Guide to Financial Services Regulations and Guidelines in Switzerland

August 2024

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.

This document is provided for informational purposes only; it is not legal or compliance advice and should not be relied on as legal or compliance advice. Customers are responsible for making their own independent assessments and should obtain appropriate advice from their own legal and compliance advisors regarding compliance, with all regulatory and legal requirements that are relevant to their business, including in relation to Swiss laws, standards, circulars, regulations, and guidelines.

Contents

Abstract

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

This guide covers the following topics:

- Respective roles that the customer and AWS play in managing and securing the different aspects of a customer's cloud environment.
- AWS security systems and the shared responsibility model.
- Overview of Swiss regulatory requirements and guidance through the lens of a customer's use of AWS.

Additional resources designed to assist customers with architecting their AWS environment in a way that helps meet Swiss security and regulatory requirements.

Introduction

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 that the Swiss Financial Market Supervisory Authority (FINMA) oversees directly or indirectly.

This guide covers the requirements created by the following regulations and publications of interest to 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 Financial Services Industry (FSI) customers understand certain key regulatory, technical and operational requirements when they use AWS services. This guide includes a description of the advanced tools and security measures that AWS offers, which Swiss FSI customers can use to assist them with evaluating, meeting, and demonstrating compliance with regulatory requirements outlined in applicable Swiss laws, circulars, regulations, and guidelines.

This guide focuses on typical security-related questions that AWS customers often ask when considering Swiss laws, circulars, regulations, and guidelines and their use of AWS services. The following sections provide information that customers can use to better understand the responsibilities of financial institutions and AWS in regard to cloud use.

Security and the 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 that Swiss FSI customers can take to align with the relevant requirement.

AWS Global Cloud Infrastructure: The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones. The AWS Cloud offers AWS customers effective ways 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 cloud outsourcing requirements.

AWS Compliance Program: 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 use 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.

Security and The 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.

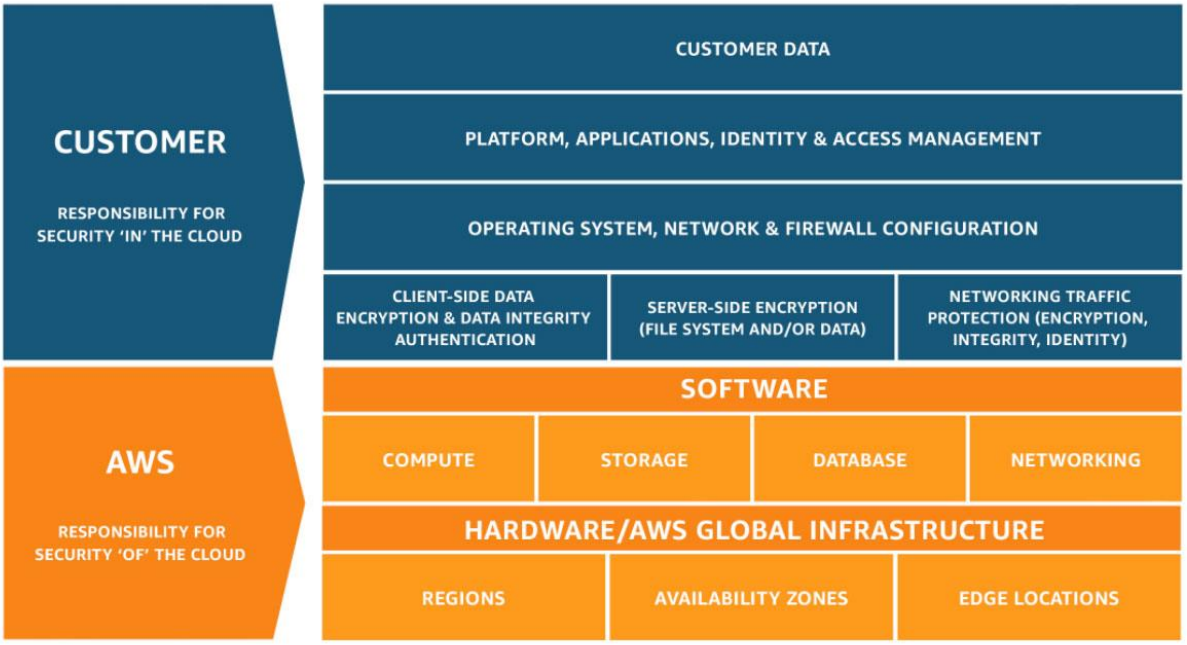

Figure 1 – The AWS Shared Responsibility Model

The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of 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 FSI who run material workloads on a cloud service provider are, in some cases, required to make sure that the outsourcing contracts between themselves and the cloud service provider include all necessary provisions that are required to make sure that 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 customers' access to and use of AWS services. To learn more, see the AWS Customer Agreement.

