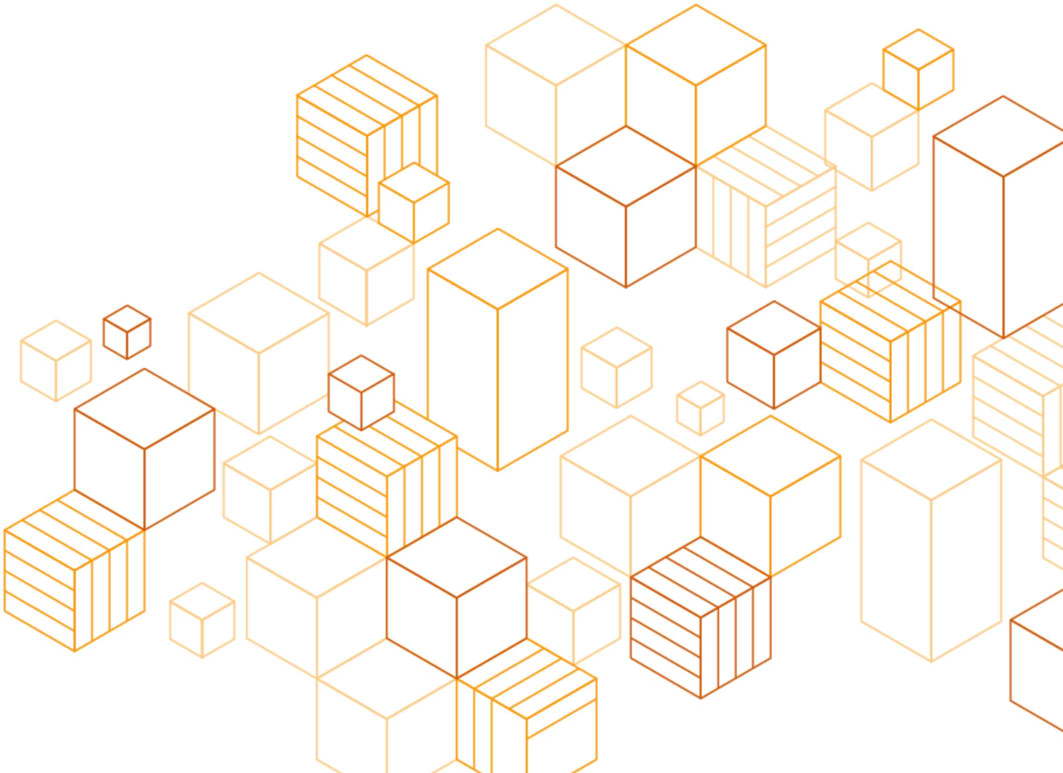
AWS User Guide to Financial Services Regulations and Guidelines in Switzerland

December 2021



Notices

Customers are responsible for making their own independent assessment of the information in this document. This document (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

About this Guide

This guide provides information to assist financial institutions in Switzerland that are regulated by the Swiss Financial Market Supervisory Authority as they accelerate their use of Amazon Web Services' (AWS) services.

This guide:

- Describes the respective roles that the customer and AWS each play in managing and securing the cloud environment;
- Provides an overview of the regulatory requirements and guidance that financial institutions can consider when using AWS; and
- Provides additional resources that financial institutions can use to design and architect their AWS environment to be secure and assist in meeting regulatory expectations.

Overview

This guide refers to certain rules applicable to financial institutions in Switzerland including banks, insurance companies, stock exchanges, securities dealers, portfolio managers, trustees and other financial entities which are overseen (directly or indirectly) by the Swiss Financial Market Supervisory Authority (FINMA).

Amongst other topics this guide covers the requirements created by the following regulations and publications of interest to Swiss financial institutions:

- **Federal Laws** - including Article 47 of the Swiss Banking Act (BA). Banks and Savings Banks, are overseen by FINMA and governed by the BA (Bundesgesetz über die Banken und Sparkassen, Bankengesetz, BankG). Article 47 BA holds relevance in the context of outsourcing.

- Response on cloud usage for Swiss Financial institutions produced by the Swiss Banking Union, Schweizerische Bankiervereinigung SBVg.

- **FINMA** is Switzerland's independent regulator of financial markets. Its mandate is to supervise banks, insurance companies, financial institutions, collective investment schemes, and their asset managers and fund management companies.

This guide is intended to be a resource to help Swiss FSI customers understand the technical and operational requirements when they use AWS services. This guide includes a description of the AWS compliance framework and advanced tools and security measures which Swiss FSI customers can use to evaluate, meet, and demonstrate compliance with their applicable regulatory requirements under Swiss laws, circulars, regulations, and guidelines.

The sections outlined below address the considerations that most frequently arise in interactions with financial institutions and provide information that can be used to better understand the responsibilities of the financial institutions and AWS in regards to cloud outsourcing:

Security and AWS Shared Responsibility Model: It is important that customers understand the AWS Shared Responsibility Model before exploring the specific technical and operational requirements outlined in the cloud outsourcing requirements. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS for security, and informs the steps Swiss FSI customers need to take to ensure they comply with the relevant requirement.

AWS Global Infrastructure: The AWS Global Cloud Infrastructure comprises AWS regions and availability zones. The AWS Global Cloud Infrastructure offers AWS customers an easier and more effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than traditional on-premises environments. AWS customers can use the AWS Global Cloud Infrastructure to design an AWS environment consistent with their business and regulatory needs, including any applicable requirements under the cloud outsourcing requirements.

AWS Compliance Programs: AWS has obtained certifications and third-party attestations for a variety of industry-specific workloads. AWS has also developed compliance programs to make these resources available to customers. Customers can leverage the AWS compliance programs to help satisfy their regulatory requirements. For more information about these third-party certifications and audit reports, see the AWS Compliance Programs webpage

Swiss Regulatory Controls and Federal Laws: This section sets out common considerations for customers that use AWS as they consider some of the key technical and operational requirements under Swiss Regulation, and it describes how customers can leverage AWS services and tools to assist them in complying with their applicable regulatory requirements.

Appendix - AWS Considerations for FINMA Circulars: Provides a list of requirements and corresponding considerations.

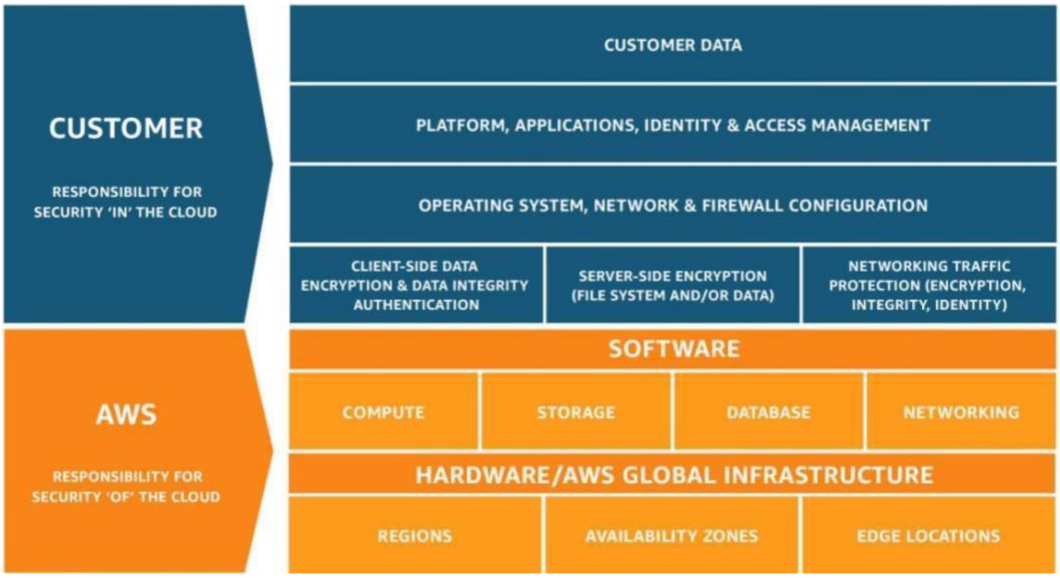
This guide focuses on typical security-related questions asked by AWS customers when considering Swiss laws, circulars, regulations, and guidelines and their use of AWS services.

The aim of this guide is to guide financial institutions to perform due diligence and apply sound governance and risk management practices to their outsourcing of a material business activity, including via their use of AWS cloud services.

This document is provided for informational purposes only; it is not legal advice and should not be relied on as legal advice. As customers' requirements will differ, AWS encourages its customers to obtain appropriate advice on their compliance with all regulatory and legal requirements that are relevant to their business, including in relation to Swiss laws, circulars, regulations, and guidelines.

Security and AWS Shared Responsibility Model

It is important that financial institutions understand the AWS Shared Responsibility Model before navigating their operational and technical requirements under Swiss laws, circulars, regulations, and guidelines. Cloud security is a shared responsibility. AWS manages security of the cloud by ensuring that AWS Cloud Infrastructure complies with global and regional regulatory requirements and best practices, but security in the cloud is the responsibility of the customer. Namely, AWS customers retain control of the security programs that they choose to implement to protect their content, applications, systems, and networks, as they would for applications in an on-premises data center.


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Shared Responsibility Model

The Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles. AWS operates, manages, and controls the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities.

Contractual compliance

Swiss financial institutions who run material workloads on a cloud service provider are, in some cases, required to ensure that the outsourcing contracts between themselves and the cloud service provider include all necessary provisions that are required to ensure the control environment is appropriately designed and implemented to address key operational risks, as well as risks related to outsourcing and business continuity management.

In some circumstances, and for some customers, these provisions include proper service descriptions and service level agreements (SLAs), rights to issue instructions, data protection, termination arrangements, sub-outsourcing arrangements, information obligations, the applicable jurisdiction, and other specific rights for the financial institution and its regulator. AWS can discuss individual customer requirements to address these respective requirements with customers.

The **AWS Customer Agreement** is the foundational contractual document which contains the terms and conditions that govern customer's access to and use of AWS Services and is provided by AWS (https://aws.amazon.com/agreement/).

The **AWS Online Service Terms** (https://aws.amazon.com/service-terms/) govern the use of the AWS Services and provide additional terms which apply to your use of specific services.

The **AWS Financial Services Addendum (FSA)** provides financial services customers provisions to assist them in meeting regulatory requirements and can be provided to customers with an AWS Customer Agreement where required. The Swiss Financial Services Addendum provides Swiss regulated customers with contractual clauses (in addition to those provided in the AWS Customer Agreement). Please reach out to your AWS account team for details.

The **AWS GDPR Data Processing Addendum (DPA)** is part of the AWS Service Terms. This means all AWS customers globally can rely on the terms of the AWS GDPR DPA since May 25, 2018, whenever they use AWS services to process personal data under the GDPR. The AWS GDPR DPA also includes EU Model Clauses, which were approved by the European Union (EU) data protection authorities, known as the Article 29 Working Party. This means that AWS customers wishing to transfer personal data from the European Economic Area (EEA) to other countries can do so with the knowledge that their personal data on AWS will be given the same high level of protection it receives in the EEA. For more information about the GDPR Data Processing Addendum visit https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/. The AWS GDPR addendum and the AWS Supplementary Addendum applies to customer's use of AWS Services in processing Customer Data and is available as part of AWS's service terms.

AWS is always vigilant about customer privacy and security, and is committed to providing customers with industry-leading privacy and security protections when using our products and services. When a request for content is received from law enforcement, it is carefully examined to authenticate accuracy and to verify that it complies with applicable law. Where there is a need to act to protect customers, AWS will continue to do so. AWS has a history of challenging government requests for customer information that it believes are overbroad or otherwise inappropriate.

