TERMS AND CONDITIONS

You hereby agree that you will not distribute, display, or otherwise make this document available to an *individual or entity*, unless expressly permitted herein. This document is AWS Confidential Information (as defined in the AWS Customer Agreement), and you may not remove these terms and conditions from this document, nor take excerpts of this document, without Amazon's express written consent. You may not use this document for purposes competitive with Amazon. You may distribute this document, in its complete form, upon the commercially reasonable request by (1) an end user of your service, to the extent that your service functions on relevant AWS offerings provided that such distribution is accompanied by documentation that details the function of AWS offerings in your service, provided that you have entered into a confidentiality agreement with the end user that includes terms not less restrictive than those provided herein and have named Amazon as an intended beneficiary, or (2) a regulator, so long as you request confidential treatment of this document (each (1) and (2) is deemed a "Permitted Recipient"). You must keep comprehensive records of all Permitted Recipient requests, and make such records available to Amazon and its auditors, upon request.

You further (i) acknowledge and agree that you do not acquire any rights against Amazon's Service Auditors in connection with your receipt or use of this document, and (ii) release Amazon's Service Auditor from any and all claims or causes of action that you have now or in the future against Amazon's Service Auditor arising from this document. The foregoing sentence is meant for the benefit of Amazon's Service Auditors, who are entitled to enforce it. "Service Auditor" means the party that created this document for Amazon or assisted Amazon with creating this document.

term-token-Yi3YZOU8rrzFfzdFt3LDE2t

Global Financial Services Regulatory Principles

Described for AWS Services

November 2016

term-token-Yi3YZOU8rrzFfzzdFt3LDE2t

© 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.

term-token-Yi3YZOU8rrzFfzdFt3LDE2t

Contents

term-token-Yi3YZOU8rrzFfzzdFt3LDE2t

Introduction

Financial Services executives are facing pressures to lower IT cost, quickly innovate the business, and utilize new technologies to design for the future. These pressures are why Financial Services executives are no longer asking "if" they will move to the cloud, but **"how" to meet their regulatory obligations** when moving to the cloud.

Most jurisdictions that regulate Financial Services don't prohibit the use of cloud services, but require a higher level of due diligence from customers who are using third-party service providers, one that is commensurate with the level of associated risk. AWS serves many customers in highly-regulated sectors, including Financial Services, Healthcare, Government and Defense. Because AWS services are designed to achieve high levels of security, regardless of the sector, we can assist you in achieving compliance with regulatory obligations through a proper risk assessment of cloud services, and achieve long-term security agility compared to the long-term alternatives of on-premise or colocation.

Although requirements vary by jurisdiction, we have identified five common principles related to Financial Services regulation that you should know when considering AWS cloud services.

- **Cloud Governance:** *Have appropriate oversight for cloud services*
- **Data Security and Privacy:** *Design for Data Security & Privacy*
- **Disaster Recovery/Business Continuity:** *Focus on Application Resiliency*
- **Incident Response:** *Understand Incident Management & Response*
- **Reversibility:** *Design with Reversibility in Mind*

This document provides guidance in meeting your compliance obligations under these regulatory principles while moving to the cloud.

term-token-Yi3YZOU8rrzFfizdFt3LDE2t

Principle 1: Have appropriate oversight for cloud services

What makes AWS cloud services unique as a third-party provider is the shared responsibility model. As such, Financial Services customers must demonstrate the steps they have taken to understand and implement their control responsibilities.

While the implementation of shared responsibility may be different for every Institution, you should consider the following steps in your use of AWS services:

Institution, you should consider the following steps in your use of AWS services:

1. Understand AWS services and the workload(s) to be moved onto AWS.

   Use AWS resources to develop your use case and educate all internal and external stakeholders on AWS services and features, including the AWS Shared Responsibility Model. These resources available to assist you include AWS Service documentation - https://aws.amazon.com/documentation/, AWS Shared Responsibility - https://aws.amazon.com/compliance/shared-responsibility-model/ and AWS customer stories - https://aws.amazon.com/solutions/case-studies.

