Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond

March 2019

[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

Introduction

Amazon Web Services (AWS) provides information technology (IT) services and building blocks that all types of businesses, public authorities, universities, and individuals utilize to become more secure, innovative, and responsive to their own needs and the needs of their customers. AWS offers IT services in categories ranging from compute, storage, database, and networking to artificial intelligence and machine learning. AWS standardizes its services and makes them available to all customers, including financial institutions. Across the world, financial institutions have used AWS services to build their own applications for mobile banking, regulatory reporting and market analysis.

The purpose of this paper is to describe how AWS and our customers in the financial services industry achieve operational resilience using AWS services. The primary audience of this paper is organizations with an interest in how AWS and our financial services customers can operate services in the face of constant change, ranging from minor weather events to cyber issues. AWS and the financial services industry share a common interest in maintaining operational resilience, i.e., the ability to provide continuous service despite disruption. Continuity of service, especially for critical economic functions, is a key prerequisite for financial stability. AWS recognizes that financial institutions, which use AWS services, need to comply with sector-specific regulatory obligations and internal requirements regarding operational resilience. These obligations and requirements are found, inter alia, in IT guidelines[1] and cyber resilience guidance.[2] Financial institution customers are able to rely on AWS to provide resilient infrastructure and services, while at the same time designing their applications in a manner that meets regulatory and compliance obligations. This dual approach to operational resilience is something that we call “shared responsibility.”

What does operational resilience mean at AWS?

Operational resilience is the ability to provide continuous service through people, processes, and technology that are aware of and adaptive to constant change. It is a real-time, execution-oriented norm embedded in the culture of AWS that is distinct from traditional approaches in Business Continuity, Disaster Recovery, and Crisis Management, which rely primarily on centralized, hierarchical programs focused on documentation development and maintenance.

Operational Resilience is a Shared Responsibility

AWS is responsible for ensuring that the services used by our customers—the building blocks for their applications—are continuously available, as well as ensuring that we are prepared to handle a wide range of events that could affect our infrastructure.

In this paper, we also explore customers’ responsibility for operational resilience—how customers can design, deploy, and test their applications on AWS to achieve the availability and resiliency they need, including for

[1] E.g., U.S. Federal Financial Institution Examination Council (FFIEC) IT Handbook; see https://ithandbook.ffiec.gov.

[2] E.g., Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions (CPMI-IOSCO), *Guidance on cyber resilience for financial market infrastructures* (June 2016); see https://www.bis.org/cpmi/publ/d146.pdf.

mission-critical applications that require almost no downtime. Those kinds of applications require that AWS infrastructure and services are available when customers need them even upon the occurrence of a disruption. As discussed below, customers are able to use AWS's services to design applications that meet this standard and provide a level of security and resilience that we consider is greater than what existing on-premises IT environments can offer.

Finally, given the importance of operational resilience to our customers, we also explore the variety of mechanisms AWS offers to customers to demonstrate assurance.[3]