The **AWS Service Terms** available in the AWS Service Terms page govern the use of the AWS services and provide additional terms that 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 FSA provides Swiss regulated customers with contractual clauses in addition to those provided in the AWS Customer Agreement. 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 that 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 the latest version of the EU Commission's Standard Contractual Clauses. This means that AWS customers who want to transfer personal data from the European Economic Area (EEA) to other countries can do so in compliance with the latest interpretation of the data transfer requirements under the EU's General Data Protection Regulation (**GDPR**). Additionally, AWS offers customers the AWS Supplementary Addendum to the AWS GDPR DPA, which sets out strengthened contractual commitments with respect to law enforcement requests and other technical and organisational measures. For more information about

the AWS GDPR DPA, visit AWS GDPR Data Processing Addendum – Now Part of Service Terms. The AWS GDPR DPA and the AWS Supplementary Addendum apply to customers' use of AWS services in processing customer data and is available as part of AWS's service terms.

Additionally, the **AWS Swiss Addendum to the AWS Data Processing Addendum** (which adds to existing obligations for AWS under the AWS GDPR DPA) allows AWS Swiss customers to use AWS services to process personal data in compliance with the new Federal Act on Data Protection (nFADP).

AWS is 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 is 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, because 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) requires the customer to perform all 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 environments, 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 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 visiting our Compliance and Security for Financial Services page.

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 Cloud 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 in a way that is 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 also covered in this guide 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 and Switzerland.

AWS customers choose the Regions 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 the locations of their choice. More information on our disaster recovery recommendations is available at Disaster recovery options in the cloud.

The **AWS Europe (Zurich)** Region is available to our customers (API name: eu-central-2). The Region has three Availability Zones designed and built to meet rigorous compliance standards globally, providing high levels of security for AWS customers. As with every Region, the Europe (Zurich) Region aligns with applicable global and Swiss data protection laws. This allows customers to store data within Switzerland and reduce latency to their Swiss users.

AWS compliance programs

AWS has obtained certifications, independent third-party attestations and independent third-party reports 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 (ISMS), 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 27701:2019 specifies requirements and guidelines to establish and continuously improve the Privacy Information Management System (PIMS), including processing of Personally Identifiable Information (PII). It is an extension of the ISO/IEC 27001 and ISO/IEC 27002 standards for information security management, and it provides a set of additional controls and associated guidance intended to address public cloud PIMS and PII management requirements for both processers and controllers, not addressed by the existing ISO/IEC 27002 control set. For more information, or to download the AWS ISO 27701 certification, see the ISO 27701 Compliance webpage.

ISO 22301:2019 standard specifies requirements to implement, maintain and improve a business continuity management system (BCMS). The requirements specified in this standard are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity. The standard is applicable to all types and sizes of organizations that:

a. Implement, maintain and improve a BCMS.

b. Seek to ensure conformity with stated business continuity policy.

c. Need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption.

d. Seek to enhance their resilience through the effective application of the BCMS.

For more information, or to download the AWS ISO 22301 certification, see the ISO 22301 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 might 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 Computing Providers whitepaper. 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 (that is, 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 AWS Swiss financial services customers with the assurance that the 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 customers

should consider implementing as part of the AWS Shared Responsibility Model to help them comply with FINMA's control objectives. The report covers the FINMA circulars that are applicable to Swiss financial services institutions in the context of outsourcing arrangements, including outsourcings 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 operational 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 establish and operate AWS environments.

For more information about other AWS certifications and attestations, see the AWS Compliance Programs 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 AWS 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 controls options to engage directly with AWS on audit, compliance, and security matters to Swiss financial services customers that are subject to the FINMA. These offerings are designed to be implemented in

sequence, starting with the compliance briefings, to deepen customers' understanding and to maximize interactions with AWS experts and compliance artifacts.

