AWS & Cybersecurity in the Financial Services Sector

July 2019

Notices

Contents

Introduction

Amazon Web Services (AWS) provides information technology (IT) building blocks for customers of all types, from governments to commercial enterprises to universities, so they can become more secure, innovative, and responsive to the needs of their end-users. We provide standardized services and make them available to all customers, including in the financial services industry, and these services range from core infrastructure such as compute, storage, database, and networking to services such as video management and streaming, Internet of Things services, and artificial intelligence/machine learning. Across all of services, our top priority is security.

The goal of this paper is to describe AWS's approach to cybersecurity with a specific lens on the financial services industry. We know how important it is for the public to maintain its trust and confidence in secure, resilient financial institutions. The high bar for security that we maintain applies to all of our customers, who trust us to operate more than 165 fully featured services. In the financial services sector, as part of our continuous engagement with finance ministries, central banks, and regulators, we discuss how AWS's services are designed and built to allow all of our customers to operate and innovate securely. We have observed that there are common, recurring topics that customers, regulators, and policymakers often express interest in: the shared responsibility model, technologies like hypervisors and encryption, our views on the financial services regulatory landscape, and our recommended best practices for individual financial institutions' cloud adoption. We have organized this whitepaper according to those subject areas and look forward to our continued, deep engagement with customers and their regulators alike.

Security as a Shared Responsibility

When customers use AWS services, they are operating in an environment of what we call *shared responsibility*. Shared responsibility means that the secure functioning of an application on AWS requires action on the part of both customers and AWS. We recommend that financial institutions explain the shared responsibility model to all of their stakeholders throughout the design, development, testing, and production phases of cloud adoption.

Customers are responsible for their security "in" the cloud. They control and manage the security of their content, applications, systems, and networks. AWS manages security "of" the cloud to protect our infrastructure and services, maintain our operational performance, and meet relevant legal and regulatory requirements. In light of the variety

of international standards and guidance on cybersecurity in the financial services sector, financial entities need to consider how the shared responsibility model applies to each of the laws, regulations, and standards they are subject to as well as the specific AWS services they seek to use.

