Journal of Advances in Developmental Research (IJAIDR)
E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Applying the AWS Well-Architected Framework in Finance

Siva Kumar Mamillapalli

siva.mamill@gmail.com

Abstract

This paper outlines the Financial Services Industry Lens for the AWS Well-Architected Framework. It provides a comprehensive overview of essential design principles tailored to the financial services sector, along with detailed best practices and recommendations. These practices are aligned with the six pillars of the Well-Architected Framework, ensuring that solutions within the financial services industry meet high standards of reliability, security, efficiency, and performance. The paper serves as a guide for creating optimized, scalable, and secure cloud environments that adhere to industry-specific requirements.

Keywords: AWS, AWS Well-Architected Framework, Finance Industry, Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization, Sustainability

1. Introduction

The financial services industry encompasses a wide range of entities, including financial service firms, independent software vendors (ISVs), market utilities, and infrastructure providers that deliver vital services across the globe. This sector is responsible forfacilitating key activities such as:

- Enabling payments for goods and services
- Supporting financial markets and asset trading
- Acting as intermediaries between savers and borrowers (channeling savings into investments)
- Providing insurance against and dispersing risk

The AWS Well-Architected Framework is designed to help you understand the advantages and challenges of decisions made when building systems on AWS. By leveraging the Framework, you can apply architectural best practices to design and operate reliable, secure, efficient, cost-effective, and sustainable cloud systems. The Framework offers a structured way to evaluate your architecture against best practices and identify opportunities for improvement. We believe that a well-architected system significantly enhances security, reliability, and the potential for business success.

In this lens, we focus on adapting the AWS Well-Architected Framework for financial services industry (FSI) workloads, emphasizing the design, deployment, and architecture of systems that promote resilience, security, cost savings, and operational performance in alignment with the risk and control objectives you define. This includes ensuring compliance with regulatory requirements and expectations from supervisory authorities.

All users should begin by reviewing the best practices and questions outlined in the AWS Well-Architected Framework whitepaper. This document expands on those best practices, specifically targeting the technical architectures and workloads relevant to financial services organizations.

The Financial Services Industry Lens identifies best practices for security, data privacy, and resiliency, tailored to meet the unique requirements of financial institutions based on our global experience. It offers guidance on establishing guardrails for technology teams, empowering them to confidently utilize AWS for building and deploying applications. The Lens also discusses how to integrate transparency and auditability into your AWS environment and provides recommendations for implementing controls to facilitate the adoption of new services while managing IT service costs.

2. Literature Review

2.1 Design Principles

The Well-Architected Framework outlines four key design principles to support effective cloud design for financial services workloads.

Documented Operational Planning – To establish a successful cloud operating model, collaboration with internal stakeholders is essential to define shared goals and strategic direction. Many organizations implement the “Three Lines of Defense” model to enhance risk management:

- First Line of Defense: Operational managers are responsible for daily risk and control procedures.
- Second Line of Defense: Risk management and compliance functions are set up to support and monitor first-line controls.
- Third Line of Defense: Internal auditors provide assurance to senior management and the governing body, maintaining independence and objectivity.

Clearly defining roles and responsibilities across these lines is crucial to building an effective model for regulated cloud adoption. More details can be found in the "Three Lines of Defense" framework from the Institute of Internal Auditors (IIA).

Automated Infrastructure and Application Deployment – Automation is key to accelerating innovation and scaling security, compliance, and governance efforts across cloud environments. Financial services firms that invest in automation are better equipped to speed up deployments and seamlessly integrate security and governance practices into the software development lifecycle.

Security by Design (SbD) – Financial services institutions should adopt a Security by Design approach to pre-test architectures from a security standpoint. SbD aids in implementing control objectives, security baselines, configurations, and audit capabilities for AWS-based applications. Using standardized, automated, and repeatable design templates speeds up common use case deployments while ensuring compliance with security standards. For instance, to protect customer data and prevent unauthorized access or alteration, encryption should be enforced across data at rest, in transit, and at the application level by default.

Automated Governance – Reliance on manual processes like runbooks and checklists can result in delays and inaccuracies. Automated governance ensures fast, accurate checks for application deployment at scale, addressing:

- Account Management: Automate account provisioning and maintain security across large user bases and business units.
- Budget and Cost Management: Monitor and enforce budgets across multiple accounts, workloads, and users.
- Security and Compliance Automation: Manage security, risk, and compliance to ensure adherence to regulations while meeting business objectives.