If AWS are required to disclose customer content, it will continue to notify customers before disclosure to provide them the opportunity to seek protection from disclosure, unless prohibited by law. AWS is transparent about the number of requests it receives.

Security in the Cloud

Customers are responsible for their security in the cloud. AWS customers are responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as any applicable network security controls.

Customers should carefully consider the services they choose, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations. It is important to note that when using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS.
- The AWS services that they use with the content.
- The country where they store their content.
- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How they encrypt their data and where they store their keys.
- Who has access to their content and how those access rights are granted, managed, and revoked.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customer responsibility is determined by the AWS Cloud services that a customer selects.

This selection, in turn, determines the amount of configuration work the customer must perform as part of their security responsibilities.

For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks.

Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using Identity and Access Management (IAM) tools to apply the appropriate permissions.

Security of the Cloud

AWS infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use AWS compliance certifications to validate the implementation and effectiveness of AWS security controls, including internationally-recognized security best practices and certifications. You can learn more by downloading the whitepaper AWS & Cybersecurity in the Financial Services Sector.

The AWS compliance program is based on the following:

- **Validating** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that customers can implement, and to better assist customers with managing their control environment.
- **Demonstrating** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with information regarding the policies, processes, and controls established and operated by AWS. Customers can use this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.

- **Monitoring**, through applicable security controls, that AWS maintains compliance with global standards and best practices.

AWS Global Infrastructure

The AWS Global Cloud infrastructure comprises AWS Regions and Availability Zones. A Region is a physical location in the world, consisting of multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, all housed in separate facilities. These Availability Zones offer customers the ability to operate applications and databases, which are more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment. Customers can learn more about these topics by downloading our Whitepaper on Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

The C5 report, covered later in this document is available for download from AWS Artifact. It lists the locations of AWS availability zones within the region, giving Swiss customers further transparency to the location of AWS Regions and Availability Zones in Europe.

AWS customers choose the AWS Region(s) in which their content and servers are located. This allows customers to establish environments that meet specific geographic or regulatory requirements. Additionally, this allows customers with business continuity and disaster recovery objectives to establish primary and backup environments in a location or locations of their choice. More information on our disaster recovery recommendations is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud

The **AWS Europe (Zurich)** region will be available in 2022. The region will have three Availability Zones designed and built to meet rigorous compliance standards globally, providing high levels of security for all AWS customers. As with every AWS Region, the Europe (Zurich) Region will be compliant with applicable global data protection laws. This will allow customers to store data within Switzerland, and reduce latency to their Swiss customers.

AWS Compliance Programs

Certifications and Third-Party Attestations

AWS has obtained certifications and independent third-party attestations for a variety of industry specific workloads. However, the following are of particular importance to financial institutions:

ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System, which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.

ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional information security controls implementation guidance specific to CSPs. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.

ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to Personally Identifiable Information (PII) in the public cloud. It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.

ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. The key to the ongoing certification under this standard is establishing, maintaining, and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, see the ISO 9001 Compliance webpage.

PCI DSS Level 1 the Payment Card Industry Data Security Standard (also known as PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.

SOC - System and Organization Controls (SOC) reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls established to support operations and compliance. For more information, see the SOC Compliance webpage. There are three types of AWS SOC Reports:

- **SOC 1:** Provides information about the AWS control environment that may be relevant to a customer's internal controls over financial reporting as well as information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).
- **SOC 2**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
- **SOC 3**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system confidentiality, integrity and availability without disclosing AWS internal information.

C5: Cloud Computing Compliance Controls Catalog (C5) is a German Government-backed attestation scheme introduced in Germany by the Federal Office for Information Security (BSI) to help organizations demonstrate operational security against common cyber-attacks within the context of the German Government's "Security Recommendations for Cloud Providers". The C5 attestation can be used by AWS customers and their compliance advisors to understand the range of IT-Security assurance services that AWS offers as they move their workloads to the cloud. C5 adds the regulatory defined IT-Security level equivalent to the IT-Grundschutz with the addition of cloud specific controls.

The C5 attestation includes additional control requirements relating to data location, service provisioning, place of jurisdiction, existing certification, information disclosure obligations, and a full-service description.

Using this information, customers can evaluate how legal regulations (i.e., data privacy), their own policies, or the threat environment relate to their use of cloud computing services. For more information, see the C5 Compliance webpage.

FINMA ISAE 3000 Type 2: The FINMA ISAE 3000 Type 2 Report, conducted by an independent third-party audit firm, provides Swiss financial industry customers with the assurance that AWS' control environment is appropriately designed and implemented to address key operational risks and risks related to outsourcing and business continuity management. Additionally, the report provides customers with important guidance on complementary user entity controls (CUECs), which they should consider implementing as part of AWS' Shared Responsibility Model to help them comply with FINMA's control objectives. The report covers the five core FINMA circulars that are applicable to Swiss financial services institutions in the context of outsourcing arrangements to the cloud.

The C5 report and FINMA ISAE 3000 Type 2 report both refer to the AWS control environment and AWS control activities (AWSCA). The terms, "Control Environment" and "Control Activities", are defined by the American Institute of Certified Public Accountants (AICPA):

Control Environment – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

Control Activities – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's control objectives are effectively carried out.

By tying together governance-focused, audit-friendly service features with such certifications, attestations and audit standards, AWS Compliance enablers build on traditional programs and help customers to establish and operate in an AWS environment. For more information about other AWS certifications and attestations, see the AWS Compliance Program webpage. For information about general AWS security controls and service-specific security, see the Best Practices for Security, Identity, & Compliance.

AWS Artifact

Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance-reporting portal available in the AWS Management Console.

The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

AWS Security and Audit Series

The AWS Security and Audit Series offers Swiss financial services customers that are subject to the FINMA controls options to engage directly with AWS on audit, compliance, and security matters. These offerings are designed to be executed in sequence, starting with the Compliance Briefings, in order to deepen customers' understanding and to maximize interactions with AWS experts and compliance artifacts.

The FINMA controls outline multiple ways in which Swiss financial institutions can exercise their audit and access rights with regards to their third-party service providers. The AWS Security and Audit Series is designed to provide AWS' Swiss financial services customers that are subject to the FINMA controls with tailored options for developing an ongoing relationship with AWS Security. In all engagements, AWS Security seeks to deepen transparency and provide avenues for direct and continued interaction with AWS to give customers assurance that they are adopting the AWS Cloud in a secure, compliant, and informed manner.

These options address our customers' security and compliance concerns on an ongoing basis, while providing necessary assurances to support the secure adoption, migration, and use of AWS services.

Compliance Briefings

Compliance Briefings offer customers regular opportunities to engage directly with AWS on audit, compliance, and security matters.

Compliance Briefings allow customers to address their security or compliance questions or concerns to AWS Security & Compliance Specialists, who are appropriately qualified and knowledgeable AWS personnel. The content of Compliance Briefings is tailored directly to customers' needs. Discussion topics may include, but are not limited to:

- The application of the AWS Shared Responsibility Model
- Deep dives into AWS audit reports and certifications
- Matters pertaining to the AWS control environment
- Best practices for secure architecture

AWS Audit Symposium

The AWS Audit Symposium is a four-day event designed to enable AWS customers to perform direct audit of AWS on a continual basis. The AWS Audit Symposium offers deepened transparency into the AWS control environment and direct engagement with AWS evidence artifacts accessed by AWS auditors during assessments.

Prior to each AWS Audit Symposium, customers request both topics for discussion, as well as specific controls from the AWS control framework they wish to see explained and demonstrated by AWS control owners. An AWS Audit Symposium offers customers opportunities to review evidence supporting AWS audit and compliance programs, ask questions of AWS Security, provide feedback around the effectiveness of AWS controls, and submit requests for future control modifications.

The agenda of each AWS Audit Symposium is subject to change, as agendas are tailored to meet the specific needs and requirements of attending AWS customers. Additionally, audit artifacts are available for customers' independent review throughout the duration of the AWS Audit Symposium, and customers can request breakout sessions with AWS personnel at any time to discuss topics and questions specific to their institution.

An AWS Audit Symposium is offered at least quarterly and limits attendance to three customer audit employee representatives. At the discretion of AWS, customers have an option to bring additional attendees.

Community Audit

A Community Audit is a pooled audit executed by a customer-chosen, reputable, and independent auditor performing testing of the AWS environment on behalf of a group of customers. These audits can be either based on an existing AWS audit program (e.g., C5), or a set of controls driven by the members of the community. A Community Audit provides financial, regulatory, and time efficiencies to the institutions represented by the community, where all members input into the audit scope while mutually benefitting from sharing the cost and effort of a single audit. Community Audits additionally serve to minimize audit duration while increasing overall control transparency, ensuring the highest bar of assurance for the most security-conscious Community member.

Individual Audit

Through Individual Audits, AWS offers customers the ability to directly execute an audit with AWS.

These audits are based on customer-defined controls, as agreed upon with AWS, and are performed by qualified representatives from the customer's audit team or a third party designated by the customer to assess AWS on their behalf.

After initiating an Individual Audit, AWS will contact customers to schedule a Compliance Briefing to walk through the audit process, provide an initial overview of the AWS control environment, determine the greatest areas of concern for the audit, identify needed timelines, and discuss audit pricing.

AWS and customers will establish the full scope of the audit. We encourage customers to attend an AWS Audit Symposium prior to initiating any onsite Individual Audit activities with AWS to gain an in-depth overview of the AWS control environment, help satisfy as many audit requests as possible, and direct future evidence requests for a future onsite visit.

Core Regulatory Bodies, Laws, and Regulations

Article 47 of the Banking Act

Disclaimer: This guide focuses on typical security-related questions asked by AWS customers when considering Swiss laws, circulars, regulations and guidelines and their use of AWS services. To guide financial institutions to perform due diligence and apply sound governance and risk management practices to their outsourcing of a material business activity, including via their use of AWS cloud services. This document is provided for informational purposes only; it is not legal advice and should not be relied on as legal advice. As customers' requirements will differ, AWS encourages its customers to obtain appropriate advice on their compliance with all regulatory and legal requirements that are relevant to their business, including in relation to Swiss laws, circulars, regulations, and guidelines.

Customers should note that Article 47 BA, in substance, states that it is prohibited to disclose confidential information entrusted or acquired in one's capacity as a member of an executive or supervisory body, employee, delegate, agent, attorney, representative, auditor or liquidator of a bank, or a person or entity active in the financial sector and calling for or accepting deposits from the public on a professional basis. Any violation or attempt to induce a violation of the confidentiality obligation (even in case of negligence) is sanctioned by a fine or imprisonment of up to three years (or up to five years if the violation is performed with an enrichment purpose). In such context, the decisive factor is the client's interest in maintaining banking secrecy and no other conditions should be considered.

However, anonymous information, for example information that cannot be traced back to a specific natural or legal person because it has been encrypted, is not protected by Article 47 BA. Moreover, in order for 47 BA to apply, there has to be a certain disclosure of the confidential information. That is, an unauthorized third party has actual knowledge of the confidential information.

In this context, outsourcing is in principle admissible when the client-identifying data has been encrypted and is not accessible to a third party. Furthermore, outsourcing is usually considered admissible if the data is not encrypted and the client has not given its consent, but the outsourcing: (i) serves a reasonable interest of the financial institution, (ii) covers the delegation of auxiliary tasks, (iii) is made under the financial institution's supervision; and (iv) is not expressly excluded by a contractual arrangement.

