a reseller of Akka's products, where Akka is incorporated into or used by their own product.. 2

ITSEF **I**nformation **T**echnology **S**ecurity **E**valuation **F**acility. It is an accredited laboratory responsible for conducting security evaluations of IT products and systems according to the Common Criteria standards. *see* IT

LLM **L**arge **L**anguage **M**odel – a type of AI model trained on large text corpora and capable of generating, summarising, translating, and reasoning about natural language.. *see* AI

Major ICT-Related Incident In the context of the EU DORA, an ICT-Related Incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity.. *see* EU DORA & ICT-Related Incident

MGF **M**odel **G**overnance **F**ramework – Singapore's regulatory framework, published by the Monetary Authority of Singapore, for governing the responsible development and deployment of AI models in financial services.. *see* AI

ML **M**achine **L**earning – a branch of AI in which systems learn from data to improve performance on tasks without being explicitly programmed for each case.. *see* AI

NACL **N**etwork **A**ccess **C**ontrol **L**ist - A stateless firewall rule set in AWS that controls inbound and outbound traffic at the subnet level within a VPC, evaluated in rule-number order.. *see* AWS & VPC

Nasjonal sikkerhetsmyndighet The Norwegian National Security Authority, responsible for supervising protective security in Norway and acting as the national authority for Common Criteria evaluation and EUCC certification activities.. *see* EUCC

Network and Information System In the context of the EU DORA, An electronic communications network as defined in Article 2(1) of Directive (EU) 2018/1972; Any device or group of devices connected or associated with each other, one or more of which carry out automated processing of digital data based on a programme; or Digital data stored, processed, retrieved or transmitted by the elements specified for the purpose of their operation, use, protection and maintenance.. *see* EU DORA

NIS2 **N**etwork and **I**nformation **S**ystems Directive 2 – the EU cybersecurity directive (2022/2555) that strengthens security requirements and incident reporting obligations, extending scope to additional critical sectors compared to its predecessor.. *see* EU

NVD **N**ational **V**ulnerability **D**atabase - The US NIST repository of vulnerability management data, providing CVSS scores, remediation guidance, and searchable CVE records used to assess and prioritise security vulnerabilities.. *see* CVE, CVSS & NIST

OEM Original Equipment Manufacturer: Often a reseller of Akka's products, where Akka is incorporated into or used by their own product.. 2

OPC **O**ffice of the **P**rivacy **C**ommissioner – the Canadian federal authority responsible for overseeing compliance with PIPEDA and other federal privacy laws and promoting privacy rights.. *see* PIPEDA

P90 A statistical measure used to describe the performance of a system (usually latency or response time). If an SLA specifies a P90 of 500ms, it means that 90 percent of all requests are completed in 500ms or less.. *see* SLA

PDPA Singapore's **P**ersonal **D**ata **P**rotection **A**ct – Singapore's primary data protection legislation, enacted in 2012 and administered by the PDPC, governing the collection, use, and disclosure of personal data.. *see* PDPC

PEM Security of Critical Infrastructure Act 2018 (Cth) — Australian legislation that imposes risk management and mandatory incident notification obligations on owners and operators of critical infrastructure assets, including a 12-hour notification window to the ASD for critical cyber security incidents.. *see* ASD

Personal Device A device not owned by Akka, but owned by a User. Examples include personal cell phones, tablets, smart watches and so forth. See BYOD.. *see* BYOD

PHD **A**WS **P**ersonal **H**ealth **D**ashboard - An AWS service providing personalised, real-time information about the health of AWS services and resources, including scheduled maintenance events and security notifications relevant to an account.. *see* AWS

PII **P**ersonally **I**dentifiable **I**nformation is any data that can be used on its own or with other relevant information to identify, contact, or locate a single person. See Personal Information.. *see* Personal Information

PIMS **P**rivacy **I**nformation **M**anagement **S**ystem — A management system for establishing, implementing, maintaining, and continually improving an organisationś privacy governance framework, built as an extension to an ISMS in accordance with ISO/IEC 27701.. *see* ISMS & ISO/IEC 27701

Privileged Users In the context of the EU DORA, Privileged users: system administrators and operators who supervise the operation of the system as a whole. In addition, there may also be users with privileged user rights or user rights with advanced functionality in a specific IT system (e.g. they may grant users read/write permissions).. *see* EU DORA

Quarterly Business Review A regular (typically per Quarter) review of a customer's performance goals and objectives, and how Akka is supporting them.. 6

RDS **R**elational **D**atabase **S**ervice - An AWS managed database service supporting multiple relational database engines (including PostgreSQL, MySQL, and Aurora), providing automated backups, encryption at rest, and high availability.. *see* AWS

REST **R**epresentational **S**tate **T**ransfer - An architectural style for distributed hypermedia systems in which clients interact with server resources using standard HTTP methods; the dominant paradigm for designing web APIs.. *see* API & HTTP

RoPA **R**ecord **o**f **P**rocessing **A**ctivities - A mandatory documentation requirement under Article 30 of the GDPR that organisations must maintain, listing all personal data processing activities, their purposes, data categories, retention periods, and technical/organisational safeguards.. *see* GDPR