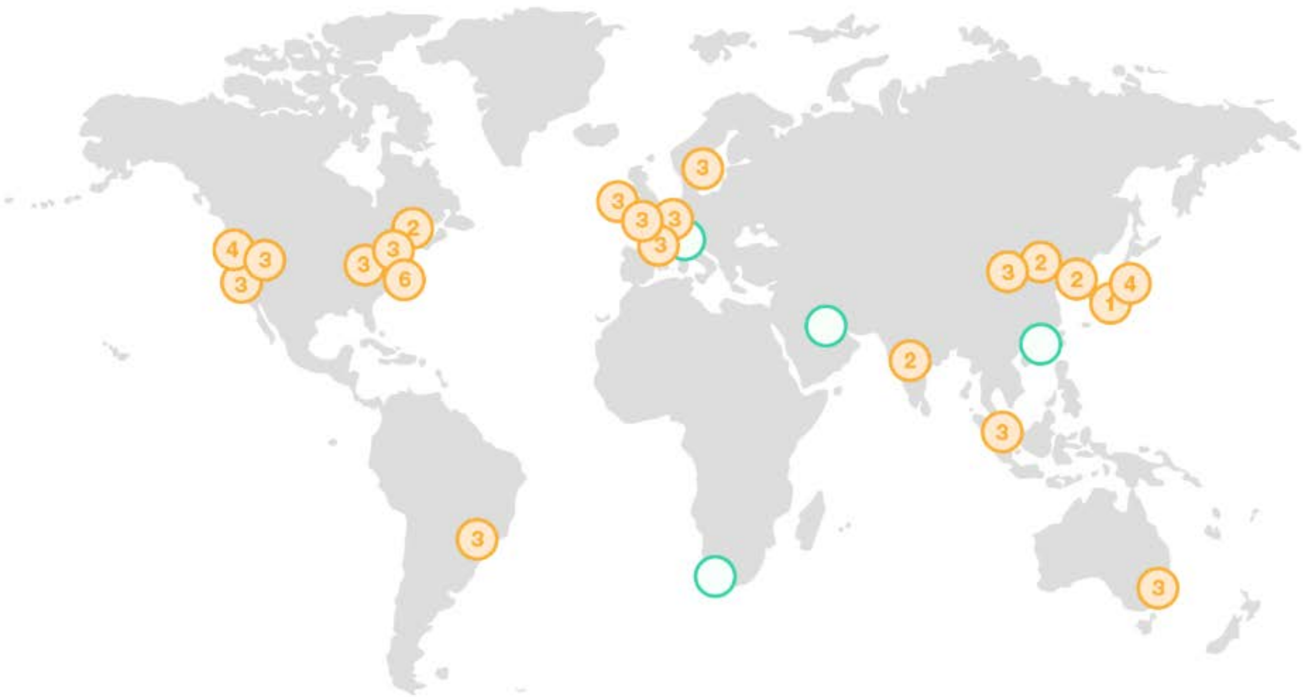
How AWS Maintains Operational Resilience and Continuity of Service

AWS builds to guard against outages and incidents, and accounts for them in the design of AWS's services—so when disruptions do occur, their impact on customers and the continuity of services is as minimal as possible. To avoid single points of failure, AWS minimizes interconnectedness within our global infrastructure. AWS's global infrastructure is geographically dispersed over five continents. It is composed of *20 geographic Regions, which are composed of 61 Availability Zones (AZs), which, in turn, are composed of data centers* (Figure 1).[4] The AZs, which are physically separated and independent from each other, are also built with highly redundant networking to withstand local disruptions. Regions are isolated from each other, meaning that a disruption in one Region does not result in contagion in other Regions. Compared to global financial institutions' on-premises environments today, the locational diversity of AWS's infrastructure greatly reduces geographic concentration risk. We are continuously adding new Regions and AZs, and you can view our most current global infrastructure map here: https://aws.amazon.com/about-aws/global-infrastructure.

At AWS, we employ compartmentalization throughout our infrastructure and services. We have multiple constructs that provide different levels of independent, redundant components. Starting at a high level, consider our AWS Regions. To minimize interconnectedness, AWS deploys a dedicated stack of infrastructure and services to each Region. Regions are autonomous and isolated from each other, even though we allow customers to replicate data and perform other operations across Regions. To allow these cross-Region capabilities, AWS takes enormous care to ensure that the dependencies and calling patterns between Regions are asynchronous and ring-fenced with safety mechanisms. For example, we have designed Amazon Simple Storage Service (Amazon S3) to allow customers to replicate data from one Region (e.g., US-EAST-1) to another Region (e.g., US-WEST-1), but at the same time, we have designed S3 to operate autonomously within each Region, so that an outage

[3] Please note: this paper reflects only an overview of our ongoing efforts to ensure our customers can use AWS services safely. To complement our concept of shared responsibility, we are also dedicated to exceeding customer and regulatory expectations. To that end, AWS technical teams, security architects, and compliance experts assist financial institutions customers in meeting regulatory and internal requirements, including by actively demonstrating their security and resiliency through continuous monitoring, remediation, and testing. AWS continuously engages with financial regulators around the world to explain how AWS's infrastructure and services enable all sizes and types of financial institutions—from fintech start-ups to stock exchanges—to improve their security and resiliency compared to on-premises environments. We always want to receive feedback from customers and their regulators about AWS's approach and their experience.

