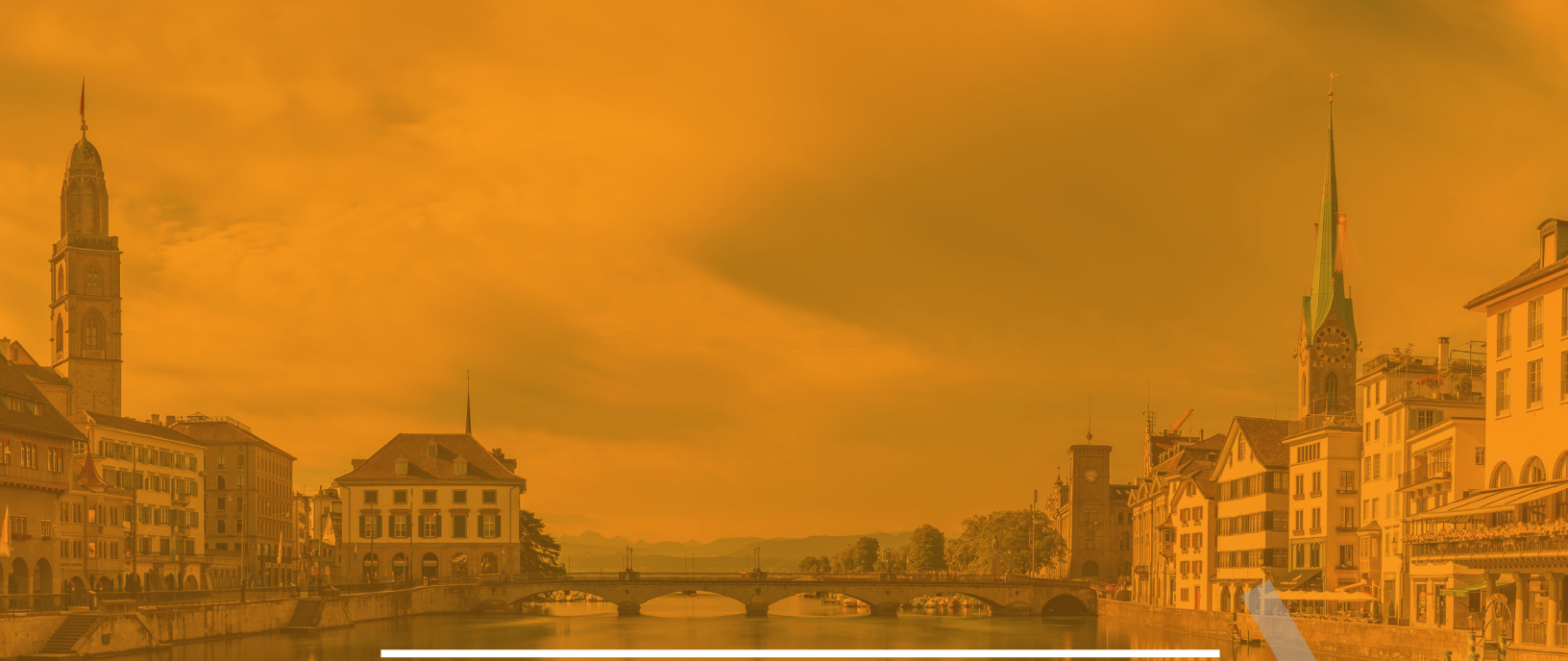


Swiss Financial Market Supervisory Authority (FINMA) Circular 2018/3

April 2018

This paper has been archived.

For the latest technical content, see the AWS Whitepapers & Guides page:

https://aws.amazon.com/whitepapers/

aws

[Resource Guide]

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. 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

Abstract

This document provides information to Swiss financial institutions seeking to use AWS services. FINMA Outsourcing Circular 2018/3 applies to banks, securities dealers, and insurance companies.