In any case, financial institutions subject to banking secrecy under Article 47 BA must comply with their duty of care and loyalty when outsourcing services that include clients' data, as well as with all relevant laws, regulations and recognized professional standards.

Such standards are, among other, issued by the Swiss Bankers Association[1], an umbrella organisation of Swiss financial institutions, made up of the majority of banks in Switzerland.

One of the goals of the Swiss Banking Association is to interpret laws, circulars and frameworks and represent the interests of its members in Switzerland and abroad.

In June 2020, the Swiss Bankers Association released a second version of the paper Cloud-Leitfaden Wegweiser für sicheres Cloud Banking (Cloud Guidelines. A guide to Secure Cloud Banking) or SBVg Guidelines providing guidance to financial institutions when using cloud computing services.

The SBVg Guidelines are divided into four key sections, namely:

- Choosing and changing cloud providers and subcontractors;
- Maintaining banking secrecy in the cloud;
- Transparency and collaboration between institutions and cloud providers with regard to measures ordered by the authorities and the courts; and
- Audit of the cloud services and infrastructures used to deliver them.

The four sections of the SBVg Guidelines closely align to AWS technical and organizational measures.[2]

The SBVg Guidelines acknowledges the potential of cloud computing for banks and the ability of cloud computing to democratize IT, giving smaller financial institutions the same access to IT and IT security as larger institutions.

The paper makes some non-legally binding recommendations around governance, data processing, authorities and proceedings, auditability and traceability to enable the use of cloud computing (including from cloud providers with data centers **outside of Switzerland**) while still being compliant with Swiss regulations.

[1] https://www.swissbanking.ch/en

[2] https://aws.amazon.com/compliance/

In addition to the SBVg Guidelines, the Swiss Banking Association has also made available for consultation on their website a legal opinion produced by Laux Lawyers on the extent to which financial institutions may use cloud services under Article 47 BA[3]. AWS in no way endorses this opinion or suggests that customers rely on it. The link is provided for informational purposes only.

Security Assurance programs provided by AWS can allow you to establish appropriate central control systems and procedures to allow you, relying on your own legal advice, to comply with article 47 of the BA. AWS gives you ownership and control over your content through simple, powerful tools that allow you to determine where your content will be stored, secure your content in transit and at rest, and manage your access to AWS services and resources for your users. We also implement responsible and sophisticated technical and physical controls that are designed to prevent unauthorized access to or disclosure of your content.

As mentioned in the section Security and AWS Shared Responsibility Model, a reasonable security standard to protect bank client's confidentiality is the responsibility of the bank and AWS.

AWS provides Customers with evidence of its compliance with applicable legal, regulatory, and contractual requirements through audit reports, attestations, certifications and other compliance enablers. The FINMA ISAE 3000 Type 2 report verifies that AWS's control environment is appropriately designed and implemented to align with certain Swiss Financial Market Supervisory Authority (FINMA) requirements applicable to regulated financial services customers in Switzerland. visit https://aws.amazon.com/artifact/ for information on how to review the AWS external attestation and assurance documentation.

AWS provides customers with the ability to properly configure and use the AWS service offerings in order to maintain appropriate security, protection, and backup of content, which may include the use of encryption technology to protect content from unauthorized access. Customers maintain full control and responsibility for configuring access to their data.

The FINMA section below and appendices give a detailed overview of technical and organizational measures, with focus on data protection to comply with technical security controls set forth by the five FINMA circulars.

[3] https://www.lauxlawyers.ch/en/rechtsgutachten-bankgeheimnis-und-cloud/ and https://www.swissbanking.ch/_Resources/Persistent/2/6/c/6/26c6140bc424e416ad9c2dbe67d9dea2d2e7c3b6/SBA_Permissibility_of_disclosure_by_Swiss_banks_of_bank_client_information_to_agents_in_foreign_countries_V020b_EN.pdf

AWS has developed a security assurance program that uses best practices for global privacy and data protection to help you operate securely within AWS, and to make the best use of our security control environment.

These security protections and control processes are independently validated by multiple third-party independent assessments (see also https://aws.amazon.com/artifact/).

FINMA

FINMA is Switzerland's independent financial-markets regulator. Its mandate is to supervise banks, insurance companies, financial institutions, collective investment schemes, and their asset managers and fund management companies. It also regulates insurance intermediaries.

It is charged with protecting creditors, investors and policyholders. FINMA is responsible for ensuring that Switzerland's financial markets function effectively.[4]

FINMA is responsible for ensuring that Switzerland's financial markets function effectively and publishes FINMA circulars explaining how it applies financial market legislation in carrying out its supervisory duties. FINMA is bound by its circulars when applying the law. It issues its individual decisions based on the applicable financial-market law and in accordance with the relevant circulars. [5]

The following five FINMA circulars are issued by FINMA and intended by FINMA to assist regulated financial institutions in understanding approaches to due diligence, third party management, and key technical and organizational controls that should be implemented in cloud outsourcing arrangements, particularly for material workloads.

- 2018/03 FINMA Circular "Outsourcing – banks and insurers" (31.10.2019);
- 2008/21 FINMA Circular "Operational Risks – Banks" (31.10.2019) – Principal 4 Technology Infrastructure;
- 2008/21 FINMA Circular "Operational Risks – Banks" (31.10.2019) – Appendix 3 Handling of electronic Client Identifying Data;
- 2013/03 "Auditing" (04.11.2020) - Information Technology (21.04.2020);

[4] https://www.finma.ch/en/finma/finma-an-overview/

[5] https://www.finma.ch/en/documentation/circulars/

- Business Continuity Management (BCM) minimum standards proposed by the Swiss Insurance Association (01.06.2015) and Swiss Bankers Association (29.08.2013)

“Circular 2018/3 Outsourcing – banks and insurers” defines the supervisory requirements applicable to outsourcing solutions at banks, securities dealers, and insurance companies in terms of appropriate organisation and risk limitation.[6] The circular outlines requirements and duties for “the company”—the AWS customer—and the “service provider” or “outsourcer”—AWS. The AWS Shared Responsibility model outlines how cloud security is a shared responsibility between the customer and AWS.

FINMA provides that all significant functions, with some exceptions, may be outsourced. Outsourcing activities must be aligned with the requirements set forth by that circular and include the following categories:

- Inventory of outsourced functions
- Selection, instruction and monitoring of the service provider
- Outsourcing within a group or conglomerate
- Responsibility
- Security
- Audit and Supervision
- Outsourcing to another country
- Agreement

FINMA further defines guiding principles with respect to the handling of electronic client data within “**Circular 2008/21, Operational Risk – Banks, Annex 3**”. As the title of the circular suggests, those principles apply to banks and not insurers. Circular 2008/21 stipulates that the confidentiality of client identifying data (CID) must be a decisive criterion and an integral component of the underlying due diligence upon selecting a provider of outsourcing services such as AWS.

The customer can demonstrate that workloads are appropriately designed and implemented to address key operational risks, as well risks related to outsourcing and business continuity management described by the FINMA circulars.

[6] https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-03-01012021_de.pdf?la=en

The customer demonstrates this by producing evidence and assurance that both the **AWS control environment** and the **complementary user entity controls (CUEC)** comply with the FINMA objectives (sometimes referred to as controls or margins) outlined in the above 5 circulars.

The relationship between CUECs and the AWS control environment relates closely to the AWS Shared Responsibility Model. The CUECs are controls describing the “in the cloud” commitment of the customer. The AWS control environment describes the AWS responsibility for the “of the cloud” commitment. AWS provides customers a wide range of information on its IT control environment in whitepapers, reports, certifications, accreditations, and other third-party attestations.

The ISAE 3000 Type 2 report is conducted with an independent auditor registered in Zurich, Switzerland. The report, accessed via AWS Artifact, has 22 regions in scope and 124 services in scope. The FINMA ISAE 3000 Type 2 report, conducted by an independent auditor in Zurich, provides Swiss financial industry customers with assurance that the AWS control environment is appropriately designed and implemented to address key operational risks, as well as risks related to outsourcing and business continuity management.

The AWS control environment is described by a series of AWS control activities (AWSSCA) which are divided into 5 main areas: Policies (Control Environment and Risk Management), Communications (Communication and Information), Service Commitments, Procedures (Control Activities), and Monitoring. In the ISAE 3000 Type 2 report the auditor examines all of the AWS Control Activities against FINMA controls (requirements) outlined in the five circulars and tracks whether deviations are noted or not.

The ISAE 3000 report also highlights CUECs for the customer but the detail mainly focuses on the AWS controls (as it is AWS that is being evaluated). Both the CUECs and the AWS Control environment are of importance to FSI customers and FINMA. Similar to the Shared Responsibility Model AWS provides tools to the customer to support them on their side of the shared responsibility model for FINMA—the CUECs in this case.

The Appendix of this document contains a table for FINMA Circular “2018/03 - V. Requirements for outsourcing companies”. The table caters to both the AWS Control Activities and the CUECs and has three columns:

> **Requirement:** Lists the requirements or controls mandated by FINMA.
>
> **Customer:** Lists best practices for security in the cloud from the AWS Well-Architected Framework that customers can implement as a starting point to support their compliance efforts. Details on each best practice and associated

AWS services that customers may leverage can be found in the AWS Well-Architected Framework. The Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars—operational excellence, security, reliability, performance efficiency, and cost optimization—the Framework provides a consistent approach for customers to evaluate architectures, and implement designs that will scale over time.

AWS: Lists AWS controls evaluated by a Swiss independent auditor for that FINMA control.

General Data Protection Regulation (GDPR)

The European Union’s General Data Protection Regulation (GDPR) protects European Union data subjects' fundamental right to privacy and the protection of personal data. It introduces robust requirements that will raise and harmonize standards for data protection, security, and compliance.

All AWS Services are GDPR ready.

AWS is always vigilant about customer privacy and security, and is committed to providing customers with industry-leading privacy and security protections when using AWS products and services.

In addition to its own compliance, AWS is committed to offering services and resources to AWS customers to help them comply with GDPR requirements that may apply to their activities. New features are launched regularly, and AWS has 500+ features and services focused on security and compliance.

Detailed information on AWS Services readiness for GDPR can be found at https://aws.amazon.com/compliance/gdpr-center/.

Data Residency

Data residency is a requirement imposed whereby customer content processed and stored in an IT system must remain within a specific country's borders, and it can be one of the foremost concerns of many organizations that want to use commercial cloud services. General cybersecurity concerns and concerns about government requests for data have contributed to a continued focus of some governments on keeping data within countries' borders.

Customers maintain full control of their content and responsibility for configuring access to AWS services and resources. AWS provides an advanced set of access, encryption, and logging features to help customers do this effectively. The customer chooses the AWS Region(s) in which their content is stored and the type of storage. The customer can replicate and back up the content in more than one AWS Region. AWS does not move or replicate the content outside of the chosen AWS Region(s) without the consent of the customer, except in each case as necessary to comply with the law or a binding order of a governmental body. For more information on this topic please see the data privacy FAQ.

The SBVg states in their cloud leitfaden paper that *"The cloud is a critical success factor for Switzerland and its financial centre."* For customers that wish to retain data in Switzerland, AWS will provide a Swiss region. Customers that want to retain their data in Switzerland can also use services such as AWS Outposts and AWS Snowball.

A separate white paper on data residency addresses the real and perceived security risks expressed by governments when they demand in-country data residency by identifying the most likely and prevalent IT vulnerabilities and security risks, explaining the native security embedded in cloud services, and highlighting the roles and responsibilities of cloud service providers (CSPs), governments, and customers in protecting data.