[4] You can take a virtual tour of an AWS data center here: https://aws.amazon.com/compliance/data-center.



# **Region & Number of Availability Zones**

US East
N. Virginia (6),
Ohio (3)

US West
N. California (3),
Oregon (4)

Asia Pacific
Mumbai (2),
Seoul (2),
Singapore (3),
Sydney (3),
Tokyo (4),
Osaka-Local (1)[1]

Canada
Central (2)

China
Beijing (2),
Ningxia (3)

Europe
Frankfurt (3),
Ireland (3),
London (3),
Paris (3),
Stockholm (3)

South America
São Paulo (3)

GovCloud (US)
US-East (3),
US-West (3)

○ **New Region (coming soon)**

Bahrain

Cape Town

Hong Kong SAR

Milan

Figure 1. AWS Global Infrastructure

of S3 in US-EAST does not result in an S3 outage in US-WEST.[5] The vast majority of services operate entirely within single Regions. The very few exceptions to this approach involve services that provide global delivery, such as Amazon Route 53 (an authoritative Domain Name System), whose data plane is designed for 100.000% availability. As discussed below, financial institutions and other customers can architect across both multiple Availability Zones and Regions.

Availability Zones (AZs), which comprise a Region and are composed of multiple data centers, demonstrate further compartmentalization. Locating AZs within the same Region allows for data replication that provides redundancy without a substantial impact on latency—an important benefit for financial institutions and other customers who need low latency to run applications. At the same time, we make sure that AZs are independent in order to ensure services remain available in the event of major incidents. AZs have independent physical infrastructure and are distant from each other to mitigate the effects of fires, floods, and other events. Many AWS services run autonomously within AZs; this means that if one AZ within a single Region loses power or connectivity, the other AZs in the Region are unaffected, or in the case of a software error, the risk of that error propagating is limited. AZ independence allows AWS to build Regional services using multiple AZs that, in turn, provide high availability to and resiliency for our customers.

In addition, AWS leverages another concept known as cell-based architecture. Cells are multiple instantiations of a service that are isolated from each other; these internal service structures are invisible to customers. In a cell-based architecture, resources and requests are partitioned into cells, which are capped in size. This design minimizes the chance that a disruption in one cell—for example, one subset of customers—would disrupt other cells. By reducing the blast radius of a given failure within a service based on cells, overall availability increases and continuity of service remains. A rough analogy is a set of watertight bulkheads on a ship: enough bulkheads, appropriately designed, can contain water in case the ship's hull is breached and will allow the ship to remain afloat.

Incident Management

Although the likelihood of such incidents is very low, AWS is prepared to manage large-scale events that affect our infrastructure and services. AWS becomes aware of incidents or degradations in service based on continuous monitoring through metrics and alarms, high-severity tickets, customer reports, and the 24x7x365 service and technical support hotlines. In case of a significant event, an on-call engineer convenes a call with problem resolvers to analyze the event to determine if additional resolvers should be engaged. A call leader drives the group of resolvers to find the approximate root cause to mitigate the event. The relevant resolvers will perform the necessary actions to address the event. After addressing troubleshooting, repair procedures, and affected components, the call leader will assign follow-up documentation and actions and end the call engagement. The call leader will declare the recovery phase complete after the relevant fix activities have been addressed. The post mortem and deep root cause analysis of the incident will be assigned to the relevant team. Post-mortems

[5] As evidenced by the Amazon S3 service disruption of February 28, 2017, which occurred in the Northern Virginia (US-EAST-1) Region, but not in other Regions. See "Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region," https://aws.amazon.com/message/41926.

are convened after any significant operational issue, regardless of external impact, and Correction of Errors (COE) documents are composed such that the root cause is captured and preventative actions may be taken for the future. Implementation of the preventative measures is tracked during weekly operations meetings.