The controls set out within the FINMA ISAE 3000 Type 2 report outline multiple ways in which AWS Swiss financial services customers 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 tailored options for developing an ongoing relationship with AWS Cloud Security to AWS Swiss financial services customers that are subject to the FINMA controls. In all engagements, AWS Cloud 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 and Compliance Specialists, who are appropriately qualified and knowledgeable AWS personnel. The content of compliance briefings is tailored directly to customers' needs. Discussion topics can 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 transparency into the AWS control environment and direct engagement with AWS evidence artifacts accessed by AWS auditors during their assessments.

Prior to each AWS Audit Symposium, customers request topics for discussion and specific controls from the AWS control framework that 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 to AWS Cloud 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, because agendas are tailored to meet the specific needs and requirements of attending AWS customers. Additionally, audit artifacts are available for independent review by customers 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.

The AWS Audit Symposium is offered at least quarterly and attendance is limited to three customer audit employee representatives.

Community audit

A community audit is a pooled audit led 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 (such as 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 members input into the audit scope while mutually benefitting from sharing the cost and effort of a single audit. Community audits minimize audit duration while increasing overall control transparency, ensuring the highest bar of assurance for the most security-conscious community member.

Individual audit

AWS offers customers the ability to perform an audit directly with AWS through individual audits. 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 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

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 and the purpose of the guide is to help financial institutions to perform due diligence and apply sound governance and risk management practices to their outsourcing of a material business activity, including through 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 requirements from customers 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.

Article 47 of the Banking Act

Customers should note that Article 47 BA, in substance, states that it is prohibited to disclose information that is subject to the banking secrecy entrusted or acquired in one's capacity as a member of an executive or supervisory body, employee, delegate, agent, representative, auditor or liquidator of a bank. Any violation or attempt to induce a violation of this confidentiality obligation (even in case of negligence) is sanctioned by a fine or imprisonment. 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 is not protected by Article 47 BA. Moreover, for Article 47 BA to apply, there must be a certain disclosure of the information that is subject to the banking secrecy. That is, an unauthorized third party must have actual knowledge of the protected 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: serves a reasonable interest of the financial institution, covers the delegation of auxiliary tasks, is made under the financial institution's supervision, and 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 others, issued by the Swiss Bankers Association, an umbrella organization 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:

- 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.
- 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 compliance measures.

The SBVg Guidelines acknowledge 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 while still being compliant with Swiss regulations.

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. 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 align with Article 47 BA. AWS gives you ownership and control over your content through simple, powerful tools that allow you to determine where your content is 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 the AWS Shared Responsibility Model, a reasonable security standard to protect bank clients' confidentiality is the responsibility of the bank and AWS.

AWS provides its 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 provides further information about how the AWS control environment can assist a Swiss financial services customer's compliance efforts with certain Swiss Financial Market Supervisory Authority (FINMA) outsourcing requirements applicable to regulated financial services customers in Switzerland. Visit AWS 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 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 gives a detailed overview of technical and organizational measures, with focus on data protection and technical security controls set forth by applicable FINMA circulars.

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 AWS 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.

The following FINMA circulars are issued by FINMA and intended to assist regulated financial institutions in understanding approaches to due diligence, management of third parties, 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).
- Business Continuity Management (BCM) minimum standards proposed by the Swiss Insurance Association (01.06.2015) and Swiss Bankers Association (29.08.2013).

In December 2022, FINMA, the Swiss Financial Market Supervisory Authority, announced a fully revised circular called Operational risks and resilience – banks. This circular came into effect on January 1, 2024. The circular replaces the Swiss Bankers Association's *Recommendations for Business Continuity Management (BCM)* and 2008/21 "Operational Risks – banks."

The new circular also adopts the revised principles for managing operational risks, and the new principles on operational resilience, that the Basel Committee on Banking Supervision published in March 2021.

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 organization and risk limitation. 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.

The Circular 2018/3 **"**Operational risks and resilience – banks" defines the supervisory requirements on the segregation of duties, risk management, and internal controls. It defines critical data as follows:

> "Critical data are data that, in view of the institution's size, complexity, structure, risk profile and business model, are of such crucial significance that they require increased security measures. These are data that are crucial for the successful and sustainable provision of the institution's services or for regulatory purposes. When assessing and determining the criticality of data, the confidentiality as well as the integrity and availability must be taken into account. Each of these three aspects can determine whether data is classified as critical."