2. Conduct a risk and control assessment.

   Your risk and control assessment will be distinct to your Institution, and as such, you should seek to align the control responsibility and add any new controls that should be considered for AWS services. AWS provides services that enable customers to meet their security and control requirements, including Financial Services regulations in regions worldwide. Customers can view evaluations of the design and operating effectiveness of AWS controls performed by third-party auditors. For example, customers can request a copy of the SOC 2 report, under NDA, here: https://aws.amazon.com/compliance/contact/. AWS also provides supporting documentation for control mapping, including the AWS FFIEC Workbook.

3. Design for Regulatory Compliance in advance.

   AWS's assurance program is designed to meet the needs of Financial Services customers and their regulatory requirements. There are three

term-token-Yi3VZOU8rrZFfzzdFt3LDE2t

underlying principles for continuous supervision of your use of cloud services:

a. Partner cloud tech SMEs with security/ compliance SMEs. Through this partnership, compliance SMEs will be able to update regulators on cloud adoption, influence the use of audit capabilities (see point 3), and determine the appropriate regulatory requirements to consider.

b. Understand the regulatory requirements applicable to your use of cloud services: The majority of regulatory requirements applicable to cloud services were not written for cloud technology. It is important to consider how your use of cloud services can change the fundamental meaning of a regulation and the method with which you will comply with it.

   It is occasionally necessary to consider the principle of a regulatory requirement and to re-image your current requirement to adapt to virtualization and shared responsibility. Contact your account manager and request AWS' Financial Services Contract Guidance, provided under NDA, for additional guidance.

c. Supervision plan: This plan details your use case and procedures for procurement of cloud services, the management of your environment and account(s), and the internal departments and plans with responsibilities for cloud service operations. This plan should be a primer for any regulatory exam regarding cloud services.

d. Automate and formalize security and compliance: Security by Design (SbD) is a security assurance approach that formalizes AWS account design, automates security controls, and streamlines auditing. Instead of relying on auditing security retroactively, SbD provides security controls built in throughout the AWS IT management process. By utilizing Security by Design CloudFormation templates, security and compliance in the cloud can be made more efficient and expansive. SbD enables customers to automate the front end structure of an AWS account, reliably coding security and compliance into AWS accounts, making non-compliance of IT controls a thing of the past.

term-token-Yl3YZOU8rrzFfzdFt3LDE2t

Commonly Asked Question(s)

How do Institutions demonstrate comprehensive governance in AWS' shared responsibility model that meets regulatory expectations?

AWS has worked with Institutions worldwide to help them achieve regulatory alignment for cloud services. This alignment may be architectural or contractual, but worldwide, institutions are able to consider AWS services because they can achieve and demonstrate greater transparency and compliance with their requirements.

Principle 2: Design for Data Security & Privacy

Maintaining customer trust is an ongoing commitment, and we strive to provide transparency to the privacy and data security policies and practices and technologies we've put in place. There are four distinct AWS security and privacy principles that you should know:

1. **Data Location**: You retain complete control and ownership over the region in which your data is physically located, making it easy to meet regional compliance and data residency requirements. As a customer, you choose the region(s) in which Your Content will be stored. We will not move or replicate Your Content outside of the customer's chosen region(s), except as legally required and as publically documented to provide services to the customer.
2. **Access & Content Disclosure:** You manage access to Your Content and AWS services and resources. We do not access or use Your Content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. You also should discuss with your account manager the contractual commitments AWS may offer with respect to your regulatory authority's access requirements.
3. **Privacy:** AWS gives customers ownership and control over their content by design through simple, but powerful tools that allow customers to determine where their customer content will be stored, when to secure

term-token-Yi3YZOU8rrzFfzzdFt3LDE2t

content in transit or at rest, and how to manage access to AWS services and resources for their users. We also implement responsible and sophisticated technical and physical controls designed to prevent unauthorized access to or disclosure of customer content. We are vigilant about our customers' privacy. We do not disclose customer content unless we're required to do so to comply with the law or a valid and binding order of a governmental or regulatory body. Governmental and regulatory bodies need to follow the applicable legal process to obtain valid and binding orders, and we review all orders and object to overbroad or otherwise inappropriate ones. It's also important to point out that our customers can encrypt their content, and we provide customers with the option to manage their own encryption keys.