Customers Can Achieve and Test Resiliency on AWS

AWS believes that financial institutions should ensure that they—and the critical economic functions they perform—are resilient to disruption and failure, whatever the cause. Prolonged outages or outright failures could cause loss of trust and confidence in affected financial institutions, in addition to causing direct financial losses due to failing to meet obligations.

AWS builds—and encourages its customers to build—for failure to occur, at any time. Similarly, as the Bank of England recognizes, "We want firms to plan on the assumption that any part of their infrastructure could be impacted, whatever the reason."[6] In the design, building, and testing of their applications on AWS, customers are able to achieve their objectives for operational resilience. AWS offers the building blocks for any type of customer, from financial institutions to oil and gas companies to government agencies, to construct applications that can withstand large-scale events. In this section, we walk through how financial institution customers can build that type of resilient application on the AWS cloud.

Starting with First Principles

AWS field teams, composed of technical managers, solution architects, and security experts, help financial institution customers build their applications according to customers' design goals, security objectives, and other internal and regulatory requirements. As reflected in our shared responsibility model, customers remain responsible for deciding how to protect their data and systems in the AWS cloud, but we offer workbooks, guidance documents, and on-site consulting to assist in the process. Before deploying a mission-critical application—whether on the AWS cloud or in another environment—significant financial institution customers will go through extensive development and testing. For a customer who begins building an application on AWS with high availability and resiliency in mind, we recommend that they begin by answering some fundamental questions,[7] including but not limited to:

1. What problems are you trying to solve?
2. What specific aspects of the application require specific levels of availability?
3. What is the amount of cumulative downtime that this workload can realistically accumulate in one year?
4. What is the actual impact of unavailability?

[6] Charlotte Gerken, "The Bank of England's approach to operational resilience," (13 June 2017), accessible at https://www.bankofengland.co.uk/-/media/boe/files/speech/2017/the-boes-approach-to-operational-resilience.pdf.

[7] We recommend that customers review the Cloud Adoption Framework to develop efficient and effective adoption plans. See "Application Design for High Availability" on determining availability needs in the AWS Reliability Pillar whitepaper: https://d1.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf.

Financial institutions and market utilities perform both critical and non-critical types of functions in the financial services sector. From deposit-taking to loan-processing, trade execution to securities settlement, financial entities across the world perform services whose continuity and resiliency are necessary to ensure the public's trust and confidence in the financial system. At the industrywide level, for systemically important payment, clearing, settlement, and other types of applications, central banks and market regulators specify a discrete recovery time objective in the Principles for Financial Market Infrastructures (PFMI) standard: "The [business continuity] plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances."[8]

Beyond the 2-hour RTO, financial regulatory agencies expect regulated entities to be able to meet RTOs and recovery point objectives (RPOs) according to the criticality of their applications, beginning with "Tier 1 application" as the most critical. For example, regulated entities may classify their RTO and RPOs in the following way:

Resiliency requirement	Tier 1 app	Tier 2 app	Tier 3 app
Recovery Time Objective	2 Hours	< 8 Hours	24 Hours
Recovery Point Objective	< 30 seconds	< 4 Hours	24 Hours

Although systemically important financial institutions may have upwards of 8,000 to 10,000 applications, they do not classify all applications according to the same criticality. For example, disruptions in an application for processing mortgage loan requests are undesirable, but a financial institution operating such an application may decide that it can tolerate an 8-hour RTO. Other types of important, but not necessarily *systemically* important, workloads include post-trade market analysis and customer-facing chatbots.

