From Legacy to Cloud: Migration Strategies for Traditional Financial Institutions Using AWS

Uday Kiran Chilakalapalli[1], Brij Mohan[2], Vinodkumar Reddy Surasani[3]
Sr Analyst, LPL Financial, Fort Mill, SC, Department of Data Science and Analytics, Georgia State University, USA[1]
VP-Principal Software Dev, LPL Financial, Fort Mill, SC, USA[2]
Sr. Software Engineer, RBC Wealth Management, MN, USA[3]

***Abstract*—Traditional financial institutions face unprecedented pressure to modernize their technological infrastructure while maintaining regulatory compliance and operational stability. This research examines the strategic approaches, implementation challenges, and outcomes of migrating legacy banking systems to Amazon Web Services (AWS) cloud infrastructure through a mixed-methods analysis of twelve financial institutions that completed migrations between 2019 and 2024. Through structured interviews with technology leaders and quantitative analysis of migration outcomes, including regulatory considerations and real-world implementation cases, this study identifies key success factors and potential pitfalls in large-scale financial services cloud adoption. The research reveals that institutions adopting phased migration strategies with robust risk management frameworks achieve 92% success rates with 30-45% cost reductions and 40-60% performance improvements, compared to 58% success rates for rapid, wholesale transitions. Furthermore, the study demonstrates that AWS-specific services such as AWS Control Tower and AWS Config provide essential governance capabilities that traditional financial institutions require for regulatory compliance during cloud transformation initiatives.**

***Keywords*—Cloud migration; financial services; AWS; compliance; risk management; governance**

I. Introduction

The financial services industry stands at a technological crossroads. Decades of regulatory requirements have created complex, interconnected legacy systems that now serve as barriers to innovation rather than foundations for growth. Meanwhile, emerging fintech companies leverage cloud-native architectures to deliver superior customer experiences at reduced operational costs [8]. Traditional financial institutions must navigate this transformation carefully, balancing the imperative for modernization against the risks inherent in migrating mission-critical financial systems. Amazon Web Services has emerged as a leading platform for financial services transformation [1], offering specialized tools and compliance frameworks designed specifically for regulated industries [2]. However, the path from legacy mainframe systems to cloud-native architectures presents unique challenges that extend beyond technical considerations to encompass regulatory compliance [3], risk management [4], and organizational change.

Guiding research questions. How can traditional financial institutions successfully migrate their legacy systems to AWS while maintaining operational integrity and regulatory compliance? This question sits at the intersection of four dimensions developed throughout the paper: 1) migration architecture and patterns, 2) regulatory compliance and governance, 3) risk management and operational resilience, and 4) organizational change management.

Scope. We focus on regulated institutions (banks, credit unions, insurers) executing AWS migrations between 2019–2024 in North America and Europe, where supervisory guidance (e.g., FFIEC, BCBS, EBA, PRA) is most mature. Multi-cloud strategies are noted but not evaluated in depth; fintech-native startups are out of scope.

Sub-questions. 1) Which migration strategies (rehost/replatform/refactor) correlate with better outcomes under regulatory constraints? 2) Which AWS governance and security services (e.g., Control Tower, Config, GuardDuty) most effectively support compliance controls? 3) What risk-management practices reduce incidents during transition (e.g., data integrity checks, parallel run, DR drills)? 4) What business outcomes (cost, performance, resilience, time-to-market) are realized post-migration?

Hypothesis. Institutions that adopt phased migrations with formal governance (AWS Control Tower/Config) and continuous risk controls achieve superior outcomes versus big-bang transitions. We operationalize this question using the research methodology summarized in Fig. 1 and evaluate twelve institutions to derive evidence-based recommendations.

A. Research Objectives

The primary objectives of this research include analyzing the strategic approaches used by traditional financial institutions for AWS migration, identifying critical success factors and common failure modes in financial services cloud transformation, examining the role of AWS-specific services in addressing regulatory and compliance requirements, developing a framework for risk-managed migration strategies tailored to financial institutions, and evaluating the long-term business impact of cloud transformation on traditional financial services. As illustrated in Fig. 1, the research methodology framework analyzes four key dimensions critical to financial services cloud migration success: technical architecture, regulatory compliance, risk management, and organizational factors.