2.1.1 Operational Excellence

The operational excellence pillar enables financial services institutions to effectively manage risks associated with cloud workloads, comply with regulatory requirements, and enhance agility by automating traditionally error-prone manual processes.

The following design principles can support achieving operational excellence for financial services workloads:

Review Compliance and Regulatory Requirements: Financial services institutions must stay informed about all relevant regulatory and compliance obligations for their cloud service usage and take necessary actions to meet them.

Evaluate Legacy Policies for Cloud Relevance: Institutions typically have established operating policies that govern areas such as disaster recovery, capacity management, security, and compliance. However, cloud services enable new technologies, architectures, and automation that are not possible in on-premises environments. Policies created for on-premises settings should be reassessed from a cloud perspective, rather than assuming they are still applicable. For example, change control should focus on changes to the cloud deployment pipeline architecture and configuration, which may not be automatically tested or reverted in case of failure.

Report Service Disruptions to Stakeholders and Regulatory Bodies: Financial services institutions must communicate service disruptions, operational issues, and failures to both downstream stakeholders and regulatory authorities. Ongoing monitoring of cloud workloads and conducting root cause analysis (RCA) are critical to understanding the events leading to unexpected outcomes and implementing corrective actions to prevent recurrence.

Prioritize Financial Services Workloads Based on Risk Impact: Workloads should be continually reviewed and prioritized according to their potential impact on the business, including reputational, financial, or regulatory consequences. Clear roles and responsibilities should be defined within the organization to understand the risks related to delivering business value through cloud services.

Implement a Risk Management Process: Financial institutions often adopt the Three Lines of Defense model for risk management:

- First Line of Defense: Operational managers handle day-to-day risk and control procedures.
- Second Line of Defense: Risk management and compliance functions build and monitor the first line of defense controls.
- Third Line of Defense: Internal auditors provide independent assurance to senior management and the governing body, ensuring objectivity within the organization.

2.1.2 Security

The security pillar emphasizes the importance of safeguarding information, systems, and assets through risk assessments and mitigation strategies, while still delivering business value. Financial institutions face additional challenges beyond general business regulations, including industry-specific requirements like frequently changing regulations that vary by region. Institutions operating in multiple countries or regions must adhere to different regulatory demands in each location. Due to the assets they manage and their essential role in modern society, financial institutions are often frequent targets of security incidents. To maintain operational continuity, financial institutions must comply with laws and regulations around the protection of personal and financial data, ensuring they implement strong security resilience.

The following security design principles can help enhance the security posture of financial services workloads:

Security by Design (SbD): Financial institutions must adopt a Security by Design approach to implement architectures that are pre-tested for security. SbD helps enforce control objectives, security baselines, configurations, and audit capabilities for applications running on AWS. Standardized, automated, and repeatable design templates streamline the deployment of common use cases and align with security standards across multiple workloads. For example, to protect customer data and reduce the risk of unauthorized access or data manipulation, institutions should implement encryption and manage encryption key access carefully. SbD ensures encryption is applied by default for data at rest, in transit, and at the application level when necessary.

Identify Regulatory Requirements for Implementation: Financial regulators expect institutions to define security objectives for their workloads and implement policies to meet these objectives. They may also impose external requirements on specific workloads, demanding institutions monitor and report compliance. Non-compliance can result in penalties. These requirements should be converted into security control objectives that are sustainable and adaptable to evolving regulations.

Automated Infrastructure and Application Deployment: Automation enables faster performance and innovation while scaling security, compliance, and governance across cloud environments. Financial institutions that invest in automation can speed up deployments and integrate security and governance best practices into their software development lifecycle.

Automated Governance: Manual governance processes, such as using runbooks and checklists, often cause delays and inaccuracies. Automated governance ensures fast, accurate checks for application deployments at scale. Governance at scale typically includes:

- **Account Management**: Automate account provisioning while ensuring security as numerous users and business units request cloud resources.
- **Budget and Cost Management**: Enforce and monitor budgets across various accounts, workloads, and users.
- **Security and Compliance Automation**: Scale security, risk, and compliance management to ensure the organization remains compliant while achieving its business goals.