While the majority of financial entities' applications are non-critical from a systemic perspective, disruption of some Tier 1 applications would jeopardize not only the safety and soundness of the affected financial institution, but also other financial services entities and possibly the broader economy. For example, a settlement application may be a Tier 1 application and have an associated RTO of 30 minutes and an RPO of < 30 seconds. Such applications are the heart of financial markets and disruptions could cause operational, liquidity, and even credit risks to crystallize. For such applications, there is little to virtually no time for humans to make an active decision on how to recover from an outage or failover to a backup data center. Recovery would need to be automatic and triggered based on metrics and alarms.[9]

AWS provides guidance to customers on best practices for building highly available, resilient applications, including through our Well-Architected Framework.[10] For example, we recommend that the components comprising an application should be independent and isolated to provide redundancy. When changing

[8] Key Consideration 17.6 of PFMI, available at https://www.bis.org/cpmi/publ/d101a.pdf.

[9] Customers can enable automatic recovery using a variety of AWS services, including Amazon CloudWatch metrics, Amazon CloudWatch Events, and AWS Lambda. See also the following AWS re:Invent presentation, "Disaster Recovery and Business Continuity for Financial Institutions" for additional information on applicable AWS services and example architecture: https://www.youtube.com/watch?v=Xa-xTwhP1UU.

[10] See https://aws.amazon.com/architecture/well-architected.

components or configurations in an application, customers should make sure that they can roll back any changes to the application if it appears that the changes are not working. Monitoring and alarming should be used to track latency, error rates, and availability for each request, for all downstream dependencies, and for key operations. Data gathered through monitoring should allow for efficient diagnosis of problems.[11] Best practices for distributed systems should be implemented to enable automated recovery. Recovery paths should be tested frequently—and most frequently for complex or critical recovery paths.

For financial institutions, it can be difficult to practice these principles in traditional, on-premises environments, many of which reflect decades of consolidation with other entities and ad-hoc changes in their IT infrastructures. On the other hand, these principles are what drive the design of AWS's global infrastructure and services and form the basis of our guidance to customers on how to achieve continuity of service.[12] Financial institutions using AWS services can take advantage of AWS's services to improve their resiliency, regardless of the state of their existing systems.

From Design Principles to Implementation

Customers have to make many decisions: where to place their content, where to run their applications, and how to achieve higher levels of availability and resiliency. For example, a financial institution can choose to run its mobile banking application in a single AWS Region to take advantage of multiple Availability Zones (AZs), as described earlier and shown in Figure 2.

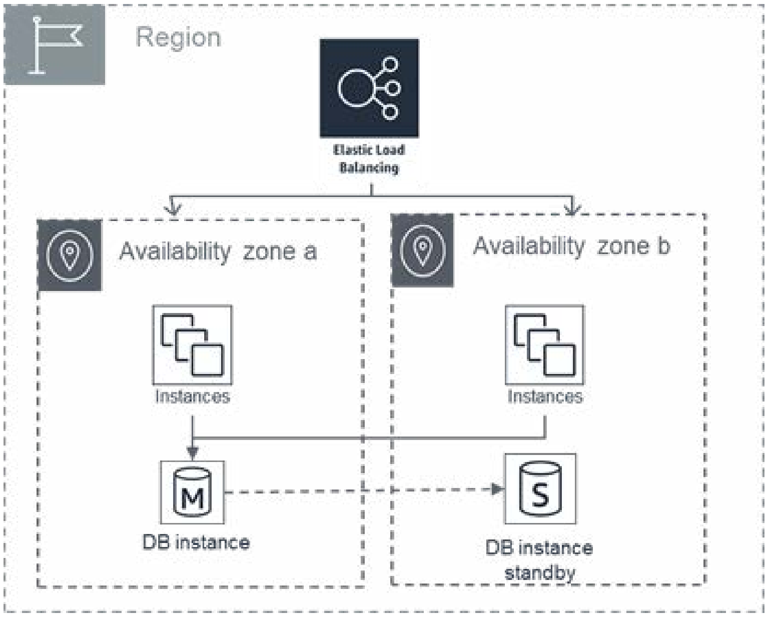


Figure 2. Example of Multi-AZ Design

Let's take the example of a deployment across 2 AZs to illustrate how AZ independence provides resiliency. As shown in Figure 2, the customer deploys its mobile banking application so that its architecture is stable and consistent across AZs, i.e., the workload in each AZ has sufficient capacity as well as stable infrastructure, configurations, and policies that keep both AZs up to date. Elastic Load Balancing routes traffic only to healthy instances and data layer replication allows for fast failover in case a database instance fails in one AZ, thus minimizing downtime for the financial institution's mobile banking customers.