A second whitepaper Using AWS in the Context of Common Privacy & Data Protection Considerations covers data lifecycle stages and how it relates to Common Privacy and Data Protection Considerations.

Strengthened Contractual Commitments

When AWS receives a request for content from law enforcement, it is carefully examined to authenticate accuracy and to verify that it complies with applicable law. Where AWS needs to act to protect customers, it will continue to do so. AWS has a history of challenging government requests for customer information that AWS believes are overbroad or otherwise inappropriate.

If AWS is required to disclose customer content, AWS will continue to notify customers before disclosure to provide them the opportunity to seek protection from disclosure, unless prohibited by law. AWS is transparent about the number of requests that it receives.

Our **strengthened contractual commitments** include:

- **Challenging law enforcement requests**: AWS will challenge law enforcement requests for customer data from governmental bodies, whether inside or outside the EEA, where the request conflicts with EU law, is overbroad, or where AWS otherwise has any appropriate grounds to do so.
- **Disclosing the minimum amount necessary**: AWS also commits that if, despite challenges, it is ever compelled by a valid and binding legal request to disclose customer data, it will disclose only the *minimum amount* of customer data necessary to satisfy the request.

These commitments are automatically available to all customers using AWS to process their customer data, with no additional action required, through a new supplementary addendum to the AWS GDPR Data Processing Addendum.

Data Encryption

Encryption is a fundamental technical and organizational measure to protect data and prevent unauthorized access.

AWS provides cryptographic services to enable a wide range of encryption and storage technologies that can assure the integrity of your data at rest or in transit

Encrypt data in your applications

The AWS Encryption SDK (ESDK) is a client-side encryption library to help you implement best-practice encryption and decryption within your application locally, using industry standards and best practices.

Using simple APIs you can also build encryption and key management into your own applications wherever they run.

Since the security of your encryption is only as strong as the security of your key management, the ESDK integrates with the AWS Key Management Service (AWS KMS), though the ESDK doesn’t require you to use any particular source of keys. Get started with client side encryption here.

Manage encryption for AWS services

AWS Key Management Service is integrated with AWS services to simplify using your keys to encrypt data across your AWS workloads. You choose the level of access control that you need, including the ability to share encrypted resources between accounts and services. AWS KMS logs all use of keys to AWS CloudTrail to give you an independent view of who accessed your encrypted data, including AWS services using them on your behalf.

Encryption Key Management

When choosing AWS KMS related AWS cryptographic services, there are three options for encryption key management:

- AWS KMS with customer or AWS-managed keys
- AWS KMS with BYOK (KMS Import key)
- AWS KMS with a KMS custom key store key management backed by CloudHSM

Every AWS cryptographic service is backed by a FIPS 140-2 validated HSM. With AWS KMS, your keys are generated and managed on AWS operated multi-tenant HSMs. You access these keys and cryptographic operations using the KMS service API. AWS KMS also offers complete control over where you generate and store your encryption keys.

If your compliance or internal policies must demonstrate control over your encryption key generation process, such as provable encryption key entropy, AWS KMS offers an option to bring your own key (BYOK). If you want the convenience and integration of KMS but require a single-tenant HSM under your control for the root of trust, AWS KMS offers custom key stores. Once you create a key in AWS KMS, KMS applies access control through identity and resource policies, integrity checks, and AWS CloudTrail. Using the available AWS technologies, you can ensure that your encryption key usage follows the restrictions you've specified and in a manner consistent with cryptographic best practices.

Learn more about demystifying KMS Key operations here.

If you need a FIPS 140-2 Level 3 validated HSM, you can use an AWS CloudHSM that you control with your Amazon Virtual Private Cloud (Amazon VPC). With this approach, you need to develop functionality for your applications to access your CloudHSMs. AWS CloudHSM a service for creating and managing cloud-based hardware security modules. A hardware security module (HSM) is a specialized security device that generates and stores cryptographic keys.

FINMA ISAE 3000 Type 2 report & Encryption

The FINMA ISAE 3000 Type 2 report, accessed via AWS Artifact, has a series of AWS Control activities related to AWS cryptographic services.

The following control activities are mapped to the requirements of the FINMA Circulars 2018/03 "Outsourcing – banks and insurers" (31.10.2019), 2008/21 Operational risks– Banks (31.10.2019) - Principal 4 Technology Infrastructure and Appendix 3 Handling of electronic Client Identifying Data, 2013/03 "Auditing" (04.11.2020) – Information Technology (21.04.2020) and Business Continuity Management (BCM) minimum standards proposed by the Swiss Insurance Association (01.06.2015) and Swiss Bankers Association (29.08.2013):

Control Id	Detail
AWSCA-4.5	Customer master keys used for cryptographic operations in KMS are logically secured so that no single AWS employee can gain access to the key material.
AWSCA-4.6	AWS Services that integrate with AWS KMS for key management use a 256-bit data key locally to protect customer content.
AWSCA-4.7	The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit AES master key unique to the customer's AWS account.
AWSCA-4.8	Requests in KMS are logged in AWS CloudTrail.
AWSCA-4.9	KMS endpoints can only be accessed by customers using TLS with cipher suites that support forward secrecy.
AWSCA-4.10	Keys used in AWS KMS are only used for a single purpose as defined by the key_usage parameter for each key.

Control Id	Detail
AWSCA-4.11	Customer master keys created by KMS are rotated on a defined frequency if enabled by the customer.
AWSCA-4.12	Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
AWSCA-4.13	Access attempts to recovery key materials are reviewed by authorized operators on a monthly cadence.
AWSCA-4.14	The production firmware version of the AWS Key Management Service HSM (Hardware Security Module) has been validated with NIST under the FIPS 140-2 standard or is in the process of being validated.

Business Continuity

Business continuity and disaster recovery strategies are important aspects to be considered by customers, and especially customers planning to host material workloads on AWS. Within such strategies, customers should plan for disaster events (such as natural disasters like earthquakes or floods, technical failures such as power failure or network connectivity or human actions) and how to recover from such events.

Business continuity and disaster recovery is a shared responsibility between AWS and customers. The planning for such events by AWS is validated within the FINMA ISAE 3000 report to meet specific requirements set forth by FINMA in this area. It is the responsibility of customers to architect their workloads on top of that validated infrastructure to meet the overall objectives set forth in that domain.

AWS Global Infrastructure

The AWS Global Cloud infrastructure comprises AWS Regions and Availability Zones. A Region is a physical location in the world, consisting of multiple Availability Zones.

Availability Zones (AZs) consist of one or more discrete data centers, each with redundant power, networking, and connectivity, all housed in separate facilities. AZs are physically separated by a meaningful distance, many kilometres from any other AZ, as audited within the C5 report where more transparency is provided on AWS Regions and AZ locations.

Availability Zones offer customers the ability to operate applications and databases, which are more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment. Customers can learn more about these topics by downloading our Whitepaper: Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

AWS customers choose the AWS Region(s) in which their content and servers are located. This allows customers to establish environments that meet specific geographic or regulatory requirements.

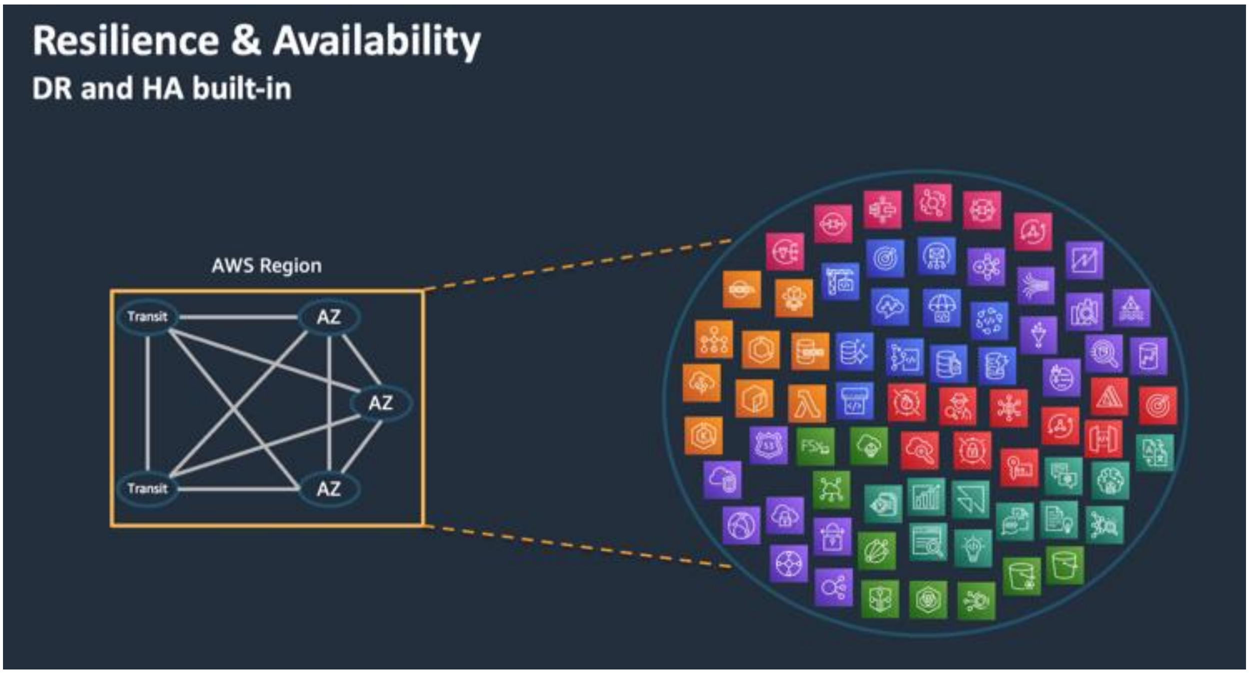
Additionally, this allows customers with business continuity and disaster recovery objectives to establish primary and backup environments in a location or locations of their choice.

More information on our disaster recovery recommendations is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

To better isolate any issues and achieve high availability, the customer can partition applications across multiple availability zones in the same region. In addition, AWS control planes and the AWS management console are distributed across regions, and include regional API endpoints, which are designed to operate securely for at least 24 hours if isolated from the global control plane functions without requiring customers to access the region or its API endpoints via external networks during any isolation.

What is meant by meaningful distance between availability zones in our documentation?

Physical events like fire, flood, storms can impact & cause failure to infrastructure. AWS availability zones have been designed with this in mind.



Resilience & Availability

DR and HA built-in

As shown above, all availability zones (AZ) in an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fiber providing high-throughput, low-latency networking between zones. All traffic between availability zones is encrypted. The network performance is sufficient to accomplish synchronous replication between zones. Availability zones simplify the process of partitioning applications for high availability. This means many AWS Services, for example Amazon S3, AWS Lambda, AWS DynamoDB, Amazon Relational Database Service can withstand the temporary lack of access to an availability zone.

Many customers need to build highly stateful realtime applications and have strict SLAs they need to pass onto their customers. When you are trying to keep realtime data consistent with strong or eventual consistency, latency matters.

With a synchronous strategy the latency between replicas will directly impact your maximum transaction rate. With an asynchronous strategy the higher the latency the more out of date your replicas will be.

All modern realtime applications seek to provide high transaction rates and seek to provide realtime data to their users and customers. To address this, datacenters in availability zones could be brought closer together. However, there is a trade-off, the further apart you put two datacenters the less likely they are impacted by a single physical event. The further apart locations and infrastructure are the more unlikely a physical event can impact datacenters in the same availability zones. However, adding distance adds latency. The further apart data centers are placed the more latency is introduced from 10s of microseconds all the way up to milliseconds.