2.1.3 Reliability

The reliability pillar offers guidance on best practices for designing, delivering, and maintaining AWS environments. It focuses on ensuring systems can recover from disruptions, dynamically scale to meet demand, and mitigate issues like misconfigurations or transient network problems.

Financial institutions' technology systems are complex and interconnected with both financial and non-financial entities. Industries rely on critical workloads like payment processing, trading, and financial messaging. Regulatory bodies such as the Basel Committee and the Federal Reserve focus on the resilience of financial institutions, issuing policies that must be followed.

This section provides best practices for financial institutions to build highly available, resilient, and scalable solutions using AWS services at a lower cost than traditional on-premises IT. Service availability is discussed in relation to Recovery Time Objective (RTO) and Recovery Point Objective (RPO), key concepts covered in the Well-Architected Reliability Pillar.

Financial institutions can leverage AWS services to ensure resilience and availability based on workload criticality. AWS's global infrastructure consists of Regions, Availability Zones (AZs), Local Zones, and edge locations. Services such as Amazon EC2 and Amazon EBS are zonal, meaning they operate and fail independently within a single Availability Zone, while services like Amazon S3 and Amazon DynamoDB are Regional, spanning multiple AZs for high availability.

AWS also offers global services like IAM and Route 53, where the control plane is in one region and the data plane is globally distributed. Understanding fault isolation boundaries is key when building critical workloads on AWS. For instance, disruptions in one AZ do not affect resources in other AZs, and Regional services remain unaffected by issues in other AWS Regions. Global services use separate control and data planes to ensure continued functionality during control plane disruptions.

2.1.4 Performance efficiency

The performance efficiency pillar emphasizes the optimal use of resources to meet requirements and maintain or improve that efficiency as demands change and technology evolves.

Key topics include selecting the appropriate infrastructure based on workload needs, monitoring performance, and making informed decisions to sustain efficiency.

Performance optimization should be an ongoing, data-driven process that involves confirming business requirements, tracking workload performance, identifying underperforming components, and adjusting

infrastructure to meet evolving needs. By periodically reviewing your choices, you can leverage the continuously evolving AWS Cloud.

In addition to the AWS Well-Architected Framework whitepaper's design principles, the following can help achieve performance efficiency for financial services workloads:

Consider both internal and external requirements

Regulators expect financial institutions to define operational performance objectives for workloads and implement policies to achieve them. Regulators may impose Key Performance Indicator (KPI) requirements on critical workloads, such as Open Banking interfaces or trading transaction reporting, and require monitoring and reporting of compliance. Institutions face penalties for non-compliance. These objectives should include both qualitative and quantitative measures of performance to explicitly state the standards the workload must meet.

Architect for performance-driven workloads

Certain financial services workloads, like high-frequency trading systems or risk calculation engines, are highly performance-sensitive. Factors such as speed and latency directly impact profitability. For these workloads, performance must be prioritized over cost efficiency or reliability, requiring trade-offs to achieve performance goals while maintaining essential non-functional requirements such as transactional consistency and recoverability. More details on trade-offs are available in the pillar's Trade-offs section.

Use managed services

Leverage AWS cloud services to allow teams to experiment with various technologies to meet performance goals, while maintaining overall control. Managed services reduce configuration time, operational overhead, and ongoing management efforts, enabling teams to focus on achieving performance objectives using the right tools for the job.

2.1.5 Cost optimization

The cost optimization pillar provides guidance for designing, delivering, and maintaining AWS environments with maximum efficiency and minimal cost. It emphasizes continuous refinement throughout a system's lifecycle to optimize resource use.

Financial services institutions often have high performance, low latency, and changing security and regulatory requirements. These needs, combined with economic pressures, demand dynamic cost optimization across workloads. Larger enterprises have the flexibility to optimize resources, but even SMBs can achieve ROI by migrating to AWS and applying cost optimization best practices.

From initial design to ongoing operations, adopting cost optimization practices enables financial services organizations to minimize costs while meeting business objectives, maximizing IT investment returns.