[11] A variety of AWS services support these practices; for examples, see pp. 26-28 at https://d0.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf.

[12] For a comprehensive overview of our guidance to customers, see the "Reliability Pillar" whitepaper (September 2018) at https://d0.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf.

Compared to AWS's infrastructure and services, traditional, on-premises environments present several obstacles for achieving operational resilience. For example, let's assume a significant event shuts down a financial institution's primary, on-premises data center. The financial institution also has a secondary data center in addition to its primary data center. The capacity of the secondary data center is able to handle only a proportion of the overall workload that would otherwise operate at the primary data center (e.g., 11,000 servers at the secondary center instead of 12,000 servers at the primary center; network capacity increased 300% at the primary center in the last 4 years, but only 250% at the secondary center) and errors in replication mean that the secondary center's data has not been updated in 36 hours. Furthermore, macroeconomic factors have driven transaction volume higher at the primary data center by 15% over the past 6 months. As a result, the financial institution may find that its secondary data center cannot process current transaction volume within a given time period per its internal and regulatory requirements.

By using AWS services, the financial institution would have been able to increase its capacity at frequent intervals to support increasing transaction volumes, as well as track and manage changes to maintain all of its deployments with the same, up-to-date capacity and architecture. In addition, customers can maintain additional "cold" infrastructure and backups on AWS that can activate if necessary—at much lower cost than procuring their own physical infrastructure. This is not a hypothetical issue—key regulatory requirements highlight the need for regulated entities to account for capacity needs in adverse scenarios.[13]

On AWS, customers can also deploy workloads across AZs located in multiple Regions (Figure 3) to achieve both AZ redundancy and Region redundancy. Customers that have regulatory or other requirements to store data in multiple Regions or to achieve even greater availability can use a multi-Region design. In a multi-Region set-up, the customer will need to perform additional engineering to minimize data loss and ensure consistent data between Regions. A routing component monitors the health of the customer's application as well as dependencies. This routing layer will also handle automatic failovers, changing the destination when a location is unhealthy and temporarily stopping data replication. Traffic will go only to healthy Regions.

AWS improves operational resilience compared to traditional, on-premises environments not only for failover, but also for returning to full resiliency. For the financial institution with a secondary data center, it may have to perform data backup and restoration over several days. Many traditional environments do not feature bidirectional replication, resulting in current data at the backup site and "outdated" data in the primary site that makes fast failback difficult to achieve. On AWS, the financial institution is not "stuck" as it would be in a traditional environment—it can *fail forward* by quickly launching its workload in another location. The key point is that AWS's global infrastructure and services offer financial institutions the capacity and performance to meet aggressive resiliency objectives.

To achieve assurance about the resiliency of their applications, we recommend that financial institution customers perform continuous performance, load, and failure testing; extensively use logging, metrics, and alarms; maintain

[13] See, for example, U.S. Securities and Exchange Commission (SEC), Regulation Systems Compliance and Integrity, 17 C.F.R. § 240, 242 & 249; see also adopting release: https://www.sec.gov/rules/final/2014/34-73639.pdf. See also FFIEC, Business Continuity Planning, IT Examination Handbook (February 2015), available at https://ithandbook.ffiec.gov/media/274725/ffiec_itbooklet_businesscontinuityplanning.pdf.