AWS designs availability zones with this balance in mind; risk—the further away the better—and latency. When selecting separation distances, we typically target a latency round trip of around 1 millisecond.[7]

The C5 report, available for download from AWS artifact, lists the locations of AWS availability zones within the region, giving customers further transparency to the AWS global infrastructure and availability zone selection.

Disaster Recovery Options

An AWS region is typically composed of 3 Availability Zones (AZs), one Availability Zone can contain many physically separated datacenters. Therefore, a single AWS Region with workloads deployed across the different AZs of that Region is sufficient to architect solutions mitigating large scale disasters affecting single datacenters (for example, fire, floods, earthquakes).

If the objective set forth by the customer is to mitigate disaster events that include the risk of losing multiple data centers and AZs (with a significant distance between each other), further options exist.

One option to mitigate such risks is using multiple AWS Regions. Using multiple AWS Regions allows customers to setup different models and strategies for disaster recovery and depending on the RTO and RPO, the most adequate solution can be chosen by the customer:

[7] Pete DeSantis's Infrastructure Keynote at Re:Invent 2020 (starts at 17:46 min. mark)

https://www.youtube.com/watch?v=AaYNwOh90Pg&t=1054s

- Backup and Restore: using this model, customer backup data and recovery capabilities are in a second region (the backup region). All the data is replicated to the backup region and plans can be developed to restore services within that region using the backed-up data.
- Pilot Light: within this model, not only data is replicated to a second AWS region, but core services and workloads are pre-provisioned. This allows to decrease drastically the time required to operate the services in the secondary region as opposed to only backup data (and improve the recovery time).
- Multi-region active/active or active/passive: this model operates the full infrastructure in the secondary region. Either using the secondary region in an active mode (i.e., serving and processing end customer requests on it) or in a passive mode (i.e., using the secondary region only in case of disaster events).

A potential challenge faced by Swiss FSI customers of AWS is when cross-region replication is not desired. In such cases where the risk of losing multiple data centers and availability zones needs to be mitigated, hybrid architectures can be considered. Such hybrid architectures might be:

- Using on-premise infrastructure as recovery option: AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations to establish a reliable private link between an on-premise data center and an AWS region. This connection can be used to establish a "Backup and Restore" or "Pilot Light" model as a disaster recovery strategy using the on-premise environment as the disaster recovery option.
- AWS Outposts is a fully managed service that offers the same AWS infrastructure, AWS services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility for a truly consistent hybrid experience. AWS Outposts is ideal for workloads that require low latency access to on-premises systems, local data processing, data residency, and migration of applications with local system interdependencies.
- The AWS Partner Network (APN) is the global community of Partners who leverage Amazon Web Services to build solutions and services for customers. AWS helps Partners build, market, and sell their AWS offerings by providing valuable business, technical, and marketing support. AWS Technology Partners, such as NetApp and CloudEndure (an Amazon Web Services Company), can support a Swiss FSI customer with their hybrid architectures.

If customers have signed up for **Enterprise Support**, they can reach out to their Technical Account Manager (TAM).

TAMs work with Solutions Architects to help customers identify potential risks and potential mitigations. With Enterprise Support, you get 24x7 technical support from high-quality engineers, tools and technology to automatically manage the health of your environment, consultative architectural guidance delivered in the context of your applications and use-cases, and a designated Technical Account Manager (TAM) to coordinate access to proactive / preventative programs and AWS subject matter experts.

More details on disaster recovery options on AWS can be found in the Disaster Recovery of Workloads on AWS: Recovery in the Cloud whitepaper. This whitepaper from Amazon Web Services describes how AWS builds to guard against disruption within Regions and Availability Zones. It describes in detail how AWS maintains operational resilience and continuity of service while guarding against outages and incidents.

Getting Started

Each organization's cloud adoption journey is unique. In order to successfully execute a cloud adoption, customers need to understand their organization's current state, the target state, and the transition required to achieve the target state. Knowing this will help customers set goals and create work streams that will enable staff to thrive in the cloud.

The AWS Cloud Adoption Framework (AWS CAF) offers structure to help organizations develop an efficient and effective plan for their cloud adoption journey. Guidance and best practices prescribed within the framework can help customers build a comprehensive approach to cloud computing across their organization, throughout the IT lifecycle. The AWS CAF breaks down the complicated process of planning into manageable areas of focus.

Many organizations choose to apply the AWS CAF methodology with a facilitator-led workshop. To find more about such workshops, please contact your AWS representative.

Next steps typically also include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, as well as AWS Solution Architects, Professional Services teams and Training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please contact us.
- Obtain and review a copy of the latest C5 report, FINMA ISAE 3000 Type 2 report, AWS SOC 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification from the AWS Artifact portal (accessible via the AWS Management Console).
- Consider the relevance and application of the CIS AWS Foundations Benchmark[8] as appropriate for your cloud journey and use cases. These industry-accepted best practices published by the Center for Internet Security go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.

[8] https://d1.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf and https://d1.awsstatic.com/whitepapers/compliance/CIS_Amazon_Web_Services_Three-tier_Web_Architecture_Benchmark.pdf

- Dive deeper on other governance and risk management practices as necessary in light of your due diligence and risk assessment, using the tools and resources referenced throughout this whitepaper and in the Additional Resources section below.

- Speak with your AWS representative to learn more about how AWS is helping financial services customers migrate their critical workloads to the cloud.

Additional Resources

Set out below are additional resources to help FIs think about security, compliance and designing a secure and resilient AWS environment.

- AWS Compliance Quick Reference Guide: AWS has many compliance-enabling features that you can use for your regulated workloads in the AWS cloud. These features allow you to achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry, easier operations, and improved agility by providing more oversight, security control, and central automation.

- AWS Well-Architected Framework: The Well-Architected framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help implement designs that will scale application needs over time. The Well-Architected framework consists of five pillars: Operational Excellence; Security; Reliability; Performance Efficiency; Cost Optimization.

    - AWS has produced whitepapers addressing each pillar of the Well-Architected Framework: AWS Operational Excellence Pillar; AWS Security Pillar; AWS Reliability Pillar; AWS Performance Efficiency Pillar; AWS Cost Optimization Pillar.

- Global Financial Services Regulatory Principles: AWS has identified five common principles related to financial services regulation that customers should consider when using AWS cloud services and specifically, applying the shared responsibility model to their regulatory requirements. Customers can access a whitepaper on these principles under a non-disclosure agreement at AWS Artifact.

- NIST Cybersecurity Framework (CSF): The AWS whitepaper NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud demonstrates how public and commercial sector organizations can assess the AWS environment against the NIST CSF and improve the security measures they implement and operate (i.e., security in the cloud). The whitepaper also provides a third-party auditor letter attesting to the AWS cloud offering's conformance to NIST CSF risk management practices (i.e., security of the cloud). FIs can leverage NIST CSF and AWS resources to elevate their risk management frameworks

- Using AWS in the Context of Common Privacy and Data Protection Considerations This document provides information to assist customers who want to use AWS to store or process content containing personal data, in the context of common privacy and data protection considerations. It will help customers understand the way AWS services operate, including how customers can address security and encrypt their content. The geographic locations where customers can choose to store content and other relevant considerations. The respective roles the customer and AWS each play in managing and securing content stored on AWS services.
- Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 on AWS This guide provides customers with sufficient information to be able to plan for and document the Payment Card Industry Data Security Standard (PCI DSS) compliance of their AWS workloads. This includes the selection of controls that meet specific PCI DSS 3.2.1 requirements, planning of evidence gathering to meet assessment testing procedures, and explaining their control implementation to their PCI Qualified Security Assessor (QSA).
- AWS Risk and Compliance This document is intended to provide information to assist AWS customers with integrating AWS into their existing control framework supporting their IT environment. This document includes a basic approach to evaluating AWS controls and provides information to assist customers with integrating control environments. This document also addresses AWS-specific information around general cloud computing compliance questions.

For additional help visit the Security, Identity and Compliance Whitepapers.

Appendix: AWS Considerations for FINMA Circular 2018/03

This appendix maps the requirements identified in the FINMA Circular “2018/03 - V. Requirements for outsourcing companies” to the AWS Well-Architected Framework, relevant AWS controls, and Customer User Entity Controls (CUECs) along with links to detailed descriptions of these controls.

The mapping table in this Appendix is organized into the following columns:

Requirement: This column lists requirements or controls in FINMA Circular 2018/03.

Customer: This column lists best practices for security in the cloud from the AWS Well-Architected Framework that customers can implement as a starting point to support their compliance efforts. Details on each best practice and associated AWS services that customers may leverage can be found in the AWS Well-Architected Framework.

AWS: This column lists the AWS controls evaluated by an independent Swiss auditor for the FINMA requirement or control.

Additional mappings can be found in AWS Artifact for other FINMA circulars:

FINMA Circular 2008/10 - Self-regulation as minimum standard - Business Continuity Management (BCM)

FINMA Circular 2008/21 - Operational Risk Banks

FINMA Circular 2008/21 - Operational Risk Banks - Principle 4: Technology Infrastructure

FINMA Circular 2013/03 - Auditing – Information Technology

FINMA Circular 2018/03 - V. Requirements for Outsourcing Companies

Requirement	Customer	AWS
A. Inventory of outsourced functions **Margin no. 14 and 15**	OPS-1 - Evaluate threat landscape OPS-1 - Evaluate compliance requirements OPS-1 - Evaluate governance requirements OPS-2 - Processes and procedures have identified owners OPS-2 - Operations activities have identified owners responsible for their performance OPS-2 - Resources have identified owners	AWSCA-16.1 AWSCA-5.11 AWSCA-16.5 Third-Party Management - Third Party Audits

Requirement	Customer	AWS
B. Selection, instruction and monitoring of the service provider **Margin no. 16**	OPS-2 - Mechanisms exist to request additions, changes, and exceptions OPS-3 - Team members are empowered to take action when outcomes are at risk OPS-2 - Resources have identified owners OPS-1 - Evaluate governance requirements OPS-2 - Processes and procedures have identified owners OPS-2 - Operations activities have identified owners responsible for their performance OPS-3 - Communications are timely, clear, and actionable SEC-6 - Enable people to perform actions at a distance OPS-2 - Mechanisms exist to identify responsibility and ownership	AWSCA-12.1 AWSCA-1.10 AWSCA-1.5 AWSCA-16.12 AWSCA-11.1 AWSCA-11.2 AWSCA-16.2
Margin no. 17	OPS-1 - Evaluate governance requirements	AWSCA-12.1 AWSCA-11.2 AWSCA-16.2 AWSCA-5.12 AWSCA-9.3

Requirement	Customer	AWS
Margin no. 18 and 18.1	REL-10 - Use bulkhead architectures OPS-11 - Perform Knowledge Management OPS-1 - Evaluate tradeoffs OPS-1 - Manage benefits and risks REL-5 - Fail fast and limit queues	AWSCA-16.15 AWSCA-5.12 AWSCA-7.7 AWSCA-11.1 AWSCA-11.2 AWSCA-16.2 AWSCA-5.11 AWSCA-16.3
Margin no. 19	OPS-1 - Evaluate compliance requirements OPS-1 - Evaluate internal customer needs OPS-1 - Evaluate external customer needs	AWSCA-13.14 AWSCA-12.1 AWSCA-11.3 AWSCA-11.1 Data Security & Privacy - Policy & Legal