This definition is consistent with the AWS approach to privacy and security. We believe that for AWS to realize its full potential, customers must have control over their data. This means that customers have:

- Control over the location of their data.
- Verifiable control over data access.
- Ability to encrypt everything everywhere.
- Resilience of AWS.

These commitments further demonstrate our dedication to securing your data—it's our highest priority. We implement rigorous contractual, technical, and organizational measures to help protect the confidentiality, integrity, and availability of your content regardless of which AWS Region you select. You have complete control over your content through powerful AWS services and tools that you can use to determine where to store your data, how to secure it, and who can access it.

You also have control over the location of your content on AWS. For example, in Europe, at the time of publication of this guide, customers can deploy their data into any of eight Regions (for an up-to-date list of Regions, see AWS Global Infrastructure). One of these Regions is the Europe (Zurich) Region, also known by its API name: *eu-central-2*, which customers can use to store data in Switzerland.

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

The relationship between CUECs and the AWS control environment relates closely to the AWS Shared Responsibility Model. The CUECs are controls that describe 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 and is available through AWS Artifact. The FINMA ISAE 3000 Type 2 report provides further information about how the AWS control environment can assist with a Swiss financial services customer's compliance with certain Swiss Financial Market Supervisory Authority (FINMA) outsourcing requirements applicable to regulated financial services customers in Switzerland.

The AWS control environment is described by a series of AWS control activities (AWSSCA) which are divided into five 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 the AWS control activities against FINMA controls (requirements) outlined in the circulars and tracks whether deviations are noted or not.

The ISAE 3000 Type 2 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 AWS 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.

Swiss Federal Act on Data Protection (nFADP)

Switzerland has fully revised its Federal Act on Data Protection, which came into force on September 1, 2023, together with the new Data Protection Ordinance (**nFADP**).

AWS customers can use AWS services in compliance with the nFADP because AWS offers:

- Multiple technical, organizational, and contractual measures that allow customers to protect their data when using AWS services.
- A Swiss Addendum to the AWS Data Processing Addendum (AWS DPA) that together address the contractual requirements of the nFADP.

The revisions to the nFADP were mostly intended to align it more closely with the EU's GDPR. So, in broad terms—and with a few exceptions—compliance with the GDPR continues to ensure compliance with the nFADP.

With AWS, customers manage the privacy controls of their data, control how their content is being used, who has access to it, and how it is encrypted. To find out more about the measures, tools and services AWS offers to meet requirements of the nFADP, customers can visit the Data Protection and Privacy at AWS page. The page sets out the commitments AWS has made on data sovereignty, security, data privacy, and data controls and residency.

The AWS DPA sets out AWS commitments with respect to processing of personal data uploaded to the AWS services under a customer's AWS account (*customer data*), and the Swiss Addendum to this AWS DPA addresses the specific requirements under the nFADP. The AWS DPA and the Swiss Addendum are both incorporated in the AWS Service Terms (Section 1.14) and apply automatically when customer's use of AWS services is subject to the nFADP.

The Swiss Addendum also includes the Standard Contractual Clauses (SCCs) adopted by the European Commission and amended as required by the Swiss Federal Data Protection and Information Commissioner. As set out in the Swiss Addendum, the SCCs

will automatically apply whenever a customer uses AWS services to transfer customer data subject to the nFADP to countries outside Switzerland not recognised under the nFADP as providing an adequate level of protection for personal data.

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.

AWS Services are GDPR ready

AWS is 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 might apply to their activities. New features are launched regularly, and AWS has over 500 features and services focused on security and compliance.

Detailed information on AWS Services readiness for GDPR can be found at the AWS General Data Protection Regulation (GDPR) Center.

Additional data protection considerations

Swiss customers also benefit from AWS adherence to the CISPE Code of Conduct. The CISPE Code goes beyond compliance with the GDPR or the nFADP by requiring cloud infrastructure service providers to give customers the choice to use services to store and process customer data exclusively in the European Economic Area (EEA). AWS has initially declared over 100 services under the CISPE Code and is committed to bringing additional AWS services into the scope of the CISPE compliance program. For further information, see the blog post: AWS cloud services adhere to CISPE Data Protection Code of Conduct for added GDPR assurance.

In addition to providing customers with a number of tools and services to build nFADP-compliant environments, AWS has achieved a number of internationally recognized certifications and accreditations. AWS has demonstrated compliance with third-party assurance frameworks such as ISO 27001, ISO 27017 for cloud security, ISO 27018 for

cloud privacy, PCI DSS Level 1 and SOC 1, SOC 2, and SOC 3 (see AWS Compliance Programs).