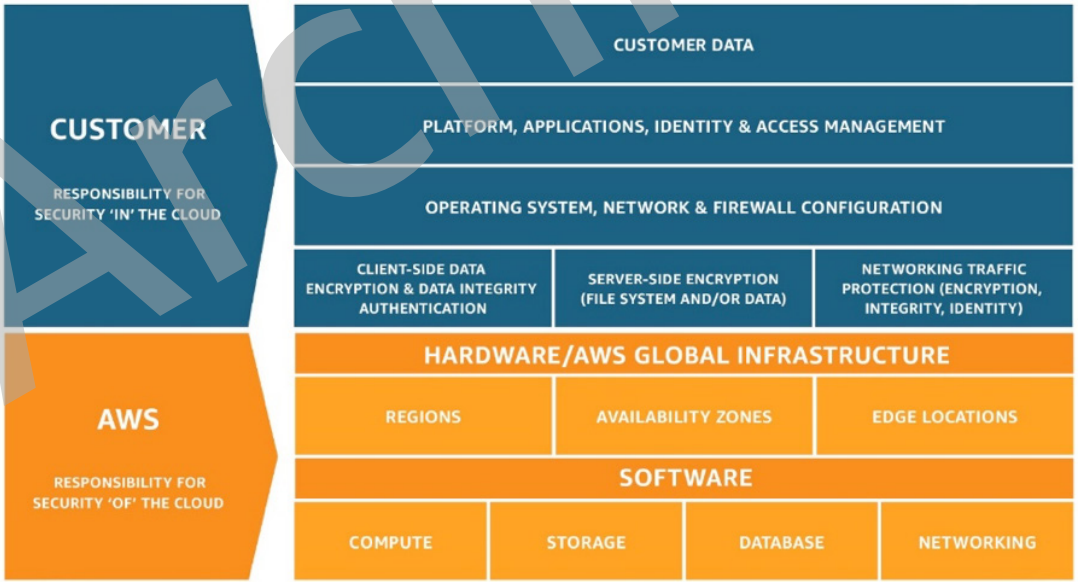
Introduction

The Swiss Financial Market Supervisory Authority (FINMA) published Circular 2018/3 Outsourcing with requirements for banks, securities dealers, and insurance companies that outsource functions that are material for their business. The purpose of this Resource Guide is to describe important considerations for FINMA-regulated entities who want to use AWS services to build highly available, resilient applications on the AWS Cloud.

FINMA supervises banks, insurance companies, and other financial entities in Switzerland. You should review the full text of FINMA's Circular 2018/3 Outsourcing, available at https://www.finma.ch/en/news/2017/12/20171205-mm-rs-outsourcing/. Customers should also review other applicable laws and regulations, such as the Swiss Federal Data Protection Act and revised FINMA Circular 2008/21 – "Operational Risks Banks."

Security and Shared Responsibility

Cloud security is a shared responsibility. AWS manages security of the cloud by ensuring that AWS infrastructure complies with global and regional regulatory requirements and best practices, but security in the cloud is the responsibility of the customer. What this means is that customers retain control of the security program they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site data centre.



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.

Security in the Cloud

Customers are responsible for their security in the cloud. Much like a traditional data centre, the customer is responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as the configuration of the AWS-provided security group firewall. 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 are used with the content.
- The country where their content is stored.
- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How their data is encrypted and where the keys are stored.
- 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. Customers are responsible for the security of the content they put on AWS, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, platforms, databases, or other services.

Security of the Cloud

In order to provide Security of the Cloud, AWS continuously audits its environments. The infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use the AWS compliance certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications.

The AWS compliance program is based on the following actions:

- **Validate** 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 can be implemented, and to better assist customers with managing their control environment.

- **Demonstrate** 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.
- **Monitor**, through the use of thousands of security control requirements, that AWS maintains compliance with global standards and best practices.

Governance and Monitoring

FINMA-regulated entities are responsible for establishing a governance framework and monitoring their own environments, while AWS provides many tools to help customers efficiently achieve compliance. For example, AWS Config allows customers to continuously monitor and record their AWS resource configurations, and automatically evaluate the recorded configurations against the desired configurations. Amazon CloudWatch allows customers to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health.

AWS provides up-to-the-minute information on the health of AWS services at the publicly available Service Health Dashboard. Customers can configure a Personal Health Dashboard to receive a personalized view of the performance and availability of the AWS services underlying their resources and applications. The dashboard displays relevant and timely information to help customers manage events in progress, and it provides proactive notification to help customers plan for scheduled activities. With Personal Health Dashboard, changes in the health of AWS resources automatically trigger alerts, providing event visibility and guidance to help quickly diagnose and resolve issues. Customers can use these insights to react and keep their applications running smoothly.

AWS Regions

The AWS Cloud infrastructure is built around AWS Regions and Availability Zones. An AWS Region is a physical location in the world that is made up of multiple Availability Zones. Availability Zones consist of one or more discrete data centres that are housed in separate facilities, each with redundant power, networking, and connectivity. These Availability Zones offer customers the ability to operate production applications and databases at higher availability, fault tolerance, and scalability than would be possible from a single data centre. The AWS Cloud operates 54 Availability Zones within 18 AWS Regions around the world. For current information on AWS Regions and Availability Zones, see https://aws.amazon.com/about-aws/global-infrastructure/.