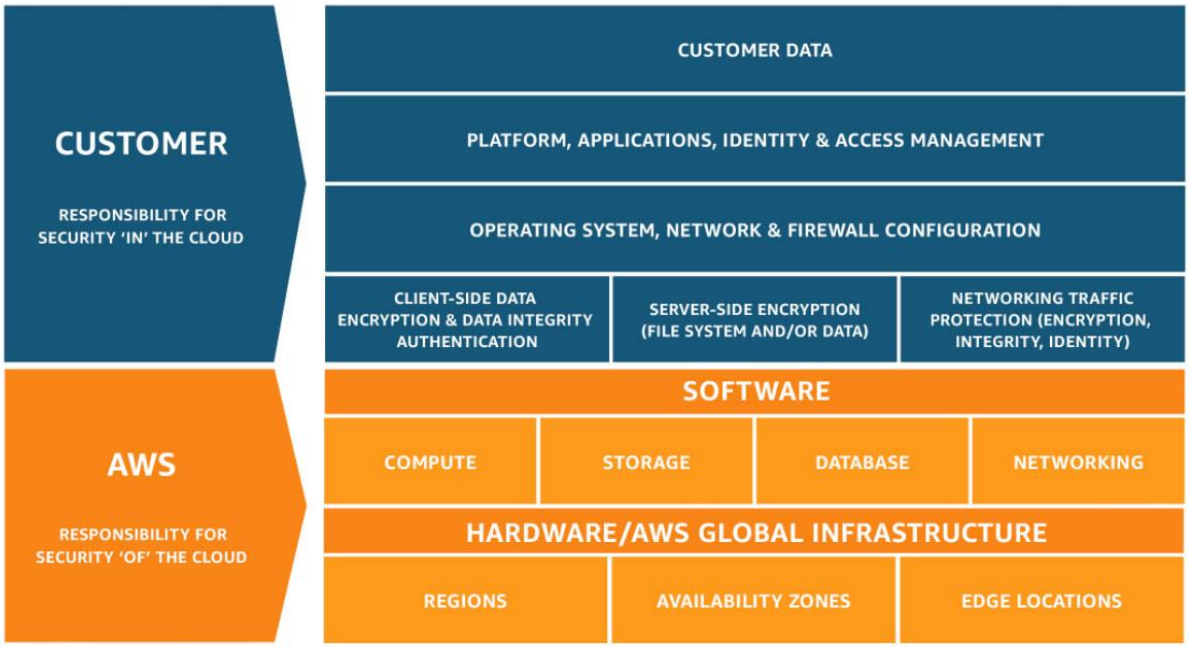

Figure 1. Shared Responsibility Model

Security of the Cloud

AWS operates the global cloud infrastructure that customers use to provision a variety of computing resources, such as processing and storage. The AWS global infrastructure includes the facilities, network, hardware, and operational software (*e.g.*, host operating system, virtualization software) that support the provisioning and use of these resources. The AWS Global infrastructure is built around Regions and Availability Zones (AZs). AWS Regions provide multiple, physically separated, and isolated Availability Zones which are connected with low latency, high throughput, and highly redundant networking. As of the writing of this paper, the AWS Cloud spans 66 Availability Zones within 21 geographic Regions around the world, with announced plans for 12 more Availability Zones and 4 more Regions in Bahrain, Cape Town, Jakarta, and Milan. We are continuously adding new Regions and AZs, and you can view our most current global infrastructure maps here https://aws.amazon.com/about-aws/global-infrastructure/ and https://infrastructure.aws.

At AWS, information security is a critical aspect of each individual's roles and responsibilities. The high bar that we maintain for security benefits our financial services customers of all types and sizes—from community banks to systemically important financial institutions, from fintech start-ups to financial market utilities. Because we serve virtually every commercial and public sector segment, we build our services and our own systems so that they are secure by design. We validate and provide assurance that our security practices align and comply with the appropriate and relevant laws, frameworks, standards, and regulations.

Cybersecurity governance begins at the top of AWS. We implement not only a rich variety of state-of-the-art technical mechanisms, but also strong organizational mechanisms to drive good behavior. Once a week, the CEO of AWS meets with senior AWS leaders to discuss any security issues and how they are being addressed throughout the AWS teams that build and operate our services. Also each week, the Chief Information Security Officer (CISO) reviews the progress of Application Security ("AppSec") reviews, thousands of which we conduct each year. Every AWS service goes through an AppSec review, which includes the development and maintenance of a formal threat model, multiple informal and formal security reviews during the development phase, and, near the end of the release cycle, a set of penetration tests prior to launch. Other types of penetration tests, such as post-launch red-team tests, occur constantly throughout the year to make sure we are addressing and anticipating changes in the cyber threat landscape. Overall, we focus on enabling a positive security culture through automation, guardrails, and tooling.

We design and manage AWS's global infrastructure according to security best practices, as well as a variety of compliance standards. To continually raise the bar on security throughout AWS, we developed a program called Security Expectations that sets a series of expectations, goals, and metrics for service teams throughout AWS. We measure service teams' progress on these expectations, which cannot be achieved through "check the box" compliance or manual efforts—they must be achieved through improved automated tooling and processes. As we operate infrastructure hosting millions of active customers, we build automation into our security processes, from radically restricting and monitoring human access to data, to tearing down end-of-life or unpatched systems and launching known good systems.

We encourage financial institutions and their customers to explore the ways in which AWS provides assurance about the security of our environment. To understand our security controls and how we operate them, customers can access our third-party audit reports; financial services customers regularly review our System and Organization Controls (SOC) 2 Type II report prepared by our independent, third-party auditor.

Furthermore, an independent third-party auditor certifies regularly AWS's compliance with the ISO/IEC JTC1 27001 standard. The International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) Joint Technical Committee 1 (JTC1) brings together experts to share knowledge and to develop and publish uniform international standards for the Information and Communication Technology sector that support innovation and provide solutions to global challenges. The basis of the ISO/IEC 27001 standard is the development and implementation of a rigorous security program. The Information Security Management System (ISMS) required under the ISO/IEC 27001 standard defines how AWS manages security in a holistic, comprehensive manner. In addition to ISO/IEC 27001, AWS also complies with the ISO/IEC 27017 guidance on information security in the cloud and ISO/IEC 27018 code of practice on protection of personal data in the cloud.

Customers can use our third-party audit reports and certifications to validate the implementation of AWS's security controls and can access them through AWS Artifact.

Security in the Cloud

AWS services allow customers to maintain control over their content—and that includes decisions on how to secure their content. The AWS Cloud helps customers improve their security posture. For example, security begins with inventory—understanding what you have. Unlike on-premises environments, in which entities may have to scan their networks to find unknown servers, on AWS, customers have APIs that give full visibility of all of their AWS resources.