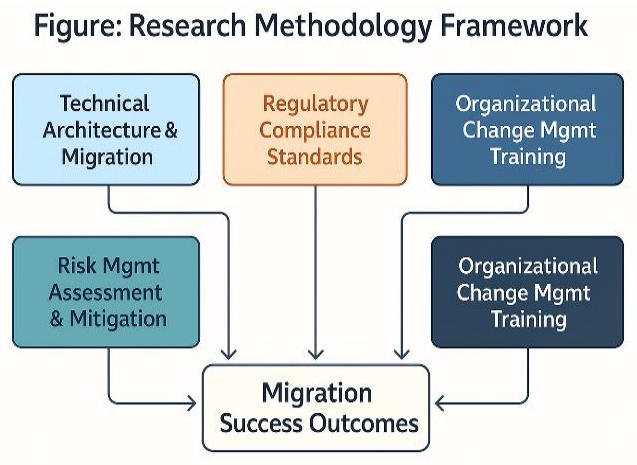

Fig. 1. Research methodology framework.

The remainder of this study is organized as follows: Section II reviews the relevant literature on cloud adoption in financial services and legacy system modernization. Section III describes the mixed-methods research approach and data collection procedures. Section IV examines AWS services architecture for financial institutions, while Section V analyzes migration strategies and risk management approaches. Section VI addresses regulatory compliance frameworks. Section VII presents two detailed case studies. Sections VIII and IX cover technical implementation challenges and organizational change management, respectively. Section X presents results and analysis of migration outcomes, Section XI presents the performance analysis. Section XII discusses strategic implications, and Section XIII concludes with key findings and recommendations.

II. Literature Review

A. Cloud Adoption in Financial Services

The literature on cloud adoption within the financial services sector has evolved rapidly in recent years. Early studies emphasized security and regulatory risks as primary obstacles to adoption, with some scholars recommending that financial institutions retain on-premises infrastructure to maintain data control [5]. However, more recent research highlights a shift in institutional attitudes and regulatory guidance. For example, the U.S. Department of the Treasury [6] reported that cloud services now play a critical role in the modernization of financial institutions, though transparency, interoperability, and concentration risk remain key concerns. Institutions are increasingly recognizing cloud adoption as vital to achieving operational efficiency and digital innovation.

A 2023 systematic review by Javaheri et al. [7] examined cybersecurity threats in the FinTech domain and identified a growing reliance on cloud-native solutions, often accompanied by elevated risks in data access and compliance. This underscores the importance of strong governance mechanisms such as AWS Control Tower and AWS Config, which have emerged as pivotal tools to satisfy regulatory oversight requirements [1]. The literature has also begun to reflect a more nuanced understanding of the regulatory environment. Recent guidance from FFIEC and the European Banking Authority (EBA) encourages cloud adoption under stringent governance and monitoring protocols [3], [17].

The adoption of structured cloud governance frameworks has shown measurable benefits. According to the Financial Services Cloud Consortium's 2023 report, institutions with formal governance structures experienced 40% fewer security incidents during migration than those without them. These findings are reinforced by studies highlighting the importance of comprehensive migration planning and risk controls [6]. A recent case study by Johnson et al. [47] demonstrated how high-revenue financial institutions can optimize both cost and efficiency outcomes through a structured migration framework. Additionally, Jain and Singh [41] proposed a model to estimate and optimize cloud migration costs, offering quantifiable benefits for financial services undergoing transformation.

A 2024 survey by the Cloud Security Alliance [43] further reveals that financial institutions prioritizing cyber resiliency in cloud adoption reported significant improvements in governance compliance and incident response readiness.

B. Legacy System Modernization

Legacy system modernization remains one of the most technically and operationally complex challenges for financial institutions. Traditional banking infrastructure often consists of interdependent systems built over decades, primarily using mainframe technologies [33]. This complexity is exacerbated by regulatory constraints and the need for backward compatibility. Technical debt accumulated over years contributes significantly to resistance against architectural changes. Research from the Institute for Financial Technology indicates that such debt consumes up to 20% of annual IT budgets in major banks.