4. **Security:** AWS services provides you with a high bar of security features and you benefit from our continuous innovation in security Our customers have direct access to our development teams, so our fast innovation is a result of helping our customers meet their compliance requirements.

One advantage of AWS are the services that can be coupled to achieve a high levels of security and transparency. With services like AWS CloudFormation, AWS Config, AWS Config Rules, and AWS SNS, you can easily design for mature security implementation and monitoring by:

- Creating secure, pre-vetted reference architectures which can meet specific compliance objectives and incorporate patterns and principles of the AWS Cloud Adoption Framework.
- Managing a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion.
- Reviewing AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.
- Automating rules that check the configuration of AWS resources recorded by AWS Config to ensure consistent compliance.

For institutions who must adhere to strict security, compliance, and risk management controls, AWS provides a high level of support and services, including AWS Professional Services (https://aws.amazon.com/professional-services) where we leverage hundreds of customer's learnings and their AWS experience to help you achieve your business goals.

term-token-Yi3YZOU8rrzFfzdFf3LDE2t

Contact your AWS representative for assistance or get assigned a representative today, https://aws.amazon.com/contact-us.

Commonly Asked Question(s)

What security and privacy information does AWS offer specific to meeting regulatory requirements?

Across jurisdictions, Institutions have differing levels of security and privacy concerns, here are some resources for consideration:

- AWS Compliance: https://aws.amazon.com/compliance/ - see Laws, Regulations, and Privacy
- EU Model Clauses: https://aws.amazon.com/compliance/eu-data-protection/
- AWS Security: https://aws.amazon.com/security/

Principle 3: Focus on Application Resiliency

The resiliency and stability of the Financial Services industry is critical to regional and global economies. Disaster recovery is about preparing for and recovering from a disaster. Any event that has a negative impact on a company's business continuity or finances could be termed a disaster.

AWS regions are specifically designed to meet standards for geographically dispersed resources. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area within the region. AWS's physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. You can view our certification here.

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 multi-region/Availability Zone deployment architectures. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple

term-token-Yi3YZOU8rrzFfzzdFt3LDE2t

Availability Zones within each region. Financial Services customers have used AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS cloud supports many popular disaster recovery (DR) architectures from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover. AWS gives customers fine-grained control and many building blocks to build the appropriate DR solution, given their DR objectives and budget. The AWS services are available on-demand, and customers only pay what they use. This is a key advantage for DR, where significant infrastructure is needed quickly.

Get to know more about Disaster Recovery capabilities on AWS at https://aws.amazon.com/disaster-recovery/ and https://aws.amazon.com/backup-recovery/.

Commonly Asked Question(s)

How do Institutions meet their Business Continuity and Disaster Recovery obligations using AWS services?

Institutions have varying degrees of recovery requirements. AWS Professional Services and Technical account team members have worked with thousands of clients to consider their resiliency and continuity requirements. Talk to your AWS account manager for your specific needs. AWS' disaster recovery plan is extensive and, as noted above, part of our third-party auditing program. Institutions can read about AWS's business continuity plan in the SOC 2 third-party audit report under NDA. 4:

Principle 4: Understand Incident Management & Response

Worldwide, Financial Services regulations have differing reporting requirements for incidents that impact your systems, with the goal of immediately remediating issues and overall reducing the occurrences of technical issues. The AWS shared responsibility model requires that you monitor and manage your environment at the operating system level and upward. Many services provide built-in access control audit trails (for example, Amazon S3 and Amazon EMR provide such logs). For more information on

term-token-Yi3YZOU8rrzFfzdFi3LDE2t

logging & monitoring visit, http://aws.amazon.com/whitepapers/aws-security-best-practices/.

AWS offers services such as Amazon CloudWatch, to monitor AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.