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 requirements. For example, Swiss banks and insurers can choose to launch in the AWS Regions Frankfurt, Ireland, London, and Paris. A new AWS Region, Sweden, is coming soon.

Customer Controls and Access to Customer Content

Customer control over 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, anonymised, 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 unauthorised access.

As an AWS customer, you control the entire life-cycle 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

AWS does not access any customer's content, except as necessary to provide that customer with the AWS services it has selected. AWS does not access any customer's content for any other purposes.

AWS does not know what content customers choose to store on AWS and cannot distinguish between personal data and other content, so 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 best-in-class security measures applied to the cloud infrastructure provided by AWS. Customer is then free to build on that infrastructure security based on the customer's own, unique requirements. You can also read more about AWS's views on data residency at https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf.

Business Continuity and Disaster Recovery

FINMA-regulated entities must implement policies and procedures to ensure that their applicable systems have high levels of resiliency and availability. Customers can use AWS to enable faster disaster recovery of their IT systems without incurring the infrastructure expense of a second physical site. With data centres in locations all around the world, AWS provides a set of cloud-based disaster recovery services that enable rapid recovery of customers' IT infrastructure and data. The AWS Cloud supports many popular disaster recovery architectures, including "pilot light" environments that are ready to scale up at a moment's notice and "hot standby" environments that enable rapid failover.

FINMA Circular 2018/3: Outsourcing – banks and insurers

The following table provides additional considerations about how AWS customers can meet the requirements in FINMA Circular 2018/3. This table contains a non-exhaustive sample of recommendations and considerations. This is not legal or compliance advice. Customers should consult with their legal and compliance teams. For more information, contact your AWS Account Manager.

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 17	The selection process for the service provider must consider and scrutinize its professional capabilities and its financial and human resources. If multiple functions are outsourced to a single service provider, account must be taken of concentration risk.	Customer Responsibility	Since 2006, AWS has provided flexible, scalable, and secure IT infrastructure to businesses of all sizes around the world. AWS continues to grow and scale, allowing us to provide new services that help millions of active customers. AWS maintains a systematic approach to planning and developing new services for the AWS environment to ensure that the quality and security requirements are met with each release. The 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 financial statements of Amazon.com Inc. include AWS sales and income, permitting assessment of its financial position and ability to service its debts and/or liabilities. These financial statements are available from the SEC or at Amazon's Investor Relations website at http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-irhome. For applications that need to be highly available, banks and insurers can increase their resiliency by using multiple AWS Regions and Availability Zones in AWS's infrastructure and services. AWS provides you with the capability to implement a robust continuity plan, including frequent server instance backups, data redundancy replication, and the flexibility to place instances and store data within multiple AWS Regions as well as across multiple Availability Zones within each AWS Region. For more information about disaster recovery approaches, see Disaster Recovery.

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 18	Furthermore, account must be taken when deciding on the outsourcing and selecting the service provider of the possibilities for and consequences of switching provider. The service provider must be able to guarantee the stable provision of the services. It must be ensured that the outsourced function can return to the company in an orderly fashion.	Customer Responsibility	Customers are not tied into their contracts through minimum terms or minimum commitments. AWS customers can exercise their right to terminate their agreement for convenience at any time. If you decide to leave AWS, you can manage access to your data and AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Import/Export to transfer large amounts of data into and out of AWS using physical storage appliances. For more information, see Cloud Storage with AWS. AWS offers AWS Database Migration Service, a web service that you can use to migrate a database from an AWS service to an on-premises database. AWS also provides you with the ability to delete your data. Because you retain control and ownership of your data, it is your responsibility to manage data retention according to your own requirements. In the event customers require further assistance during migration, AWS professional services can be engaged to provide assistance in the development of an exit strategy, as well as post-termination assistance. Customers also have the option to enrol in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs. For more information about Enterprise Agreements and professional services, please contact your AWS Account Manager.

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 24	Where an outsourcing is relevant for security (specifically in the area of IT), the company and the service provider must contractually establish security standards. The company must monitor compliance with these.	Shared Responsibility	AWS employs a shared responsibility model for data ownership and security. AWS operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems and content. AWS maintains a broad range of industry and geography specific compliance programs and is continually assessed by external certifying bodies and independent auditors to provide assurance that the policies, processes, and controls established and operated by AWS are in alignment with these program standards and the highest industry standards. Customers can use AWS Artifact to monitor compliance with standards that AWS is audited against, and to download security and compliance documents, such as AWS ISO certifications and System and Organization Control (SOC) reports. Customers assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS-provided security group firewalls and other security, change management, and logging features.