Key design principles for cost optimization include:

- Monitor cost and resource utilization: Financial services workloads often have cyclical usage patterns. Use AWS monitoring services to scale operations up or down and regularly optimize resource usage and costs.
- Define recovery objectives per workload: Consider varying Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) when designing disaster recovery strategies for different workloads.
- Operational efficiencies: Track and charge back IT costs to responsible business units using AWS analytics tools to encourage accountability and better manage usage costs.
- Data transfer cost: For workloads across multiple regions, monitor and manage data transfer and storage egress costs.
- Adopt cloud financial management: For large enterprise customers, aligning IT with Cloud Financial Management practices helps reduce infrastructure and operational costs through better resource and process management.

2.1.6 Sustainability

The sustainability pillar helps organizations address the long-term environmental, economic, and societal impacts of their activities. Financial institutions need to integrate sustainability into their cloud models to reduce environmental impact, adopt eco-friendly technologies, and prepare for future regulatory requirements.

Key principles for sustainability in financial services include:

- Low-latency workloads for time-critical tasks only: Financial services like trading require high-performance resources, but sectors like banking and insurance do not.
- Use tiered storage for long-term data retention: Financial records, which must be stored for at least seven years, can benefit from Amazon S3 Glacier storage classes for cost-effective, long-term archiving.
- Consider Region selection: Choose low-carbon Regions for processing financial data, but consider data residency and low-latency requirements that may necessitate regions with higher carbon footprints.
- Smart data backup practices: Back up data only when necessary and store it in the appropriate tiers to minimize the carbon footprint.

These practices align financial services with sustainability goals and promote environmentally conscious cloud usage.

3. Conclusion

The Financial Services Industry Lens for the Well-Architected Framework aims to provide financial institutions with architectural best practices for designing and operating reliable, secure, efficient, and cost-effective regulated workloads on AWS. In the operational excellence pillar, we emphasize the alignment of people, processes, and operating models to ensure that workloads on AWS effectively

support critical business services in the financial sector. Financial services architectures must integrate security measures and compliance design patterns based on evidence.

Additionally, financial institutions must continuously monitor, assess, and test failure scenarios and recovery processes in the cloud to meet business resiliency and performance goals. Achieving these objectives can result in significant cost savings through right-sizing and implementing governance models for resource consumption and monitoring on AWS.

This framework enhances security, resiliency, and operational efficiency for financial services organizations migrating to or building on AWS. It also helps institutions meet regulatory and compliance requirements, ensuring a well-rounded approach to cloud adoption.

References

1. Business Intelligence. (2017). Legacy System - Business Intelligence. [online] Available at: http://businessintelligence.com/dictionary/legacy-system/
2. Techopedia.com. (2017). What is a Legacy System (inComputing)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/635/legacy-system
3. Sommerville, I. (2008). Legacy systems. [online] Ifs.host.cs.standrews.ac.uk. Available at: https://ifs.host.cs.standrews.ac.uk/Books/SE9/Web/LegacySys/
4. Logapps LLC. August 15, 2015, "Moving from your legacy system - Cobol conversion, cost, and consequences", Whitepaper.
5. Trend Micro, 2014. Managing your legacy operating systems".Available at: http://about-threats.trendmicro.com/cloudcontent/us/entprimers/pdf/Managing_Your_Legacy_Operating_Systems.pdf
6. Zoufaly, F. (2002). Issues and Challenges Facing Legacy Systems - Developer.com. [online] Developer.com. Available at: http://www.developer.com/mgmt/article.php/1492531/Issuesand-Challenges-Facing-Legacy-Systems.htm
7. EMC, 2014. Building the Cloud Infrastructure, s.l.: EMC Corporation.
8. Vizteams. (2014). Issues and Challenges Facing Legacy Systems.[online] Available at: http://www.vizteams.com/blog/issues-andchallenges-facing-legacy-systems.
9. AWS Architecture Blog: https://aws.amazon.com/blogs/architecture/reduce-cost-and-increase-security-with-amazon-vpc-endpoints/(Accessed on 12th Jan 2023)
10. Modi, C., Patel, D., Borisaniya, B., Patel, A. and Rajarajan, M., 2013. A survey on security issues and solutions at different layers of Cloud computing. The journal of supercomputing, 63(2), pp.561-592.8.
11. AWS White Papers and Guides. www.aws.com, (Accessed on 2nd Feb 2023)