To learn more about AWS compliance, security programs, and common privacy and data protection considerations, see AWS Compliance Programs and Using AWS in the Context of Common Privacy and Data Protection Considerations.

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.

AWS 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 Regions in which their content is stored and the type of storage. The customer can replicate and back up the content in more than one Region. AWS does not move or replicate the content outside of the chosen Regions without the consent of the customer, except 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 guidelines paper that *"The cloud is a critical success factor for Switzerland and its financial centre."* For customers that want to retain data in Switzerland, AWS provides a Region in Switzerland.

A separate whitepaper 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 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 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 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 and in transit.

Encrypt data in your applications

The AWS Encryption SDK (ESDK) is a client-side encryption library designed 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. To learn more, see Using the AWS Encryption SDK with AWS KMS.

Manage encryption for AWS services

AWS KMS 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 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 cryptographic services related to AWS KMS, there are four options for encryption key management:

- AWS KMS with customer managed or AWS managed keys.
- AWS KMS with bring your own key (BYOK, KMS imported key).
- AWS KMS with a KMS custom key store key management backed by AWS CloudHSM.
- AWS KMS with external key stores.

Every AWS cryptographic service is backed by a FIPS 140-2 validated hardware security module (HSM). With AWS KMS, your keys are generated and managed on multi-tenant HSMs operated by AWS. You access these keys and cryptographic operations using the AWS 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. After you create a key in AWS KMS, AWS 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 does it in a manner consistent with cryptographic best practices. Learn more about demystifying KMS Key operations.

A *key store* is a secure location for storing cryptographic keys. The default key store in AWS KMS also supports methods for generating and managing the keys that it stores. By default, the cryptographic key material for the AWS KMS keys that you create in AWS KMS is generated in and protected by HSMs that are FIPS 140-2 level 3 validated cryptographic modules. Key material for your KMS keys never leaves the HSMs unencrypted.

However, if you require even more control of the HSMs, you can create a *custom key store*. A custom key store is a logical key store within AWS KMS that is backed by a key manager outside of AWS KMS that you own and manage.

AWS KMS supports two types of custom key stores.

- An AWS CloudHSM key store is an AWS KMS custom key store backed by an AWS CloudHSM cluster. When you create a KMS key in your AWS CloudHSM key store, AWS KMS generates a 256-bit, persistent, non-exportable Advanced Encryption Standard (AES) symmetric key in the associated AWS CloudHSM cluster. This key material never leaves your AWS CloudHSM clusters unencrypted. When you use a KMS key in AWS CloudHSM key store, the cryptographic operations are performed in the HSMs in the cluster. AWS CloudHSM clusters are backed by HSMs certified at FIPS 140-2 Level 3.
- An external key store is an AWS KMS custom key store backed by an external key manager outside of AWS that you own and control. When you use a KMS key in your external key store, all encryption and decryption operations are performed by your external key manager using your cryptographic keys. External key stores are designed to support a variety of external key managers from different vendors.

AWS KMS does not directly view, access, or interact with your external key manager or cryptographic keys.

FINMA ISAE 3000 Type 2 report and encryption

The FINMA ISAE 3000 Type 2 report, accessed through AWS Artifact, has a series of AWS control activities related to AWS cryptographic services, including (at the time of publication):

Control ID	Control details
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 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.
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	Attempts to access recovery key materials are reviewed by authorized operators on a monthly cadence.
AWSCA-4.14	The production firmware version of the AWS KMS HSM has been validated with NIST under the FIPS 140-2 standard or is in the process of being validated.

Controls and access to customer content

As an AWS customer, you maintain control over your content within the AWS environment. You can:

- Determine where your content is located, including the type of storage environment and geographic location of that storage.
- Control the format of your content, for example, plain text, masked, anonymized, or encrypted, using either AWS-provided encryption or a third-party encryption mechanism of your choice.
- Manage other access controls, such as identity management and security credentials.
- Control whether to use SSL, virtual private cloud, or other network security measures to prevent unauthorized access.

You control the entire lifecycle of your content on AWS, and you can manage your content in accordance with your own specific needs, including content classification, access control, retention, and deletion.