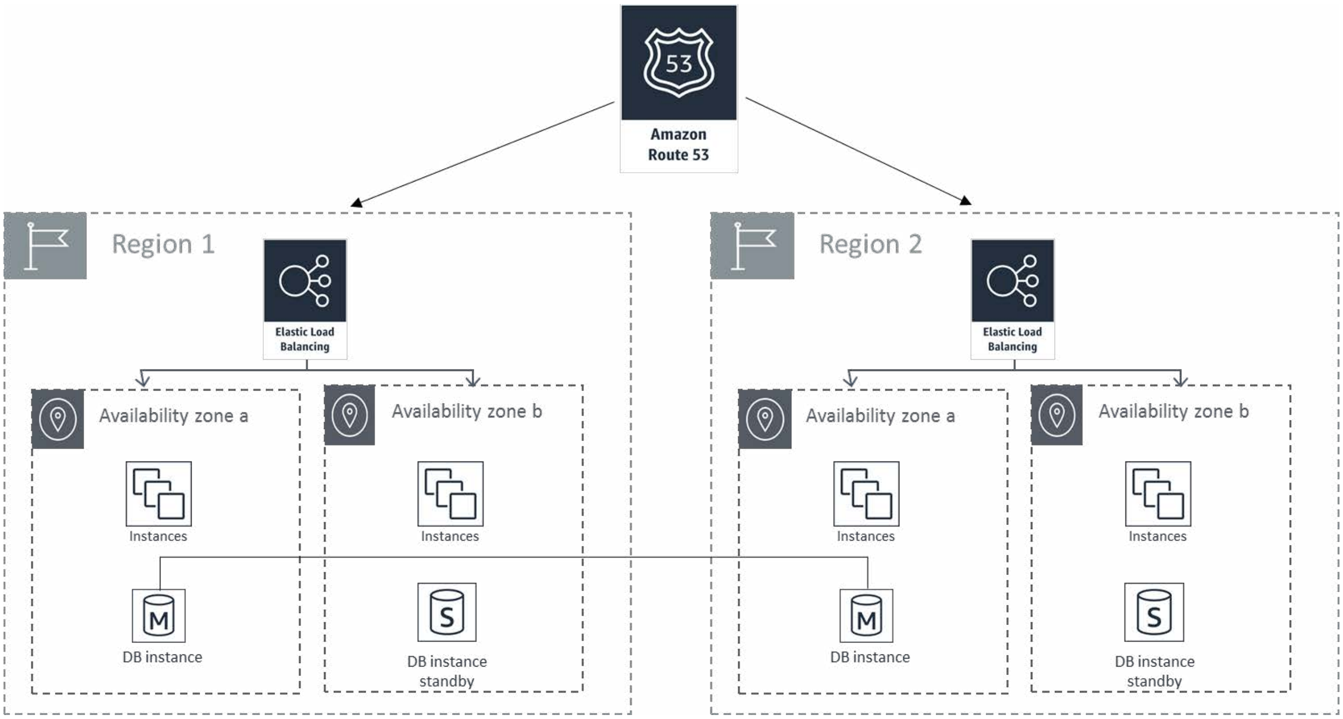


Figure 3. Example of Multi-Region Design

runbooks for reporting and performance tracking; and validate their architecture through realistic, full-scale tests known as "game day" exercises. Per the regulatory requirements in their jurisdictions, financial institutions may provide evidence of such tests, runbooks, and exercises to their financial regulatory authorities.

Assurance Mechanisms

We are prepared to deliver assurance about AWS's approach to operational resilience and to help customers achieve assurance about the security and resiliency of their workloads. Financial institutions and other customers can gain assurance about the security and resiliency of their workloads on AWS through a variety of means, including: reports on AWS's infrastructure and services prepared by independent, third-party auditors; services and tools to monitor, assess, and test their AWS environments; and direct experience with AWS through our audit engagement offerings.

Independent Third-Party Verification

With our standardized offering and millions of active customers across virtually every business segment and in the public sector, we provide assurance about our risk and control environment, including how we address operational resilience. AWS operates thousands of controls that meet the highest standards in the industry. To understand these controls and how we operate them, customers can access our System and Organization Control (SOC) 2 Type II report, reflecting examination by our independent third-party auditor, which provides an overview of the AWS Resiliency Program. Furthermore, an independent third-party auditor has validated AWS's alignment with ISO 27001 standard. The International Organization for Standardization (ISO) brings together experts to share knowledge and to develop, and publish uniform international standards that support innovation and provide solutions to global challenges. In addition to ISO 27001, AWS also aligns with the ISO 27017 guidance on information security in the cloud and ISO 27018 code of practice on protection of personal data in the cloud. The basis of these standards are the development and implementation of a rigorous security program. The Information Security Management System (ISMS) required under the ISO 27001 standard defines how AWS manages security in a holistic, comprehensive manner and includes numerous control objectives (e.g., A16 and A17) relevant to operational resilience. With a non-disclosure agreement in place, customers can download these reports and others through Artifact—more than 2,600 security controls, standards, and requirements in all. AWS can provide such reports upon request to regulatory agencies.