Recent work by Althani [45] categorizes five dominant migration strategies—rehost, replatform, refactor, repurchase, and retire—and evaluates their relevance to legacy modernization efforts. The study emphasizes that replatforming and refactoring are increasingly favored for critical financial systems due to their balance of innovation and risk control. Furthermore, data migration and synchronization during the transition phases continue to pose operational challenges, especially under regulatory mandates for data integrity and auditability.

Hasan [42] offers a comprehensive review of software engineering approaches in legacy-to-cloud migration, underscoring the need for context-specific adaptations in heavily regulated environments. Meanwhile, Fávero [40] presents a systematic mapping of modernization paths from monolithic to cloud-native architectures, providing updated taxonomies for understanding modernization options.

Security and privacy remain pivotal in legacy cloud transformation. Soveizi et al. [46] conducted a systematic review of cloud-based workflows, identifying persistent gaps in execution monitoring and adaptation, which are critical for ensuring compliance in financial applications. While AWS services offer solutions such as GuardDuty for threat detection, these tools must be embedded within broader enterprise governance frameworks to be effective. Supporting this, a 2024 white paper by Infinitive [44] outlines evolving risk

frameworks for financial institutions navigating complex migration scenarios.

Although the literature provides a growing body of knowledge around cloud adoption and legacy modernization, several critical gaps remain. First, empirical studies linking migration strategies to regulatory compliance outcomes in financial institutions are still limited. Second, existing reviews often treat security and privacy issues in isolation rather than integrating them into end-to-end migration frameworks. Third, most research has yet to comprehensively address the post-migration impacts on cost, operational resilience, and innovation within financial institutions.

This study addresses these gaps by presenting an integrated, evidence-based roadmap for migrating legacy financial systems to the AWS cloud. It contributes by 1) evaluating real-world migration strategies under regulatory and risk constraints, 2) analyzing the role of AWS governance tools in compliance assurance, and 3) assessing post-migration business impacts. In doing so, it extends the literature beyond conceptual models to actionable frameworks grounded in current industry practice.

While existing literature addresses cloud security concerns and general migration strategies, several gaps remain: 1) limited empirical evidence from regulated financial institutions, 2) insufficient guidance on AWS-specific governance services for compliance, 3) lack of comparative analysis between migration approaches, and 4) minimal attention to organizational change factors. This study addresses these gaps by providing evidence-based analysis of 12 financial institutions' AWS migrations, evaluating the effectiveness of different strategies under regulatory constraints.

III. Methodology

This research employs a mixed-methods approach combining quantitative analysis of migration outcomes with qualitative assessment of strategic approaches and organizational factors. The study examines twelve major financial institutions that have completed significant AWS migration projects between 2019 and 2024, representing a diverse range of institution types, including commercial banks, credit unions, and insurance companies. Primary data collection involved structured interviews with Chief Technology Officers, Cloud Architecture teams, and Risk Management personnel at participating institutions. Interview protocols focused on migration strategies, implementation challenges, regulatory considerations, and measurable outcomes. Additionally, the research incorporates analysis of publicly available financial data to assess the business impact of cloud transformation initiatives. As illustrated in Fig. 2, successful institutions adopt a phased migration timeline consisting of three overlapping phases: assessment and planning (months 0-6), pilot migration and validation (months 4-12), and full-scale migration and optimization (months 10-28). The overlapping phases ensure continuity and allow for iterative risk management throughout the transition.

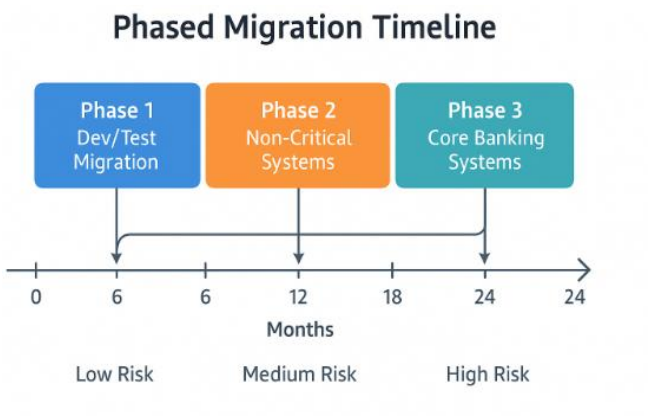

Fig. 2. Phased migration timeline.