Requirement	Customer	AWS
Margin no. 20	OPS-1 - Evaluate threat landscape REL-6 - Storage and Analytics REL-6 - Define and calculate metrics (Aggregation) OPS-1 - Manage benefits and risks REL-4 - Do constant work REL-6 - Monitor end-to-end tracing of requests through your system	AWSCA-16.7 AWSCA-1.2 AWSCA-16.4 AWSCA-1.5 AWSCA-11.2 AWSCA-16.2 Availability & Business Continuity - Data Center Utilities Change Management - New Development / Acquisition Governance and Risk Management - Shared Responsibility Model Availability & Business Continuity - Pandemic Response Plan Availability & Business Continuity - Environmental Risks

Requirement	Customer	AWS
Margin no. 21	Not applicable.	AWSCA-12.1 AWSCA-5.11 AWSCA-12.2 AWSCA-5.12 AWSCA-16.16 AWSCA-13.2
C. Outsourcing within a group or conglomerate **Margin no. 22**	OPS-1 - Evaluate governance requirements OPS-3 - Escalation is encouraged SEC-7 - Define data lifecycle management OPS-3 - Team members are empowered to take action when outcomes are at risk OPS-3 - Communications are timely, clear, and actionable OPS-2 - Resources have identified owners SEC-1 - Automate testing and validation of security controls in pipelines	Governance and Risk Management - Policy Impact on Risk Assessments Availability & Business Continuity - Business Continuity Planning Availability & Business Continuity - Equipment Maintenance Governance and Risk Management - Shared Responsibility Model Availability & Business Continuity - Environmental Risks
D. Responsibility **Margin no. 23**	OPS-1 - Evaluate compliance requirements OPS-1 - Evaluate governance requirements SEC-1 - Identify and validate control objectives	Governance and Risk Management - Shared Responsibility Model

Requirement	Customer	AWS
E. Security **Margin no. 24 and 25**	SEC-10 - Develop incident management plans SEC-6 - Perform vulnerability management SEC-4 - Analyze logs, findings, and metrics centrally REL-6 - Storage and Analytics REL-6 - Define and calculate metrics (Aggregation) SEC-1 - Automate testing and validation of security controls in pipelines SEC-7 - Define data lifecycle management OPS-1 - Evaluate compliance requirements OPS-1 - Evaluate governance requirements REL-6 - Monitor end-to-end tracing of requests through your system SEC-5 - Create network layers SEC-7 - Identify the data within your workload	AWSCA-12.1 AWSCA-10.3 AWSCA-16.13 AWSCA-16.2 AWSCA-5.11 AWSCA-16.7 AWSCA-5.12 AWSCA-16.6 Third-Party Management - Supply Chain Agreements Governance and Risk Management - Shared Responsibility Model Human Resources - Technology Acceptable Use Human Resources - Employment Termination Governance and Risk Management - Management Support and Involvement Third-Party Management - Third Party Assessment Incident Management - Customer Support Change Management - New Development / Acquisition

Requirement	Customer	AWS
F. Audit and supervision **Margin no. 26**	OPS-1 - Evaluate compliance requirements OPS-1 - Evaluate governance requirements	AWSCA-16.9 AWSCA-16.7 AWSCA-16.16
Margin no. 27	Not applicable.	AWSCA-16.9 AWSCA-16.7 AWSCA-16.16
Margin no. 28	Not applicable.	AWSCA-16.9 AWSCA-16.7 AWSCA-16.16
Margin no. 29	Not applicable.	AWSCA-16.9 AWSCA-16.7 AWSCA-16.16
G. Outsourcing to another country **Margin no. 30**	OPS-1 - Evaluate compliance requirements OPS-1 - Evaluate governance requirements	AWSCA-13.14 AWSCA-16.9 AWSCA-16.7 AWSCA-13.17

Requirement	Customer	AWS
Margin no. 31	SEC-9 - Implement secure key and certificate management SEC-9 - Authenticate network communications SEC-10 - Pre-provision access SEC-9 - Enforce encryption in transit OPS-1 - Evaluate governance requirements SEC-7 - Define data lifecycle management REL-4 - Do constant work SEC-10 - Automate containment capability SEC-6 - Enable people to perform actions at a distance SEC-10 - Identify key personnel and external resources	AWSCA-16.14 AWSCA-16.15 AWSCA-13.17 AWSCA-7.7
H. Agreement **Margin no. 32 to 35**	OPS-3 - Executive Sponsorship SEC-1 - Keep up to date with security recommendations OPS-2 - Resources have identified owners OPS-1 - Evaluate governance requirements OPS-2 - Processes and procedures have identified owners SEC-1 - Keep up to date with security threats OPS-2 - Operations activities have identified owners responsible for their performance OPS-2 - Mechanisms exist to identify responsibility and ownership	AWSCA-13.14 AWSCA-16.9 AWSCA-16.5 AWSCA-5.12 AWSCA-16.16 AWSCA-7.7 AWSCA-5.11 Data Security & Privacy - Policy & Legal

AWS Well-Architected Mapping

This table provides details on best practices for security in the cloud from the AWS Well Architected Framework:

Best Practice	Detail	Requirements
OPS-1 - Evaluate internal customer needs	Involve key stakeholders, including business, development, and operations teams, when determining where to focus efforts on internal customer needs. This will ensure that you have a thorough understanding of the operations support that is required to achieve business outcomes. Learn more...	Margin no. 19
OPS-1 - Evaluate external customer needs	Involve key stakeholders, including business, development, and operations teams, to determine where to focus efforts on external customer needs. This will ensure that you have a thorough understanding of the operations support that is required to achieve your desired business outcomes. Learn more...	Margin no. 19

Best Practice	Detail	Requirements
OPS-1 - Manage benefits and risks	Manage benefits and risks to make informed decisions when determining where to focus efforts. For example, it may be beneficial to deploy a workload with unresolved issues so that significant new features can be made available to customers. It may be possible to mitigate associated risks, or it may become unacceptable to allow a risk to remain, in which case you will take action to address the risk. Learn more...	Margin no. 18 and 18.1 Margin no. 20
OPS-1 - Evaluate compliance requirements	Evaluate external factors, such as regulatory compliance requirements and industry standards, to ensure that you are aware of guidelines or obligations that may mandate or emphasize specific focus. If no compliance requirements are identified, ensure that you apply due diligence to this determination. Learn more...	Margin no. 14 and 15 Margin no. 19 Margin no. 23 Margin no. 24 and 25 Margin no. 26 Margin no. 30

Best Practice	Detail	Requirements
OPS-1 - Evaluate governance requirements	Ensure that you are aware of guidelines or obligations defined by your organization that may mandate or emphasize specific focus. Evaluate internal factors, such as organization policy, standards, and requirements. Validate that you have mechanisms to identify changes to governance. If no governance requirements are identified, ensure that you have applied due diligence to this determination. Learn more...	Margin no. 14 and 15 Margin no. 16 Margin no. 17 Margin no. 22 Margin no. 23 Margin no. 24 and 25 Margin no. 26 Margin no. 30 Margin no. 31 Margin no. 32 to 35
OPS-1 - Evaluate threat landscape	Evaluate threats to the business (for example, competition, business risk and liabilities, operational risks, and information security threats) and maintain current information in a risk registry. Include the impact of risks when determining where to focus efforts. Learn more...	Margin no. 14 and 15 Margin no. 20

Best Practice	Detail	Requirements
OPS-1 - Evaluate tradeoffs	Evaluate the impact of tradeoffs between competing interests or alternative approaches, to help make informed decisions when determining where to focus efforts or choosing a course of action. For example, accelerating speed to market for new features may be emphasized over cost optimization, or you may choose a relational database for non-relational data to simplify the effort to migrate a system, rather than migrating to a database optimized for your data type and updating your application. Learn more...	Margin no. 18 and 18.1
OPS-2 - Operations activities have identified owners responsible for their performance	Understand who has responsibility to perform specific activities on defined workloads and why that responsibility exists. Understanding who has responsibility to perform activities informs who will conduct the activity, validate the result, and provide feedback to the owner of the activity. Learn more...	Margin no. 14 and 15 Margin no. 16 Margin no. 32 to 35

Best Practice	Detail	Requirements
OPS-2 - Resources have identified owners	Understand who has ownership of each application, workload, platform, and infrastructure component, what business value is provided by that component, and why that ownership exists. Understanding the business value of these individual components and how they support business outcomes informs the processes and procedures applied against them. Learn more...	Margin no. 14 and 15 Margin no. 16 Margin no. 22 Margin no. 32 to 35
OPS-2 - Processes and procedures have identified owners	Understand who has ownership of the definition of individual processes and procedures, why those specific process and procedures are used, and why that ownership exists. Understanding the reasons that specific processes and procedures are used enables identification of improvement opportunities. Learn more...	Margin no. 14 and 15 Margin no. 16 Margin no. 32 to 35
OPS-2 - Mechanisms exist to identify responsibility and ownership	Where no individual or team is identified, there are defined escalation paths to someone with the authority to assign ownership or plan for that need to be addressed. Learn more...	Margin no. 16 Margin no. 32 to 35

Best Practice	Detail	Requirements
OPS-2 - Mechanisms exist to request additions, changes, and exceptions	You are able to make requests to owners of processes, procedures, and resources. Make informed decisions to approve requests where viable and determined to be appropriate after an evaluation of benefits and risks. Learn more...	Margin no. 16
OPS-3 - Executive Sponsorship	Senior leadership clearly sets expectations for the organization and evaluates success. Senior leadership is the sponsor, advocate, and driver for the adoption of best practices and evolution of the organization. Learn more...	Margin no. 32 to 35
OPS-3 - Escalation is encouraged	Team members have mechanisms and are encouraged to escalate concerns to decision makers and stakeholders if they believe outcomes are at risk. Escalation should be performed early and often so that risks can be identified, and prevented from causing incidents. Learn more...	Margin no. 22

Best Practice	Detail	Requirements
OPS-3 - Communications are timely, clear, and actionable	Mechanisms exist and are used to provide timely notice to team members of known risks and planned events. Necessary context, details, and time (when possible) are provided to support determining if action is necessary, what action is required, and to take action in a timely manner. For example, providing notice of software vulnerabilities so that patching can be expedited, or providing notice of planned sales promotions so that a change freeze can be implemented to avoid the risk of service disruption. Learn more...	Margin no. 16 Margin no. 22
OPS-3 - Team members are empowered to take action when outcomes are at risk	The workload owner has defined guidance and scope empowering team members to respond when outcomes are at risk. Escalation mechanisms are used to get direction when events are outside of the defined scope. Learn more...	Margin no. 16 Margin no. 22

Best Practice	Detail	Requirements
OPS-11 - Perform Knowledge Management	Mechanisms exist for your team members to discover the information that they are looking for in a timely manner, access it, and identify that it's current and complete. Mechanisms are present to identify needed content, content in need of refresh, and content that should be archived so that it's no longer referenced. Learn more...	Margin no. 18 and 18.1
REL-4 - Do constant work	Systems can fail when there are large, rapid changes in load. For example, a health check system that monitors the health of thousands of servers should send the same size payload (a full snapshot of the current state) each time. Whether no servers are failing, or all of them, the health check system is doing constant work with no large, rapid changes. Learn more...	Margin no. 20 Margin no. 31

