



Lightbend Inc, d.b.a Akka

# Resilience Guarantee Policy

2026-04-13

Version 1

# Contents

<b>Contents</b>	<b>i</b>
1.1 Introduction . . . . .	1
1.2 Scope . . . . .	1
1.3 Referenced Policies . . . . .	1
1.4 Referenced Frameworks and Standards . . . . .	1
1.5 Resilience Guarantee . . . . .	1
1.5.1 Resilience . . . . .	1
1.5.2 Qualifying . . . . .	1
1.6 Resilience Guarantee Claims . . . . .	2
1.6.1 Filing a Claim . . . . .	2
1.6.2 Validation . . . . .	2
1.6.3 Limitations and Application of Credits . . . . .	2
1.6.4 Exclusions . . . . .	2
1.7 Compliance . . . . .	3
Glossary . . . . .	4
<b>Index</b>	<b>12</b>

## 1.1. Introduction

Akka believes in the resilience and reliability of its Software, to the point where Akka guarantees it to the extent set forth herein.

If Akka causes a loss of reliability in [Your Application Services](#), Akka will reimburse Customer for the period of unreliability in accordance with the terms and conditions set forth below.

## 1.2. Scope

This policy applies to a customer's use of Akka when licensed or subscribed for production use. If Your Agreement predates this policy, you should contact your account representative to update your agreement with us.

## 1.3. Referenced Policies

1. [Akka Federation Plane SLA Policy](#) - Akka's policy that governs the availability SLA for the Akka Federation Plane and other hosted services available at Akka.io.
2. [Access Control for Customer-Confidential Data Policy](#)

## 1.4. Referenced Frameworks and Standards

1. [Akka's Internal Assurance Framework](#)

## 1.5. Resilience Guarantee

### 1.5.1. Resilience

Resilience is the ability of an Akka application to function without a permanent loss of data. If an Akka application permanently loses information it is intended to retain, it is not resilient.

Further, for an Akka application to be non-resilient (or to lack resilience), it must have a cause rooted in Akka in its native state without third party interaction, interoperation, or interference. This policy offers remuneration for a lack of resilience caused by Akka and excludes non-resilience caused by the Exclusions (as defined below).

A lack of resilience is experienced over a period of time - the interval over which an application was non-resilient.

### 1.5.2. Qualifying

In the event [Your Application Services](#) becomes non-resilient, Akka indemnifies Customer from and against losses arising because of such non-resilience in accordance with the terms and conditions set forth in this Policy. To qualify for this indemnity:

1. [Your Application Services](#) must be using a version of Akka released within the last eighteen (18) months prior to the qualifying event of non-resilience;
2. [Your Application Services](#) must be using a version of Akka that has not been [EOL](#).
3. [Your Application Services](#) must be running in production and must be authorized for use in a production environment;

## 1.6. Resilience Guarantee Claims

### 1.6.1. Filing a Claim

Assuming Customer qualifies, to file a claim, Customer must open a support ticket via the [Support Portal](#) (as such term is defined in the Akka Customer Support Policy) within seventy-two (72) hours of the application first exhibiting signs of non-resilient behavior. The ticket should include:

1. The unreliability time frame of Your Application Services, and
2. Either debug logs showing the unreliability events, or, a minimal reproducer that demonstrates the Akka core issue.

For the sake of clarity, this seventy-two (72) hour support ticket is to log an indication of non-resilient behavior for obtaining credits against this resilience guarantee. If any of [Your Application Services](#) exhibit non-resilient or unreliable behavior, regardless of the source, that scenario should be considered a Severity 1 issue with Customer opening the related support ticket immediately upon first knowledge thereof.

### 1.6.2. Validation

Customer's claim will be approved for remuneration only after Akka verifies that the issue causing the non-resilient behavior originates within Akka.

Akka will attempt to validate the issue independently, however, Akka may require Customer's participation in order to diagnose the issue, including attempting suggested resolutions on a test system.

### 1.6.3. Limitations and Application of Credits

Once a claim is filed and validated, a reimbursement credit for twenty (20) times the applicable fees (for annual subscriptions, the pro-rata allocation of Customer's total Fees (annual Software and Managed Services spend)) of the non-resilient period will be issued to Customer.

For example, if Customer's total annual Fees are \$120,000 and it experienced a loss of resiliency caused by Akka that lasted 2 hours, the Service Credit would be  $20 * 2 / (24 * 365) * \$120,000 = \$547.95$ .

This credit will be applied to Customer's future license or subscription (as applicable) fees with Akka and cannot be redeemed for cash or cash equivalent.