Customers 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 the content is stored.
- The format and structure of that content and whether it is masked, anonymized, or encrypted.
- How the data is encrypted and where the keys are stored.
- Who has access to that content and how those access rights are granted, managed, and revoked.

Customers should carefully consider how they will manage 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. On page 13, we dive deeper into how those decisions fit into customers' overall cloud adoption process.

We recommend that customers think about their security responsibilities on a service-by-service basis because the extent of their responsibilities may differ between services. For example, customers have complete control in configuring and managing the security of virtual servers. For Amazon Elastic Compute Cloud (EC2) instances, customers can manage the guest operating system (including updates and security patches), any application software or utilities installed on the instances, and configuration of security groups. After launching an EC2 instance, a customer can then install its own database software, which may be one element of a broader application stack. A customer can also choose to use managed services, such as databases, directory, and web application firewall services,[1] which provide customers the resources they need to perform specific tasks without having to launch and maintain virtual machines. For example, a customer can launch an Amazon Aurora database, which Amazon Relational Database Service (RDS) manages to handle tasks such as provisioning, patching, backup, recovery, failure detection, and repair.

We also recommend that customers think about their security responsibilities as they relate to the expectations of their policymakers and regulators. For example, the United States Treasury Department has called for financial institutions to conduct fundamental security practices such as: (1) requiring multi-factor authentication (MFA), (2) enforcing privileged access, (3) performing regular maintenance and patching, and (4) scanning systems for malicious activity.[2]

On AWS, customers can deploy cyber hygiene best practices at scale across the services they use. We offer a number of security services that are tightly integrated into the AWS platform to help customers easily implement security controls for their environments.

Customers can enable federation with Amazon Identity and Access Management (IAM) to manage access to AWS accounts centrally by adding or removing users from their corporate directories, require MFA for all users as part of IAM best practices, use SSL/TLS to communicate securely with AWS resources, and set up API/user activity logging with AWS CloudTrail. Customers can also use Amazon Inspector assessments to help check for unintended network accessibility of Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered as pre-defined rules packages mapped to common security best practices and vulnerability

definitions. Examples of built-in rules include checking for access to your EC2 instances from the internet, remote root login being enabled, or vulnerable software versions installed. These rules are regularly updated by AWS security researchers. Furthermore, customers can use AWS Systems Manager Patch Manager to automate the process of patching managed instances with security-related updates. Customers can scan instances to see only a report of missing patches, or scan and automatically install all missing patches.

We remain at the forefront of security innovation to provide even more functionality and ease-of-use to customers through services such as Amazon GuardDuty, which is a threat detection service that continuously monitors for malicious or unauthorized behavior, and Amazon Macie, which uses machine learning to automatically discover, classify, and protect sensitive data in AWS. To provide a centralized, comprehensive view, AWS Security Hub aggregates, organizes, and prioritizes security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions. Customers' findings are visually summarized on integrated dashboards with actionable graphs and tables. Customers can also continuously monitor their environments using automated compliance checks based on the AWS best practices and industry standards that their organizations follow.

For small- and medium-sized financial institutions, AWS's security and compliance services give them the chance to operate IT environments with the level of scale and state-of-the-art technology traditionally available only to the largest financial institutions. And for the largest financial institutions, AWS's security and compliance services help simplify, protect, and transform complex, legacy infrastructure, and to achieve equal or better levels of assurance with a smaller amount of effort.

Cloud Security Topics

AWS engages continuously with finance ministries, central banks, regulatory agencies, and standard-setting bodies around the world to inform these authorities about AWS's approach to cybersecurity, as well as understand regulators' expectations for their regulated entities' secure and compliant use of cloud services. Based on that continuous engagement, the following sections of this paper cover five topics that financial services policymakers and regulators have expressed interest in:
(1) hypervisor security, (2) isolating customer instances, (3) encryption, (4) supply chain management, and (5) change management.

Hypervisor Security

We conceive, design, and build our global cloud infrastructure with multiple layers of controls and defenses at every level, starting at the level of silicon to build a trusted compute base. We are at the forefront of technological advances to improve operational performance while maintaining a high bar for security in the computing environment in which our customers operate. For example, consider the host architecture for Amazon EC2. We have a purpose-built hypervisor, which allocates Central Processing Unit (CPU) resources for each instance and is designed to protect the security of customer data even from operators of production infrastructure. We have innovated rapidly over the last few years to increase performance and reduce surface area of our hypervisor. AWS has a significantly customized hypervisor with a code base focused only on the necessary functionality that we and our customers require with encryption, segmentation, and isolation to enable separation between any given virtual machine and the hypervisor. What we call the “Nitro hypervisor” is designed to be *quiescent*: the hypervisor does not execute unless it is doing work on behalf of an instance that the instance requested.[3] Internal and external penetration testers assess the hypervisor regularly for new and existing vulnerabilities and attack vectors. Independent third-party audits also validate our hypervisor security during assessments and audits.