Best Practice	Detail	Requirements
REL-5 - Fail fast and limit queues	If the workload is unable to respond successfully to a request, then fail fast. This allows the releasing of resources associated with a request, and permits the service to recover if it's running out of resources. If the workload is able to respond successfully but the rate of requests is too high, then use a queue to buffer requests instead. However, do not allow long queues that can result in serving stale requests that the client has already given up on. Learn more...	Margin no. 18 and 18.1
REL-6 - Monitor end-to-end tracing of requests through your system	Use AWS X-Ray or third-party tools so that developers can more easily analyze and debug distributed systems to understand how their applications and its underlying services are performing. Learn more...	Margin no. 20 Margin no. 24 and 25
REL-6 - Define and calculate metrics (Aggregation)	Store log data and apply filters where necessary to calculate metrics, such as counts of a specific log event, or latency calculated from log event timestamps. Learn more...	Margin no. 20 Margin no. 24 and 25

Best Practice	Detail	Requirements
REL-6 - Storage and Analytics	Collect log files and metrics histories and analyze these for broader trends and workload insights. Learn more...	Margin no. 20 Margin no. 24 and 25
REL-10 - Use bulkhead architectures	Like the bulkheads on a ship, this pattern ensures that a failure is contained to a small subset of requests / users so the number of impaired requests is limited, and most can continue without error. Bulkheads for data are usually called partitions or shards, while bulkheads for services are known as cells. Learn more...	Margin no. 18 and 18.1
SEC-1 - Identify and validate control objectives	Based on your compliance requirements and risks identified from your threat model, derive and validate the control objectives and controls that you need to apply to your workload. Ongoing validation of control objectives and controls help you measure the effectiveness of risk mitigation. Learn more...	Margin no. 23

Best Practice	Detail	Requirements
SEC-1 - Keep up to date with security threats	Recognize attack vectors by staying up to date with the latest security threats to help you define and implement appropriate controls. Learn more...	Margin no. 32 to 35
SEC-1 - Keep up to date with security recommendations	Stay up to date with both AWS and industry security recommendations to evolve the security posture of your workload. Learn more...	Margin no. 32 to 35
SEC-1 - Automate testing and validation of security controls in pipelines	Establish secure baselines and templates for security mechanisms that are tested and validated as part of your build, pipelines, and processes. Use tools and automation to test and validate all security controls continuously. For example, scan items such as machine images and infrastructure as code templates for security vulnerabilities, irregularities, and drift from an established baseline at each stage. Learn more...	Margin no. 22 Margin no. 24 and 25

Best Practice	Detail	Requirements
SEC-4 - Analyze logs, findings, and metrics centrally	All logs, metrics, and telemetry should be collected centrally, and automatically analyzed to detect anomalies and indicators of unauthorized activity. A dashboard can provide you easy to access insight into real-time health. For example, ensure that Amazon GuardDuty and Security Hub logs are sent to a central location for alerting and analysis. Learn more...	Margin no. 24 and 25
SEC-5 - Create network layers	Group components that share reachability requirements into layers. For example, a database cluster in a VPC with no need for internet access should be placed in subnets with no route to or from the internet. In a serverless workload operating without a VPC, similar layering and segmentation with microservices can achieve the same goal. Learn more...	Margin no. 24 and 25

Best Practice	Detail	Requirements
SEC-6 - Enable people to perform actions at a distance	Removing the ability for interactive access reduces the risk of human error, and the potential for manual configuration or management. For example, use a change management workflow to deploy EC2 instances using infrastructure as code, then manage EC2 instances using tools instead of allowing direct access or a bastion host. Learn more...	Margin no. 16 Margin no. 31
SEC-6 - Perform vulnerability management	Frequently scan and patch for vulnerabilities in your code, dependencies, and in your infrastructure to help protect against new threats. Learn more...	Margin no. 24 and 25
SEC-7 - Define data lifecycle management	Your defined lifecycle strategy should be based on sensitivity level, as well as legal and organization requirements. Aspects including the duration you retain data for, data destruction, data access management, data transformation, and data sharing should be considered. Learn more...	Margin no. 22 Margin no. 24 and 25 Margin no. 31

Best Practice	Detail	Requirements
SEC-7 - Identify the data within your workload	This includes the type and classification of data, the associated business processes. data owner, applicable legal and compliance requirements, where it's stored, and the resulting controls that are needed to be enforced. This may include classifications to indicate if the data is intended to be publicly available, if the data is internal use only such as customer personally identifiable information (PII), or if the data is for more restricted access such as intellectual property, legally privileged or marked sensitive, and more. Learn more...	Margin no. 24 and 25
SEC-9 - Implement secure key and certificate management	Store encryption keys and certificates securely and rotate them at appropriate time intervals while applying strict access control; for example, by using a certificate management service, such as AWS Certificate Manager (ACM). Learn more...	Margin no. 31

Best Practice	Detail	Requirements
SEC-9 - Enforce encryption in transit	Enforce your defined encryption requirements based on appropriate standards and recommendations to help you meet your organizational, legal, and compliance requirements. Learn more...	Margin no. 31
SEC-9 - Authenticate network communications	Verify the identity of communications by using protocols that support authentication, such as Transport Layer Security (TLS) or IPsec. Learn more...	Margin no. 31
SEC-10 - Automate containment capability	Automate containment and recovery of an incident to reduce response times and organizational impact. Learn more...	Margin no. 31

Best Practice	Detail	Requirements
SEC-10 - Pre-provision access	Ensure that incident responders have the correct access pre-provisioned into AWS to reduce the time for investigation through to recovery. Learn more...	Margin no. 31
SEC-10 - Identify key personnel and external resources	Identify internal and external personnel, resources, and legal obligations that would help your organization respond to an incident. Learn more...	Margin no. 31
SEC-10 - Develop incident management plans	Create plans to help you respond to, communicate during, and recover from an incident. For example, you can start an incident response plan with the most likely scenarios for your workload and organization. Include how you would communicate and escalate both internally and externally. Learn more...	Margin no. 24 and 25

AWS Control Activities Mapping

This table provides details on the AWS controls evaluated by an independent Swiss auditor for the FINMA requirements:

Control Id	Detail	Requirements
AWSCA-1.2	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.	Margin no. 20
AWSCA-1.5	AWS maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact AWS business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer. A formal risk control matrix (RCM) is updated semi-annually. AWS Enterprise Risk Management (ERM) manages and reports risks to the appropriate AWS management on a semi-annual basis. AWS Management acknowledges risk treatment decisions and formally approves risk acceptance.	Margin no. 16 Margin no. 20
AWSCA-1.10	AWS has a process in place to review environmental and geo-political risks before launching a new region.	Margin no. 16
AWSCA-5.11	Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.	Margin no. 14 and 15 Margin no. 18 and 18.1 Margin no. 21 Margin no. 24 and 25 Margin no. 32 to 35

Control Id	Detail	Requirements
AWSCA-5.12	AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.	Margin no. 17 Margin no. 18 and 18.1 Margin no. 21 Margin no. 24 and 25 Margin no. 32 to 35
AWSCA-7.7	AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.	Margin no. 18 and 18.1 Margin no. 31 Margin no. 32 to 35
AWSCA-9.3	AWS performs annual formal evaluation of resourcing and staffing including assessment of employee qualification alignment with entity objectives. Employees receive feedback on their strengths and growth ideas annually.	Margin no. 17
AWSCA-10.3	AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.	Margin no. 24 and 25
AWSCA-11.1	Vendors and third parties with restricted access, that engage in business with Amazon are subject to confidentiality commitments as part of their agreements with Amazon. Confidentiality commitments	Margin no. 16 Margin no. 18 and 18.1 Margin no. 19

Control Id	Detail	Requirements
	included in agreements with vendors and third parties with restricted access are reviewed by AWS and the third party at time of contract creation or renewal.	
AWSCA-11.2	AWS has a program in place for evaluating vendor performance and compliance with contractual obligations.	Margin no. 16 Margin no. 17 Margin no. 18 and 18.1 Margin no. 20
AWSCA-11.3	AWS communicates confidentiality requirements in agreements when they are renewed with vendors and third parties with restricted access. Changes to standard confidentiality commitments to customers are communicated on the AWS website via the AWS customer agreement.	Margin no. 19
AWSCA-12.1	AWS informs customers of the AWS Data security and privacy commitments within the AWS Customer Agreement prior to activating an AWS account and makes it available to customers to review at any time on the AWS website.	Margin no. 16 Margin no. 17 Margin no. 19 Margin no. 21 Margin no. 24 and 25
AWSCA-12.2	AWS informs customers of changes made to the AWS Customer agreement via the AWS public website.	Margin no. 21
AWSCA-13.2	Cloud customers are able to control and monitor their system resources.	Margin no. 21

Control Id	Detail	Requirements
AWSCA-13.14	AWS maintains standard contract review and signature processes that include legal reviews with consideration to protection of AWS resources.	Margin no. 19 Margin no. 30 Margin no. 32 to 35
AWSCA-13.17	AWS customer content is stored in the region they specify and AWS does not move their data from that region.	Margin no. 30 Margin no. 31
AWSCA-16.1	AWS maintains up to date inventory of all colocation service providers	Margin no. 14 and 15
AWSCA-16.2	AWS establishes and maintains the third-party risk scoring methodology, including Third-Party vendor categorization and vendor risk tiering. Prior to onboarding a third party, AWS performs financial due diligence check, including the review of the third party's audited financials, and data security (i.e., access to data, storage of data) due diligence check that may impact ongoing operations of AWS services	Margin no. 16 Margin no. 17 Margin no. 18 and 18.1 Margin no. 20 Margin no. 24 and 25
AWSCA-16.3	AWS has contractual requirements in place with colocation service providers to facilitate the transfer of AWS materials in an orderly manner upon termination of agreement	Margin no. 18 and 18.1
AWSCA-16.4	AWS has Third-Party Risk Management Policy in place which outlines the framework, requirements and roles and responsibilities to mitigate third-party risk in data access, data privacy, subcontracting, business resiliency, and regulatory compliance.	Margin no. 20

Control Id	Detail	Requirements
AWSCA-16.5	AWS has a mechanism in place to pro-actively inform its customers prior to authorizing a Material Subcontractor by adding such Material Subcontractor to the List of Material Subcontractors on AWS' website	Margin no. 14 and 15 Margin no. 32 to 35
AWSCA-16.6	AWS creates and maintains written agreements with third parties (for example, Contractors or vendors) in accordance with the work or service to be provided, if appropriate which cover service continuity requirements (e.g., recovery time objectives - RTO)	Margin no. 24 and 25
WSCA-16.7	AWS engages qualified independent external auditors to perform external audits at least on a yearly basis. Attestation reports of these audits are made available to customers via AWS Artifact Portal	Margin no. 20 Margin no. 24 and 25 Margin no. 26 Margin no. 27 Margin no. 28 Margin no. 29 Margin no. 30
AWSCA-16.9	AWS provides its Swiss Financial Services customers with a contract addendum containing the required audit rights for regulated entities in Switzerland.	Margin no. 26 Margin no. 27 Margin no. 28 Margin no. 29 Margin no. 30

Control Id	Detail	Requirements
		Margin no. 32 to 35
AWSCA-16.12	AWS communicates service commitments to user entities (AWS customers) in the form of Service Level Agreements (SLAs), contractual agreements, or through the description of the service offerings provided online through the AWS website	Margin no. 16
AWSCA-16.13	AWS publishes relevant information on AWS official website for customers to help achieve operational resilience using AWS services	Margin no. 24 and 25
AWSCA-16.14	The ability to assign the agreement and AWS Accounts (which enable access to the regulated entity's information) is governed by the agreement between the regulated entity and AWS.	Margin no. 31
AWSCA-16.15	AWS offers services and user guides to transfer large amounts of data into and out of AWS. AWS professional services can be engaged to provide assistance in the development of an exit strategy, as well as post-termination assistance	Margin no. 18 and 18.1 Margin no. 31
AWSCA-16.16	AWS has required contractual terms in place with colocation service providers to allow Amazon personnel and its designees to inspect facilities which support AWS or its services	Margin no. 21 Margin no. 26 Margin no. 27 Margin no. 28 Margin no. 29 Margin no. 32 to 35