### 1.6.4. Exclusions

This guarantee does not apply to any unavailability, suspension or termination of Akka issues, directly or indirectly (the "**Exclusions**"):

- Caused by factors outside of Akka's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Akka;
- That result from any actions or inactions of Customer, including failure to acknowledge a recovery volume or respond to resource health concerns;
- That result from equipment, software or other technology not supplied by Akka, which includes unintended interference from Java Virtual Machine observability agents;
- That use a version of Akka's product where the root cause of the loss was caused by a known issue that has been resolved in a subsequent version;
- That result from the use of any pre-release of the Software such as Beta or Milestone releases, except for Developer Support and agreed to by Akka in an applicable Order Form;
- That result from the use of software not obtained from Akka under the Agreement.

## 1.7. 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 d'information** The French National Agency for the Security of Information Systems. [Agence nationale de la sécurité des systèmes d'information](#) 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 d'accréditation** The French national accreditation body responsible for accrediting [Conformity Assessment Bodies](#) 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 Bodies](#) and other conformity assessment organisations. Relevant to [EUCC](#) evaluations conducted by UK-based [Conformity Assessment Bodies](#) 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** AI Management System – 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](#)
- BSI Group** **B**ritish **S**tandards **I**nstitution **G**roup – 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** **C**loud-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** Cloud-Native Application Protection Platform – 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** Certified Public Accountant - 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** Cloud Security Alliance – 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](#)
- 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](#) Contractual Obligations - specific contractual obligations required to be in place by the [EU](#) [DORA](#) for regulated industries and their [ICT](#) suppliers.. *see* [DORA](#), [EU DORA](#) & [ICT](#)
- DR** Disaster Recovery 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 disasters such as fires, floods, cyberattacks (like ransomware), or massive regional power outages.. *see* [HA](#) & [IT](#)
- DRP** Disaster Recovery Plan – a documented set of procedures to recover and restore [IT](#) systems, data, and operations following a disruptive event.. *see* [IT](#)
- DSAR** Data Subject Access Request - 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** European Banking Authority – 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** Elastic Block Store - 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** Elastic Compute Cloud - 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 Elastic Container Service – an [AWS](#) managed container orchestration service for deploying, managing, and scaling containerized applications.. *see* [AWS](#)
- EIOPA** European Insurance and Occupational Pensions Authority – 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 Elastic Kubernetes Service - A managed service that automates the deployment, scaling, and management of [Kubernetes](#) control planes and infrastructure on [AWS](#).. *see* [AWS](#)
- EOL** End-of-Life - The point in a product’s lifecycle when a vendor ceases all production, distribution, and security updates, requiring replacement to mitigate unpatched vulnerabilities and compliance risks.. [1](#)
- ESMA** European Securities and Markets Authority – 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](#)
- EU CRA** [EU](#) Cyber Resiliency Act: 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** European Union Common Criteria, 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** GNU Privacy Guard - 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** Information and Communication Technology Security – The practice of protecting [ICT](#) systems, networks, and data from threats, ensuring the confidentiality, integrity, resilience, and availability of digital infrastructure.. *see* [ICT](#)
- 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](#)
- ITSEF** Information Technology Security Evaluation Facility. It is an accredited laboratory responsible for conducting security evaluations of [IT](#) products and systems according to the Common Criteria standards. *see* [IT](#)
- LLM** Large Language Model – 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** Model Governance Framework – 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** Machine Learning – 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** Network Access Control List - 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** Network and Information Systems 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** National Vulnerability Database - 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](#)
- OPC** Office of the Privacy Commissioner – 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 Personal Data Protection Act – 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** AWS Personal Health Dashboard - 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** Personally Identifiable Information 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 Privacy Information Management System** — A management system for establishing, implementing, maintaining, and continually improving an organisation's 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](#)
- RDS Relational Database Service** - 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 Representational State Transfer** - 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 Record of Processing Activities** - 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 Record of Processing Activities** - 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 Simple Storage Service** - 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 Security Assertion Markup Language** - 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 Standard Contractual Clauses** - 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 Standard Contractual Clauses** - 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 Service Control Policy** - 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 Security Domain** - 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 Service Level Objective** 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". *see* [SLA](#)
- SoA Statement of Applicability** – 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 Software Package Data Exchange** - 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 Site Reliability Engineering** – 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 Security, Trust, Assurance and Risk** – 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 Security Token Service** – an [AWS](#) service that issues temporary, limited-privilege credentials for accessing AWS resources, supporting federated identity, cross-account access, and role assumption.. *see* [AWS](#)
- Support Portal** Akka’s online support ticketing/issue system.. [2](#)
- 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 Transfer Impact Assessment** - 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](#)
- 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 Trust Services Criteria** 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 United Kingdom** - 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](#)
- Your Application Services** In the context of Akka’s policies, Your Application Services refers to application components or services developed by the customer to implement their business logic.. [1](#), [2](#)

# Index

Governance	
Governance - Resilience Guarantee .....	1
Governance - Resilience Guarantee Claims .....	2
Governance - Resilience Guarantee	
Governance .....	1
Governance - Resilience Guarantee Claims	
Governance .....	2