RoPA **R**ecord **o**f **P**rocessing **A**ctivities - A mandatory documentation requirement under Article 30 of the GDPR that organisations must maintain, listing all personal data processing activities, their purposes, data categories, retention periods, and technical/organisational safeguards.. *see* GDPR

S3 **S**imple **S**torage **S**ervice - An AWS object storage service providing high durability, scalability, and availability for storing and retrieving data, supporting encryption at rest, versioning, and access control policies.. *see* AWS

SAML **S**ecurity **A**ssertion **M**arkup **L**anguage - An XML-based open standard for exchanging authentication and authorisation data between identity providers and service providers, enabling SSO for enterprise applications.. *see* SSO

SCC **S**tandard **C**ontractual **C**lauses - Pre-approved contractual clauses issued by the European Commission that provide a legal mechanism for transferring personal data from the EEA to third countries that have not been deemed to offer an adequate level of data protection.. *see* EEA

SCC **S**tandard **C**ontractual **C**lauses - Pre-approved contractual clauses issued by the European Commission that provide a legal mechanism for transferring personal data from the EEA to third countries that have not been deemed to offer an adequate level of data protection.. *see* EEA

SCP **S**ervice **C**ontrol **P**olicy - An AWS Organizations policy type that defines the maximum set of permissions available to accounts within an organisational unit, used to enforce preventive governance guardrails across the entire AWS account hierarchy.. *see* AWS

SD **S**ecurity **D**omain - A classification framework for AI agent deployments that defines the security boundary across four dimensions: data classification, action scope, system boundary, and autonomy level; SD-1 denotes the first and most restrictive tier of this classification.. *see* AI

Significant Cyber Threat In the context of the EU DORA, a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-Related Incident or a major operational or security payment-related incident.. *see* EU DORA & ICT-Related Incident

SLO A **S**ervice **L**evel **O**bjective is a specific target or goal within an SLA. It is the technical benchmark that the team aims to hit to keep the customer happy. SLOs are usually more stringent than the SLA to provide a "safety buffer.". 2, *see* SLA

SoA **S**tatement of **A**pplicability – a document required by ISO/IEC 27001 that lists all controls from Annex A, declares whether each is applicable to the organisation, and provides justification for any exclusions.. *see* ISO/IEC 27001

SOCI Act Security of Critical Infrastructure Act 2018 (Cth) — Australian legislation that imposes risk management and mandatory incident notification obligations on owners and operators of critical infrastructure assets, including a 12-hour notification window to the ASD for critical cyber security incidents.. *see* ASD

SPDX **S**oftware **P**ackage **D**ata **E**xchange - An open ISO/IEC standard (ISO/IEC 5962) for communicating SBOM information, including package identities, versions, license obligations, and provenance data.. *see* IEC, ISO & SBOM

SRE **S**ite **R**eliability **E**ngineering – a discipline that applies software engineering practices to IT operations, focusing on building reliable, scalable, and efficient systems through automation and measured service-level objectives.. *see* IT

STAR **S**ecurity, **T**rust, **A**ssurance and **R**isk – the CSA certification and registry programme that documents the security controls of cloud service providers, enabling customers to assess provider compliance.. *see* CSA

STS AWS **S**ecurity **T**oken **S**ervice – an AWS service that issues temporary, limited-privilege credentials for accessing AWS resources, supporting federated identity, cross-account access, and role assumption.. *see* AWS

TAM A **T**echnical **A**ccount **M**anager: A customer's technical advocate and strategic partner within Akka.. 4, 6

Third Country In the context of the EU and EU customers, any State that is not a member of the EEA.. *see* EEA & EU

Threat-Led Penetration Testing In the context of the EU DORA, a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems.. *see* EU DORA

TIA **T**ransfer **I**mpact **A**ssessment - An assessment required when transferring personal data to a third country, evaluating whether the law and practice of the destination country ensures adequate protection for the data transferred in light of Article 46 of the GDPR.. *see* GDPR

ticket A filed support request about a singular topic. Akka's support system tracks customer requests, bugs, etc via such 'issues'. 4

ticket Shorthand name for a filed support issue. Akka's support system tracks customer requests, issues, bugs, etc via such 'tickets'. 4

Trade Secret In the context of the EU DORA, a fact, information, other data or an assembly thereof, connected to an economic activity, which is secret in the sense that it is not, as a body or as the assembly of its components, generally known or readily accessible to persons dealing with the affected economic activity and therefore it has pecuniary value, and which is subject to steps made with the care that is generally expected under the given circumstances, by the person lawfully in control of the information, to keep it secret. Protected knowledge (know-how), technical, economic or organisational knowledge, solution, experience or the assembly thereof that are classified as trade secret and recorded in an identifiable manner also constitute trade secrets.. *see* EU DORA

TSC The **T**rust **S**ervices **C**riteria are a set of control criteria developed by the AICPA to evaluate and report on the suitability of the design and operating effectiveness of controls at a service organization relevant to the Security (the only required criterion), Availability, Processing Integrity, Confidentiality, or Privacy of the information and systems used to process user data.. *see* AICPA

UK **U**nited **K**ingdom - The sovereign state comprising England, Scotland, Wales, and Northern Ireland. Following its departure from the EU, the UK maintains its own data protection regime under the UK GDPR and the Data Protection Act 2018.. *see* EU & GDPR

Index