Isolating Customer Instances

AWS has millions of active customers of all types and sizes operating in our global cloud infrastructure. Our core competency as a cloud provider is to protect and isolate the workloads that customers run from each other. One of the ways we allow customers to control their AWS environments, separate from another customer’s environment, is through Amazon Virtual Private Cloud (VPC).

Amazon VPC enables the creation of a logically separate network enclave within the AWS EC2 network that can house compute and storage resources. Customers can connect to Amazon VPC through a virtual private network (VPN) connection over the Internet, or through AWS Direct Connect, a service that provides private network connectivity into the AWS Cloud. The customer controls the private environment, including IP addresses, subnets, network access control lists, security groups, operating system firewalls, route tables, VPNs, and/or Internet gateways.

Amazon VPC provides robust logical isolation of all customer resources. For example, every packet flow on the network is individually authorized to validate the correct source and destination before it is transmitted and delivered. It is not possible for information to pass between multiple tenants without specifically being authorized by both the

transmitting and receiving customers. If a packet is being routed to a destination without a rule that matches it, the packet is dropped.

In addition to providing highly secure, logically isolated, multi-tenant compute services, AWS also provides three means of deploying compute to dedicated hardware using Dedicated Instances, Dedicated Hosts, and Bare Metal instances that customers may consider based on their requirements.

Encryption

For customers that are storing data on AWS storage services or transiting on our networks, we strongly recommend encryption for data-at-rest and in-transit. Encryption and data access control features are built into foundational service offerings such as Amazon Simple Storage Service (Amazon S3), a highly scalable object storage service, Amazon Elastic Block Store (Amazon EBS), which provides network-attached storage to EC2 instances, and Amazon RDS, which provides managed database engines. These features are turn-key and provide documentation to help customers understand how their data is being protected and the configuration options they can control to customize who can access the systems and the keys required to decrypt data residing on them.

AWS Key Management Service (KMS) is a fully managed, highly available regionally isolated service. The multi-tenant hardware security modules (HSMs) used in the standard KMS key store are validated by a third-party laboratory under the FIPS 140-2 standard at level 2 with level 3 in multiple categories. Customers can also choose to have their keys generated and stored in level 3 overall validated single-tenant custom key stores directly under their control by using AWS CloudHSM behind the KMS front-end APIs. AWS KMS can handle hundreds of thousands of API requests per second from customers' applications to meet customers' scaling needs. It gives customers the ability to perform key management and cryptographic functions in a way that is deeply integrated with other AWS services.

With encryption, the confidentiality of the customer's cryptographic keys is crucial. Security depends upon where the data was encrypted and who has access to and is protecting the keys. If the data is encrypted by the customer prior to being ingested into the cloud, there is no ability for the cloud service provider to access the keys or decrypt the data—the customer has full control and responsibility. On the other hand, if a particular cloud service needs to decrypt the data in order to deliver its value, then both the cloud service and the data owner are able to access the keys. Customers need assurance that the cloud provider only has access to decrypt data when the customer

allows it. AWS KMS is designed so that no one, including AWS employees, can retrieve customer plaintext keys and use them outside the service. The FIPS 140-2 validated HSMs in KMS protect the confidentiality and integrity of customer keys regardless of whether customers request KMS to create keys on their behalf, they import them into the service, or used custom key stores via AWS CloudHSM. Customer plaintext keys are never written to disk and only ever used in volatile memory of the HSMs for the time needed to perform the customer's requested cryptographic operation. KMS keys are never transmitted outside of the AWS Regions in which they were created. Updates to the KMS HSM firmware is controlled by quorum-based access control that is audited and reviewed by an independent group within Amazon. This tightly controlled software development lifecycle process minimizes the risk that the security properties of the service will be changed as new software, firmware, or hardware is introduced.

Customers may also use another service, AWS CloudHSM, which provides a dedicated, FIPS 140-2 Level 3 (overall) HSM under a customer's exclusive control, directly in the customer's Amazon VPC. The CloudHSM service provides automated availability, replication, and backup of the dedicated, single-customer HSMs across availability zones. It integrates into customer-owned applications using industry-standard crypto APIs. It also integrates with AWS services via the KMS custom key store feature. Both KMS and CloudHSM services work to ensure that the encryption algorithm is sufficiently robust to render data unintelligible and the keys sufficiently protected so the ciphertext will be unreadable by unauthorized persons. In other words, the storage of appropriately encrypted data with properly managed and secured keys can provide assurance of fully protected data.