AWS uses various methods of external communication to support its customer base and the community. The customer support team is notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

AWS has a formally documented incident response plan for AWS services which addresses purpose, scope, roles, responsibilities, and management commitments. It has been developed in alignment with ISO 27001 and NIST 800-53 standards. The AWS incident management program is reviewed by independent external auditors during audits of AWS's SOC, PCI DSS, ISO 27001, and FedRAMP compliance. Request a copy of our AWS SOC 2 report to read more about it.

Commonly Asked Question(s)

How do Institutions design for incident response that meets regulatory obligations?

AWS services offers partnerships with many of the same vendors you are currently using to monitor your current environment. Read more about how to log and monitor in your AWS environment here: https://aws.amazon.com/security/.

term:token-Yi3YZOU8rrzFfzdFf3LDE2t

How do Institutions satisfy their regulatory obligations for incidents that arise from an event in an area of AWS responsibility?

Institutions should understand shared responsibility as it relates to resiliency, availability and security. In many instances, a failure of AWS services can be mitigated through customer design. For example, if a server that a customer is using fails, a customer can design the system to fail over to a different Availability Zone or even Region.

Principle 5: Design with Reversibility in Mind

Your business continuity plan requires you to plan for reversibility and to disengage from AWS if circumstances arise. You can achieve reversibility using AWS, whether you transition back on-premise, colocation, or to another provider.

AWS offers services that can be used to design an exit strategy for services that are internally compatible or externally transferable. For example, AWS Simple Storage Service (S3) and Glacier, customers only need to consider how they will export their objects from the services. AWS offers several ways to export customer data, including a large storage appliance service called Snowball.

AWS offers a simple, pay-as-you-go pricing approach for over 50 cloud services. With AWS you pay only for the services you need, for as long as you use them, and you have the ability to terminate your contract at any time. You also don't have to worry about dependencies, complex licensing or termination fees. AWS believes that if we are not delivering the right quality of services, customers should be able to walk away. The customer should be in full control.

Institutions will find it is manageable to design for this contingency, whether it is to export objects or lift-and-shift applications.

Commonly Asked Question(s)

How does AWS support cases in which regulatory agencies request access in the case of institutional failure?

term-token-vi3YZoU8rrzFfzzdFt3LDE2t

AWS offers commitments to comply with regulatory agencies; however, institutions need to consider that AWS will only have an ability to provide information as it resides on AWS, and thus we cannot rectify data that is encrypted or in an unreadable format. One method to rectify this problem is for institutions to designate vendors for "breaking glass" methods that permit access only in the case of bankruptcy, emergencies or failures.

Conclusion

The above considerations are relevant to many jurisdictions, and AWS is confident that you can use AWS services to exceed your current level of risk for security and privacy.

AWS also provides support programs designed for highly regulated customers. More information is available at https://aws.amazon.com/premiumsupport/. Your AWS Account Manager can tell you about how you can use these programs to meet your Financial Services regulatory obligations. Some of the benefits of the Enterprise support tier includes:

- Shared commitments with AWS that are in alignment with the regulatory obligations and cloud services.
- Greater visibility into AWS services.
- Access to specialized team members for security, risk and compliance discussions.
- Participation in Financial Services AWS community discussions for shared information.

To hear directly from our Financial Services customers on how they are using AWS, go to http://aws.amazon.com/financial-services/.

Further Reading

For additional information, see the following sources:

- AWS Compliance (https://aws.amazon.com/compliance/)
- Enterprise Addendum for Financial Services (Contact your Account Manager)

term-token-Yi3YZOU8rrZEfzzdFt3LDE2t

- Get Started on AWS (https://aws.amazon.com/documentation/gettingstarted/)
- Cloud Adoption Framework (https://aws.amazon.com/professional-services/CAF/)
- Risk & Compliance Whitepaper, Appendix A CSA Consensus Assessments Initiative Questionnaire (http://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf)

Document Revisions

November 2016 First publication

term-token-Yi3YZOU8rrzFfzzdFt3LDE2t