Additional AWS Controls

This table provides details on additional AWS controls that are applicable to FINMA requirements:

Control Name	Detail	Requirements
Governance and Risk Management - Shared Responsibility Model	Security and compliance is a shared responsibility between AWS and the customer. AWS is responsible for the security and compliance 'of' the cloud, and implements security controls to secure the underlying infrastructure that runs the AWS services and hosts and connects customer resources. AWS customers are responsible for security 'in' the cloud and should determine, design and implement the security controls needed based on their security and compliance needs and AWS services they select. The customer responsibility will be determined by the AWS services that a customer selects. AWS provides customers with best practices on how to secure their resources within the AWS service's documentation at http://docs.aws.amazon.com/ . AWS customers are, at the very least , responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their AWS environment.	Margin no. 20 Margin no. 22 Margin no. 23 Margin no. 24 and 25

Control Name	Detail	Requirements
Availability & Business Continuity - Pandemic Response Plan	AWS has clearly defined pandemic response policies and procedures that aim to ensure that we are equipped with core capabilities to prevent, detect, and respond rapidly in a coordinated manner to infectious disease outbreak threats. These policies and procedures work alongside our long-standing business continuity plan so that we can respond rapidly in a coordinated manner to infectious disease outbreaks. AWS's comprehensive approach to business continuity planning is designed to mitigate risks to people, facilities, equipment, and technology. These efforts are intended to protect the safety and well-being of our employees and maintain continuity of our business operations.	Margin no. 20

Control Name	Detail	Requirements
Availability & Business Continuity - Business Continuity Planning	The AWS business continuity plan details the three-phased approach that AWS has developed to recover and reconstitute the AWS infrastructure: • Activation and Notification Phase • Recovery Phase • Reconstitution Phase This approach ensures that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and omissions. AWS maintains a ubiquitous security control environment across its infrastructure. Each data center is built to physical, environmental, and security standards in an active-active configuration, employing an n+1 redundancy model to ensure system availability in the event of component failure. Components (N) have at least one independent backup component (+1), so the backup component is active in the operation even if other components are fully functional. In order to eliminate single points of failure, this model is applied throughout AWS, including network and data center implementation. Data centers are online and serving traffic; no data center is “cold.” In case of failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.	Margin no. 22

Control Name	Detail	Requirements
Availability & Business Continuity - Equipment Maintenance	AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. In order to ensure maintenance procedures are properly executed, AWS assets are assigned an owner, tracked and monitored with AWS proprietary inventory management tools. AWS asset owner procedures are carried out by method of utilizing a proprietary tool with specified checks that must be completed according to the documented maintenance schedule. Third party auditors test AWS equipment maintenance controls by validating that the asset owner is documented and that the condition of the assets is visually inspected according to the documented maintenance policy.	Margin no. 22

Availability & Business Continuity - Environmental Risks	Each AWS data center is evaluated to determine the controls that must be implemented to mitigate, prepare, monitor, and respond to natural disasters or malicious acts that may occur. Controls implemented to address environmental risks can include but are not limited to the following: • AWS data centers are equipped with sensors and master shutoff-valves to detect the presence of water. Mechanisms are in place to remove water in order to prevent any additional water damage. • Automatic fire detection and suppression equipment has been installed to reduce risk and notify AWS Security Operations Center, and emergency responders in the event of a fire. The fire detection system utilizes smoke detection sensors in data center environments (e.g., VESDA, point source detection), mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems. • Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at specified levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. This is provided at N+1 and also utilizes free cooling as primary source of cooling when and where it is available based on local environmental conditions.	Margin no. 20 Margin no. 22

Control Name	Detail	Requirements
	• Availability Zones are physically separated within a metropolitan region and are in different flood plains. • Each Availability Zone is designed as an independent failure zone and automated processes move customer traffic away from the affected area in the case of a failure. • The AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. Power to AWS data centers is provided through local power provider. In the event of disruption, Uninterruptible Power Supply (UPS) units provide back-up power or critical and essential loads in the facility and generators are used to provide back-up power for the entire facility.	

Availability & Business Continuity - Data Center Utilities	AWS data center utilities (e.g., water, power, telecommunications, and internet connectivity) are implemented to maintain continuous operability and prevent service or operation disruption. Controls can include but are not limited to the following: • The AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. Power to AWS data centers is provided through local power provider. In the event of disruption, Uninterruptible Power Supply (UPS) units provide back-up power or critical and essential loads in the facility and generators are used to provide back-up power for the entire facility. • AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. This is carried out by method of utilizing a proprietary tool with specified checks that must be completed according to the documented maintenance schedule. • Cabling providing utility support to AWS data centers are protected from intentional or accidental damage. • Water necessary to operate AWS data centers is supplied by local water providers. In the event of disruption, AWS maintains backup supply on premise to maintain continued operability.	Margin no. 20

Control Name	Detail	Requirements
	• Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at specified levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. This is provided at N+1 and also utilizes free cooling as primary source of cooling when and where it is available based on local environmental conditions.	

Change Management - New Development / Acquisition	AWS maintains a systematic approach, to planning and developing new services for the AWS environment, to ensure the quality and security requirements are met with each release. AWS' strategy for the design and development of services is to clearly define services in terms of customer use cases, service performance, marketing and distribution requirements, production and testing, and legal and regulatory requirements. The design of new services or any significant changes to current services follow secure software development practices and are controlled through a project management system with multi-disciplinary participation. Requirements and service specifications are established during service development, taking into account legal and regulatory requirements, customer contractual commitments, and requirements to meet the confidentiality, integrity and availability of the service. Service reviews are completed as part of the development process. Prior to launch, each of the following requirements must be reviewed: • Security Risk Assessment • Threat modelling • Security design reviews • Secure code reviews • Security testing • Vulnerability/penetration testing	Margin no. 20 Margin no. 24 and 25

Control Name	Detail	Requirements
	AWS implements open source software or custom code within its services. Open source software, including binary or machine-executable code from third-parties, is reviewed and approved prior to implementation, and has source code that is publicly accessible. Code developed by AWS is available for review by the applicable service team, as well as AWS Security. By its nature, open source code is available for review prior to granting authorization for use within Amazon.	

Control Name	Detail	Requirements
Data Security & Privacy - Policy & Legal	AWS maintains internal informational websites describing the AWS environment, its boundaries, user responsibilities and services. AWS has an appointed privacy point of contact and maintains a privacy policy that states that AWS is committed to achieving compliance with applicable PII protection legislation and AWS contractual terms. AWS and customers agree to a service agreement outlining the terms of service and responsibilities of both parties prior to service delivery. AWS does not disclose customer content unless required to do so to comply with the law, or with a valid and binding order of a governmental or regulatory body. Unless AWS is prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing customer content so they can seek protection from disclosure. AWS provides publicly available mechanisms for customers to contact AWS to report security events and publishes information including a system description and security and compliance information addressing AWS commitments and responsibilities.	Margin no. 19 Margin no. 32 to 35

Control Name	Detail	Requirements
Governance and Risk Management - Policy Impact on Risk Assessments	Management reviews exceptions to security policies to assess and mitigate risks. AWS Security maintains a documented procedure describing the policy exception workflow on an internal AWS website. Policy exceptions are tracked and maintained with the policy tool and exceptions are approved, rejected, or denied based on the procedures outlined within the procedure document.	Margin no. 22
Governance and Risk Management - Management Support and Involvement	The output of AWS Leadership reviews include decisions or actions related to the following: • Improvement of the effectiveness of the ISMS. • Update of the risk assessment and risk treatment plan. • Modification of procedures and controls that affect information security, as necessary, to respond to internal or external events that may impact the ISMS. This includes, changes to business requirements, security requirements, business processes affecting the existing business requirements, regulatory or legal requirements, contractual obligations, levels of risk and/or criteria for accepting risk. • Resource needs. • Improvement in how the effectiveness of controls is being measured.	Margin no. 24 and 25

Control Name	Detail	Requirements
Human Resources - Employment Termination	AWS is responsible for the following processes upon the termination of an employee: • Communicating termination responsibilities, such as security requirements, legal responsibilities, and non-disclosure obligations to terminated personnel. • Revoking information system access. • Retrieving AWS information system-related property (e.g., authentication tokens, keys, badges). • Disabling badge access (automated).	Margin no. 24 and 25

Control Name	Detail	Requirements
Human Resources - Technology Acceptable Use	As part of the on-boarding process, personnel supporting systems and devices within the system boundary are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy. AWS has implemented data handling and classification requirements that provide specifications around: • Data encryption • Content in transit and during storage • Access • Retention • Physical controls • Mobile devices • Data handling requirements Employees are required to review and sign-off on an employment contract, which acknowledges their responsibilities to overall Company standards and information security.	Margin no. 24 and 25

Control Name	Detail	Requirements
Incident Management - Customer Support	AWS develops and maintains customer support procedures that include metrics to verify performance. When a customer contacts AWS to report that AWS services do not meet their quality objectives, their issues are immediately investigated and, where required, commercially reasonable actions are taken to resolve them. The customer support quality system includes, but is not limited to, procedures for reviewing and evaluating customer complaints, engaging necessary internal AWS resources and teams, and communicating the final disposition of the issue back to the customer. Depending on contract requirements, AWS maintains procedures for notifying customers of customer-impacting issues using the AWS Service Health Dashboard (available at http://status.aws.amazon.com/). The AWS Service Health Dashboard publishes up-to-the-minute information on service availability, where customers can subscribe to an RSS feed to be notified of interruptions to each individual service and a full status history of each individual service health.	Margin no. 24 and 25

Control Name	Detail	Requirements
Third-Party Management - Third Party Audits	AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards. AWS maintains standard contract review and signature processes that include legal reviews with consideration of protecting AWS resources. AWS proactively informs our customers of any subcontractors who have access to customer-owned content you upload onto AWS, including content that may contain personal data. There are no subcontractors authorized by AWS to access any customer-owned content that you upload onto AWS. To monitor subcontractor access year-round please refer to https://aws.amazon.com/compliance/third-party-access/.	Margin no. 14 and 15
Third-Party Management - Supply Chain Agreements		Margin no. 24 and 25

Control Name	Detail	Requirements
Third-Party Management - Third Party Assessment	AWS maintains a supplier management team to foster third party relationships and monitor third party performance. SLAs and SLOs are implemented to monitor performance using supplier scorecards. Personnel security requirements for third-party providers supporting AWS systems and devices are established in a Mutual Non-Disclosure Agreement between AWS' parent organization, Amazon.com, and the respective third-party provider. The Amazon Legal Counsel and the AWS Procurement team define AWS third party provider personnel security requirements in contract agreements with the third-party provider. All AWS employees working with AWS information must, at a minimum, meet the screening process for pre-employment background checks and sign a Non-Disclosure Agreement (NDA) prior to being granted access to AWS information.	Margin no. 24 and 25

Contributors

The following individuals and organizations contributed to this document:

- Margo Cronin, Principal Solutions Architect, AWS
- Raphael Fuchs, Senior Security Advisor, AWS

Document Revisions

Date	Description	
December 2021	First publication draft	