Protecting Our Supply Chain

At Amazon, we employ stringent security standards across our supply chain. We investigate all hardware and software prior to going into production and performing regular security audits internally and with our supply chain partners. We further strengthen our security posture by implementing our own hardware designs for critical components such as processors, servers, storage systems, and networking equipment.

We test new hardware and software extensively before we deploy them, in a managed and phased process, in the AWS Cloud. Prior to use, we inspect or verify that incoming equipment, software, and supplies, including AWS created software code, to be used in the AWS production environment conform to established requirements. We "burn in" all components, re-image incoming servers with known-good firmware and system software, and observe them in a pre-production environment to make sure that the components and systems meet specifications and are functioning as expected. We

perform final inspection and testing on AWS services prior to their release to general availability. The final service release review procedure includes verification that all specifications were met. Once in production, we continuously monitor AWS services' quality metrics.

Rigorous Change Management

To operate at the global scale that we do, we employ controlled automation in a secure change management process. The goal of AWS's change management process is to prevent unintended service disruptions and maintain the integrity of services to the customer. We endeavor to automate as much of our change management processes as possible and maintain back-up runbooks as needed. We maintain documented change management processes, including peer review of code changes, automated checks, and security scans, with the goal of providing developers feedback as soon as possible. We develop changes in a development environment that is segregated from the production environment. Customer content is not used in test and development environments. We test and confirm that the changes will behave as expected when applied and not adversely impact performance, for example, through build and unit tests, integration tests, load tests, and testing for dependencies. Authorized team members approve all changes to provide appropriate oversight and understanding of business impact.

We typically push changes into production in a phased deployment starting with lowest impact sites, and we closely monitor deployments so that we can evaluate impact. Service owners have a number of configurable metrics that measure the health of the service's upstream dependencies. These metrics are closely monitored with thresholds and alarming in place (e.g., latency, availability, fatals, CPU utilization, etc.). Through our "pessimistic" deployment process, if an issue is identified, the change can be rolled back and the last known good version is deployed. Rollback procedures are documented so that team members can revert back to the previous state if needed. When possible, we schedule changes during regular change windows. Emergency changes to production systems that require deviations from standard change management procedures are associated with an incident and are logged and approved as appropriate. We maintain processes to constantly monitor for and detect unauthorized changes made to the production environment and quickly roll back and remediate identified issues.

Financial Services Regulatory Landscape in Cybersecurity

While AWS serves millions of active customers across virtually every segment, we recognize that our customers in regulated industries face specific requirements and expectations with which they need to align and comply. In the financial services industry, individual entities develop their cybersecurity posture not only to address the threat and vulnerability environment in which they operate, but also in accordance with their regulatory environment. Over the last few years, the global regulatory environment in financial services specifically related to cybersecurity has evolved. Across the constellation of international financial regulatory bodies, cross-border coordination on financial sector cybersecurity varies from collaboration on definition of cybersecurity terms and general monitoring of cyber risks to active policy development and standard-setting. The purpose of this section is to highlight the distinct contributions to financial services cybersecurity policy made by international and national-level regulatory bodies—and how customers can internalize these regulatory developments in their cloud adoption process.

Given the diversity of its membership from the Group of 20 (G-20) countries, the Financial Stability Board (FSB) has focused its work to date on increasing understanding of the prevailing cybersecurity regulatory and supervisory practices in member jurisdictions. To that end, the FSB published the *Cyber Lexicon* in October 2018 as a non-binding tool for financial sector authorities to apply in several efforts, such as building common understanding of relevant terminology, supporting the FSB's work on monitoring financial stability risks, and facilitating appropriate information sharing.[4]

Other international bodies have begun to develop guidance documents. For example, the G-7 Cyber Expert Group, composed of leading finance ministries, central banks, and supervisory authorities, has established non-binding guidance and expectations on cybersecurity practices for both firms and public authorities in the following domains: (1) Cybersecurity Strategy and Framework, (2) Governance, (3) Risk and Control Assessment, (4) Monitoring, (5) Response, (6) Recovery, (7) Information Sharing, and (8) Continuous Learning.[5] The G-7 Cyber Expert Group has issued additional guidance on effective assessment, third-party cyber risk management, and threat-led penetration testing.