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 25	The company and the service provider must develop a security framework that allows the outsourced function(s) to be continued in an emergency. In developing and applying the security framework, the company must exercise the same care that it would if it were to provide the outsourced function itself.	Shared Responsibility	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 all AWS Regions. Each data centre 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 have at least one independent backup component, so the backup component is active in the operation even if all other components are fully functional. In order to eliminate single points of failure, this model is applied throughout AWS, including network and data centre implementation. All data centres 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. For more information, see the Overview of Security Processes whitepaper and the SOC 2 report in Artifact. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 26 - 27	The company, its auditors and FINMA must be able to verify compliance by the service provider with supervisory requirements. They must be contractually granted an unlimited, unhindered right of inspection and audit at any time in relation to the outsourced function(s). Audit activities may be delegated to the service provider's internal audit unit where this has the requisite specialist expertise. If such delegation takes place, the company's audit firm may make use of the audit findings of the service provider's internal audit unit.	Shared Responsibility	The AWS service offering is different to typical managed outsourcing. The AWS services are set up to be used in a self-service way, putting customers in the driver's seat when it comes to architecting, provisioning, and monitoring the services. This means that customers do not outsource management or supervisory functions to AWS. Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001, Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards. In particular, ISO 27018 focuses on protection of personal data in the cloud. Independent assessment and certification against ISO 27018 demonstrates AWS's system of controls to specifically address the privacy protection of customer content. Customers can download a copy of our current ISO 27018 certification here. Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS compliance reports identify the scope of AWS services and regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by using these reports and certifications. If you have any further questions about AWS's approach to security and compliance, please contact your AWS Account Manager.

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 28-29	Outsourcing of a function must not make supervision by FINMA more difficult, particularly when outsourcing abroad. If the service provider is not subject to supervision by FINMA, it must contractually undertake to the company to make available to FINMA all information and documents relating to the outsourced business area that FINMA requires for supervisory purposes. If audit activities are delegated to the service provider's internal audit unit, its report must be made available to FINMA, the company's internal audit unit and the company's auditors upon request.	Shared Responsibility	AWS proactively engages with financial regulatory agencies, central banks, and finance ministries around the world, including FINMA, to explain AWS's approach to security and compliance across our global infrastructure. In addition, AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.
§ 30-31	Outsourcing to another country is permitted provided that the company can give express assurance that it itself, its auditors and FINMA can exercise and enforce their rights of inspection and audit. It must be possible for the company to be restructured or liquidated in Switzerland. The necessary information in this regard must be accessible in Switzerland at all times.	Customer Responsibility	These requirements relate to ownership and control of customer content. Customers manage access to their customer content and AWS services and resources. We provide an advanced set of access, encryption, and logging features to help customers do this effectively (such as AWS CloudTrail). Customers choose the AWS Region(s) in which their customer content will be stored. We will not move customer content outside of the customer's chosen AWS Region(s), except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users. Customers choose how their customer content is secured. We offer our customers strong encryption for customer content in transit or at rest, and we provide customers with the option to manage their own encryption keys. Customers can also grant cross-account read-only permission to data stored within their AWS accounts to third parties, including their auditors and regulators.

Requirement Reference	Requirement	Implementation	Implementation Considerations
§ 32-34	Outsourcing must be based on a written agreement. As well as naming the parties and describing the function, the agreement must contain the following information as a minimum (Margin nos. 33–34): The company must make the use of subcontractors in the performance of significant functions dependent on its prior consent. If such subcontractors are used, the duties and assurances of the service provider required for compliance with this circular shall transfer to it too. Contractual provisions on the implementation of the requirements under this circular, and in particular Margin nos. 21, 24, 26, 29, 30 and 31 must be included.	Shared Responsibility	A written AWS customer agreement is a pre-requisite to using the AWS service offerings. 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 currently no subcontractors authorized by AWS to access any customer-owned content that customers upload onto AWS. To monitor subcontractor access year-round, please refer to https://aws.amazon.com/compliance/third-party-access/.

Conclusion

AWS's resilient, secure, and elastic cloud solutions allow customers to meet the requirements of FINMA Circular 2018/3. Customers who are running well-architected applications on the AWS Cloud can decrease their operational risk and increase the security, availability and resiliency of their systems. For more information about AWS's regulatory compliance programs, see https://aws.amazon.com/compliance/resources/.

Document Revisions

Date	Description
April 2018	First publication.