Access to customer content

As an AWS customer, you maintain full control of your content and are responsible for configuring access to AWS services and resources. AWS provides an advanced set of access, encryption, and logging features to help you do this effectively (for example, AWS Identity and Access Management (IAM), AWS Organizations, and AWS CloudTrail). AWS provides APIs for you to configure access control permissions for any of the services you develop or deploy in an AWS environment. AWS does not access or use your content for any purpose without your consent. AWS never derives information from your content for marketing or advertising.

Because AWS does not know what content customers choose to store on AWS and cannot distinguish between personal data and other content, AWS treats all customer content the same. In this way, all customer content benefits from the same robust AWS security measures, whether this content includes personal data or not. AWS simply makes available the compute, storage, database, and networking services selected by the customer with security measures applied to the cloud infrastructure provided by AWS. The customer is free to build on that infrastructure based on the customer's own unique security requirements.

AWS does not disclose customer information unless required to do so to comply with a legally valid and binding order. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS products or services, AWS notifies customers before disclosing content information.

Operational resilience

AWS builds to guard against outages and incidents and accounts for them in the design of AWS services—so when disruptions occur, their impact on customers and the continuity of services is as minimal as possible. To help avoid single points of failure, AWS minimizes interconnectedness within our global infrastructure. The AWS Global Infrastructure is geographically dispersed over five continents. It is composed of multiple geographic AWS Regions, which are composed of three or more Availability Zones (AZs), which in turn are composed of data centers. The AZs, which are physically separated and independent from each other, are also built with highly redundant networking to withstand local disruptions. Regions are isolated from each other, meaning that a disruption in one Region does not result in contagion in other Regions. Compared to global financial institutions' on-premises environments today, the locational diversity of the AWS infrastructure greatly reduces geographic concentration risk. AWS is continuously adding new Regions and AZs, and you can view our most current global infrastructure map on the Global Infrastructure page.

Customers have to make many decisions: where to place their content, where to run their applications, and how to achieve higher levels of availability and resiliency. For example, customers can choose to run a set of banking applications in a single Region across multiple AZs. Customers can increase or decrease their capacity at frequent intervals to align with transaction volumes, and track and manage changes to maintain its deployments with the same, up-to-date capacity and architecture. In addition, customers can maintain additional *cold* infrastructure and backups on AWS that can be activated if necessary—at much lower cost than procuring their own physical infrastructure. It is generally difficult to implement these designs through on-premises environments. AWS provides guidance to customers on best practices for building highly available, resilient applications, including through our Well Architected Framework.

Getting started

Each organization's cloud adoption journey is unique. In order to successfully manage 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 learn more about such workshops, 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, contact us.
- Obtain and review a copy of the latest C5 report, FINMA ISAE 3000 Type 2 report, AWS SOC 1 and 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification from the AWS Artifact portal (accessible through the AWS Management Console).
- Consider the relevance and application of the CIS AWS Foundations Benchmark 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.
- 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.
- Speak with your AWS representative to learn more about how AWS is helping financial services customers migrate their critical workloads to the cloud.

Further reading

The following are additional resources to help Swiss financial services customers 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, less complicated operations, and improved agility by providing more oversight, security control, and central automation.
- AWS Well-Architected Framework: The AWS 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 to meet application needs over time. The framework consists of six pillars: Operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability.
- AWS has produced whitepapers addressing each pillar of the AWS Well-Architected Framework: AWS Operational Excellence Pillar, AWS Security Pillar, AWS Reliability Pillar, AWS Performance Efficiency Pillar, AWS Cost Optimization Pillar, and AWS Sustainability Pillar.
- The Financial Services Industry Lens of the AWS Well-Architected Framework focuses on designing, deploying, and architecting financial services industry workloads that promote resiliency, security, and operational performance.
- Global financial services regulatory principles: AWS has identified five common principles related to financial services regulation that customers should consider when using AWS services and specifically, applying the AWS Shared Responsibility Model to their regulatory requirements. Customers can access a whitepaper on these principles under a non-disclosure agreement via 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 (that is, security in the cloud). The whitepaper also provides a third-party auditor letter attesting to the AWS Cloud offerings' conformance to NIST CSF risk management practices (that is, security of the cloud). Swiss FIs can use 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 that 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 how AWS services operate, including how they 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 plan for and document the 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 provides 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 more information, visit the Security Learning page.

Document revisions

Date	Description
June 2021	First publication.
August 2024	Second publication.