Specific international financial sector standard-setting bodies have also issued guidance for regulated entities under their purview. For payments, clearing, and settlement

entities, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) issued guidance in June 2016[6] that directs financial market infrastructures to implement governance arrangements and controls to improve their cyber resilience—in particular, to "enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios."[7]

For international banks, the Basel Committee on Banking Supervision published a descriptive report on cyber resilience practices across jurisdictions that reflects supervisory concerns, including: (1) global banks should focus on secure design and resilience based on current threats rather than only seeking to meet compliance obligations; (2) boards of directors need to oversee cyber risk tolerance; and (3) there is no standard set of cyber resilience metrics within the banking sector.[8] At the time of writing, for insurance companies, the International Association of Insurance Supervisors (IAIS) is working on guidance based on the G-7 *Fundamental Elements of Cybersecurity* as a framework to provide recommendations on supervision of cybersecurity at insurers.[9]

In parallel, at the domestic level, major regulatory agencies have published guidance for financial institutions to identify cybersecurity risks and enhance their security posture. For example, in June 2015, the U.S. Federal Financial Institutions Examination Council (FFIEC) published the Cybersecurity Assessment Tool (CAT),[10] which allows financial institutions to determine their inherent cyber risks and cybersecurity maturity level; the U.S. Office of the Comptroller of the Currency (OCC) has also utilized the CAT in the course of examining regulated entities' cybersecurity programs. Several regulators in other regions of the world have also issued cybersecurity guidance. For example, the Central Bank of Brazil (BCB) issued Resolution No. 4,658 of April 26, 2018, which requires regulated financial institutions to adopt a cybersecurity policy that addresses a wide range of issues, including the use of service providers for data processing, data storage, and cloud computing.[11] In September 2018, the Monetary Authority of Singapore (MAS) issued a public consultation for a Notice on Cyber Hygiene to prescribe essential cybersecurity practices that financial institutions need to put in place.[12] With these and other regulatory agencies, AWS provides insight and expertise to inform policy development.

Other frameworks focus on financial services firms' cyber resilience testing. For example, in May 2014, the Bank of England launched CBEST, which provides a framework for firm-specific, threat intelligence-led penetration testing as a means of determining a financial firm's ability to secure its critical functions.[13] Similar to CBEST,

the European Central Bank (ECB) published the European framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) in May 2018 both for implementation in individual EU Member States and to encourage cross-border cooperation on red-team testing.[14] To address concerns that malicious actors may access critical functions or processes in customers' environments, customers can conduct vulnerability and penetration testing of their own AWS environments.[15]

Finally, although the financial services regulatory landscape in cybersecurity is composed of dozens of different laws, regulations, and guidance documents,[16] most regulatory and supervisory frameworks leverage already developed national and international standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), ISO 27000 series, and CPMI-IOSCO guidance.[17] Nonetheless, regulated financial institution customers need to consider their jurisdiction-specific regulatory requirements and obligations related to cybersecurity—and depending on their needs, map those often overlapping requirements and obligations to their own control environments. Given the substantively similar regulatory and supervisory requirements across jurisdictions, the Financial Services Coordinating Council (FSCC) developed the *Financial Services Sector Cybersecurity Profile*, based on the NIST CSF, to serve as both a baseline internal examination assessment and an external evaluation of partners, vendors, and third-party service providers.[18] AWS also aligns with the NIST CSF. Developed originally to apply to critical infrastructure entities, the foundational set of security disciplines in the CSF can apply to any organization in any sector, regardless of size. AWS's alignment with the CSF, validated by a third-party auditor, reflects the suitability of AWS services to enhance the security and resiliency of financial sector entities.

Path to Production

Now that we have discussed the shared responsibility model, topics in cloud security, and the financial services regulatory landscape in cybersecurity, how does a financial services customer use AWS services to become more secure and resilient? Our best practices recommend that financial institutions have a comprehensive understanding of the benefits and risks of using the cloud, develop appropriate risk management and governance policies, and design for secure and resilient deployment of their applications. We have enumerated best practices for financial institutions to follow before deploying an application in AWS into ten steps called the "Path to Production."