AWS also aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (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 and regardless of size. The U.S. Financial Services Sector Coordinating Council has developed a Financial Services Sector Specific Cybersecurity Profile (available here) that maps the CSF to a variety of international, U.S. federal, and U.S. state standards and regulations. AWS's alignment with CSF, attested by a third-party auditor, reflects the suitability of AWS services to enhance the security and resiliency of financial sector entities.

Direct Assurance for Customers

Customers may also achieve continuous assurance about the resilience of their own workloads. Through services and tools available from the AWS management console, customers have unprecedented visibility, monitoring, and remediation capabilities to ensure the security and compliance of their own AWS environments. Financial institution customers no longer have to rely on periodic snapshots or quarterly and annual assessments to validate their security and compliance.

Consider just a few examples of the many ways customers achieve direct assurance about the security and compliance of their AWS resources.[14] First, customers can integrate their auditing controls into a notification and workflow system using AWS services. For example, in such a system, a change in the state of a virtual server from pending to running would result in corrective action, logging, and, as needed, notify the appropriate personnel. Customers can also integrate their notification and workflow system with a machine learning-driven, cybersecurity service offered by AWS that detects unusual API calls, potentially unauthorized deployments, and other malicious activity.

Second, customers can also translate discrete regulatory requirements into customizable managed rules and continuously track configuration changes among their resources; for example, if a bank has a requirement that developers cannot launch unencrypted storage volumes, the bank can predefine a rule for encryption that would flag the volume for non-compliance and automatically remove the volume.

[14] The AWS services discussed in this section include: Amazon CloudWatch Events, AWS Config, Amazon GuardDuty, AWS Config rules, and Amazon Inspector.

Finally and third, another AWS service allows customers to automatically assess the security of their environment, targeting their network, file system, and process activity and collecting a wide set of activity and configuration data. This data includes details of communication with AWS services, use of secure channels, details of the running processes, network traffic among the running processes, and more—resulting in a list of findings and security problems ordered by severity.

While these and other services correct for non-compliant configurations or security vulnerabilities, AWS also recommends that customers test their applications for operational resilience. Financial institution customers should test for the transient failures of their applications' dependencies (including external dependencies), component failures, and degraded network communications. One major customer has developed open source software that can be a basis for this type of testing. To address concerns that malicious actors may access critical functions or processes in customers' environments, customers can also conduct penetration testing of their AWS environments.[15]

Finally, AWS's efforts to provide transparency about our risk and control environment do not stop at our third-party audit reports or formal audit engagements. Our security and compliance personnel, security solution architects, engineers, and field teams engage daily with customers to address their questions and concerns. Such interaction may be a phone call with the financial institution's security team, an executive meeting with a customer's Chief Information Security Officer and Chief Information Officer, a briefing on AWS's premises—and countless other ways. Customers drive our overall infrastructure and service roadmap, and meeting and exceeding their security and resiliency needs is our number one objective.

[15] For example, in the United Kingdom, the Bank of England has developed the CBEST framework for testing financial firms' cyber resilience. Accredited penetration test companies attempt to access critical assets within the target firm. An accredited threat intelligence company provides threat intelligence and provides guidance how the penetration testers can attack the firm. Financial institution customers subject to the CBEST framework and planning to have a penetration test conducted on their AWS resources need to notify AWS by submitting a request (at https://aws.amazon.com/security/penetration-testing) because such activity is indistinguishable from prohibited security violations and network abuse.