1. ***Identify and Engage Stakeholders:*** Early engagement with Security and Risk and Compliance teams in the financial institution is important for an effective path to production. Often, these teams are separate from other teams responsible for cloud delivery and have different functions (e.g., reduce material risk to the institution). Through our engagements with customers, we often witness two distinct sets of stakeholders; one set composed of Security teams reporting to the Chief Information Security Officer (CISO) and another set composed of Risk and Compliance teams (often in the first or second "line of defense").
2. ***Capability and Enablement:*** We encourage Security and Risk and Compliance teams at the financial institution to familiarize themselves with the AWS shared responsibility model, cloud security benefits, and the AWS security services that can enhance their security posture. The AWS Cloud Adoption Framework – Security Perspective helps customers get started across four main components of the framework: Directive, Preventive, Detective, and Responsive controls. Regular security immersion days, training (e.g., AWS Security Fundamentals, AWS Security Engineering), and certifications (e.g., AWS Certified Security – Specialty) are important ways to help train and enable Security and Risk and Compliance teams.
3. ***Operating Model:*** When developing their operating model for cloud delivery, financial institutions can consider incorporating their Security and Risk and Compliance teams. The customer's Security and Risk and Compliance teams can feed in their requirements to the platforms or standards adopted by the cloud delivery teams through a documented and published methodology. The customer's Security team can review its AWS workloads and architecture at the design stage, while the Technology Risk team can review and approve the workloads prior to deployment to validate that security, compliance, and regulatory controls are in place.
4. ***Security of the Cloud:*** We encourage a wide range of stakeholders within financial institutions to understand the shared responsibility model and the way AWS operates its compliance programs. Inside the financial institution, first-, second-, and third-line risk management functions can consider the AWS controls relevant to their institution's deployment. The relevant teams can access and review AWS compliance reports, such as our SOC 2 report, available on AWS Artifact. Through mechanisms such as an annual vendor risk management process, financial institutions can track their vendor risk assessments and have a forward-looking view of all of their future such assessments.

5. ***Security in the Cloud:*** Financial institutions can use AWS services to automate security processes, improve visibility of their security and control environment, and enable near-real time continuous compliance across domains such as identity, logging and monitoring, data protection, and incident response. We encourage financial institutions to develop, review, and approve application, data, and resiliency classification processes, as well cloud security standards and policies. Customers can also establish a process for reviewing AWS services and approving them for internal use, as well as an approval process for moving confidential or personally identifiable information (PII) data to AWS.
6. ***Regulatory requirements:*** Financial institutions' production workloads may be subject to applicable regulatory requirements, such as those frameworks and standards described in the previous section. Mapping regulatory obligations to common controls and establishing mechanisms to demonstrate compliance are critical steps in adopting cloud services. Customers should also consider whether they need to notify or seek approval from their regulators prior to production, for example, if they are using cloud services for "critical or important" functions.
7. ***Agreements:*** Legal, procurement, and outsourcing teams within financial institutions can also familiarize themselves with the shared responsibility model and cloud services, as using the cloud can be different from the ways that financial institutions traditionally procure and consume hardware and software. Customers may also need to verify that they have the appropriate agreements in place prior to production.
8. ***Establish Security Controls:*** Once financial institutions have identified their security control requirements (per items 4-6 above), they can then build them in to automated, scalable architectures. AWS Landing Zones, automatic provisioning, continuous compliance,[19] and AWS Well-Architected are important components of this build phase.

9. ***Internal & External Assessment:*** Before deploying production workloads, customers may need to design and/or go through an existing production sign-off, operational readiness, or permit process. Control owners in the first line of defense, risk management teams in the second line, and audit functions in the third line may need to perform assessments, in addition to external third parties; these assessment activities include security assessments of the customer's platform and workloads, reviewing the cloud security strategy with internal or external audit functions, and penetration testing of customer resources. Finally, depending on the materiality of cloud usage, a comprehensive risk assessment of the financial institution's cloud strategy and security controls followed by presentation to the board of directors for approval may be necessary.
10. ***Regulatory Approval or Notification:*** Depending on the jurisdiction, financial institutions may need to notify or seek approval from their regulator before using cloud services for regulated workloads. Preparing for regulatory engagement may involve specific due diligence and risk assessment activity mandated by applicable requirements, such as recording AWS usage in the institution's outsourcing register. AWS can assist customers with preparing for regulatory engagement, notification, and approval.

AWS solution architects and security and compliance experts help our financial services customers with answering questions about AWS's security and control environment and providing best practices on how customers should secure their systems and data on the AWS Cloud. Our teams provide this guidance based on the wide variety of internal control frameworks that financial institution customers utilize for their deployments on AWS.

Conclusion

Financial institutions are improving their customers' digital experiences, preventing fraud, managing records, running core banking systems, and imagining the next generation of financial services on the AWS Cloud. We're amazed by what our customers are doing, and they help drive us every day to raise the bar on our security and operational performance. Security is a shared responsibility between us and our customers, and we know that there are common security topics that interest customers and regulators, including: hypervisor security, isolating customer instances, encryption, supply chain management, and change management. At the same time, policymakers are shaping the financial services regulatory environment for cybersecurity risk management at financial services entities. In light of that "big picture"—what security in and of the cloud means, what the regulatory environment looks like—individual financial

institutions can approach their path to production on the AWS Cloud in a strategic and rigorous way that embeds security and compliance considerations from the start. We have observed that customers who approach their path to production in a strategic manner accelerate adoption, scale their businesses, and maintain a strong security posture—benefitting not only their individual organizations, but also the security, stability, and prosperity of our financial system and economy.

Contributors

Contributors to this document include:

- Rahul Prabhakar, Global Financial Services, AWS Security Assurance
- Mark Ryland, Director, Office of the CISO, AWS Security
- Bill Shinn, Sr. Principal, Office of the CISO, AWS Security
- Jaswinder Hayre, Sr. Manager, AWS FSI Solutions Architecture
- Ilya Epshteyn, Principal Solutions Architect, AWS FSI Solutions Architecture

Document Revisions

Date	Description
July 2019	First publication

Notes

[1] E.g., Amazon Relational Database Service (RDS), Amazon Redshift, AWS Directory Service, and AWS Web Application Firewall.

[2] See *Remarks by Deputy Secretary Sarah Bloom Raskin at the American Bankers Association Summer Leadership Meeting*, July 14, 2015, available at https://www.treasury.gov/press-center/press-releases/Pages/jl0112.aspx.

[3] For more on the Nitro System, see "AWS re:Invent 2018: Powering Next-Gen EC2 Instances: Deep Dive into the Nitro System," https://www.youtube.com/watch?v=e8DVmwj3OEs.

[4] FSB, *Cyber Lexicon*, November 12, 2018, available at http://www.fsb.org/wp-content/uploads/P121118-1.pdf. See also FSB, *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices*, October 13, 2017, available at http://www.fsb.org/wp-content/uploads/P131017-1.pdf.

[5] G-7 Cyber Expert Group, *Fundamental Elements of Cybersecurity for the Financial Sector*, October 2016, available at https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf.

[6] CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, June 2016, available at https://www.bis.org/cpmi/publ/d146.pdf.

[7] *Ibid.,* p. 16.

[8] The report is framed as a "first assessment of observed cyber-resilience practices at authorities and firms" and does not direct national authorities to implement specific standards. Basel Committee on Banking Supervision, *Cyber-resilience: Range of practices*, December 2018, available at https://www.bis.org/bcbs/publ/d454.pdf.

[9] IAIS, Public Consultation: Application Paper on Supervision of Insurer Cybersecurity, June 29, 2018, available at https://www.iaisweb.org/page/consultations/closed-consultations/2018/application-paper-on-cyber-security/.

[10] FFIEC, *Cybersecurity Assessment Tool*, May 2017, available at https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf.

[11] Banco Central do Brasil, *Resolution CMN 4,658 of April 26, 2018*, available at https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf.

[12] Monetary Authority of Singapore, *Notice on Cyber Hygiene*, Consultation Paper P014-2018, September 2018, available at http://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Consultation%20Papers/Consultation%20Paper%20on%20Notice%20on%20Cyber%20Hygiene.pdf.

[13] Bank of England, *CBEST Intelligence-Led Testing: CBEST Implementation Guide*, Version 2.0, 2016, available at: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf.

[14] ECB, *TIBER-EU Framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*, May 2018, available at https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.

[15] Financial institution customers subject to the CBEST or similar framework and planning to have a penetration test conducted on their AWS resources should visit https://aws.amazon.com/security/penetration-testing/.

[16] See, for example, the Regulatory Digest maintained by the World Bank, available here: https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision.

[17] See p. 5 of Basel Committee on Banking Supervision, *Cyber-resilience: Range of practices*, December 2018, available at https://www.bis.org/bcbs/publ/d454.pdf and p. 3 of FSB, *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices*, October 13, 2017, available at http://www.fsb.org/wp-content/uploads/P131017-1.pdf.

[18] Financial Services Sector Coordinating Council, *Financial Services Sector Cybersecurity Profile*, available at https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile.

[19] See, for example, *Continuous Compliance on AWS at Scale*, AWS re:Invent 2017, available at https://www.youtube.com/watch?v=h4eClhXPvoc.