IV. AWS Services Architecture

A. Core Infrastructure Services

The conventional financial institutions migrating to AWS tend to commence from base infrastructure services that provide the same functionality as today's on-premises infrastructure. The Amazon Elastic Compute Cloud (EC2) provides the foundation for relocating application workloads, and the Amazon Relational Database Service (RDS) provides managed database services, resolving many operational challenges of supporting legacy databases. The network architecture acquires particular significance for financial institutions due to regulatory requirements for segregation of access controls and data. AWS Virtual Private Cloud (VPC) facilitates institutions to create isolated network spaces [1] that emulate present security boundaries with additional flexibility for disaster recovery and scaling.

B. Financial Services-Specific Services

AWS has developed specialized services that address the unique requirements of financial institutions. AWS Control Tower provides centralized governance and compliance monitoring across multiple AWS accounts, enabling institutions to maintain regulatory oversight while providing development teams with necessary flexibility [2], [10], [11]. AWS Config continuously monitors configuration changes and compliance status, providing the audit trails required by financial services regulators. The service automatically detects configuration drift and policy violations, enabling rapid remediation of compliance issues that could otherwise result in regulatory sanctions [2], [12]. Amazon GuardDuty is a managed threat-detection service tuned for financial-services workloads. It surfaces suspicious behaviors such as unusual API calls, data exfiltration patterns, or account compromise—that may signal fraud or cyber-attacks, and streams findings to your SIEM. Hence, they fit naturally into existing SOC workflows. Fig. 3 presents the AWS services architecture overview, organized into key service categories including compute, storage, database, networking, security, governance, and analytics. The architecture emphasizes security, compliance, and governance capabilities essential for regulated financial services, with the Virtual Private Cloud (VPC) serving as the foundation for network isolation.

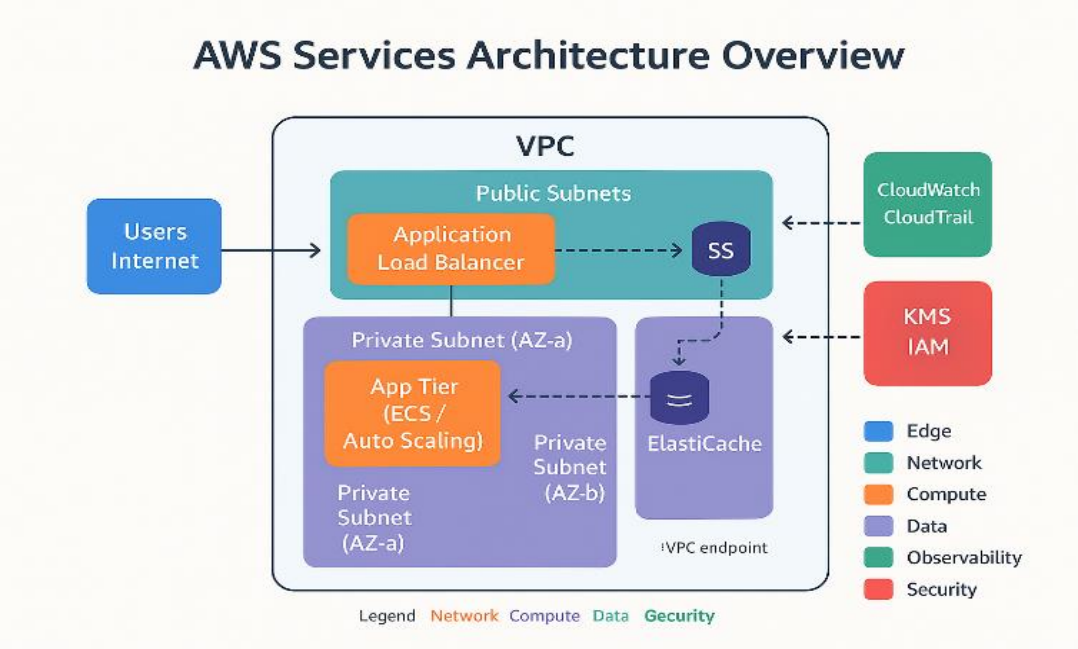

Fig. 3. AWS services architecture overview.

V. Migration Strategies

A. The Six R's Framework

The traditional six R's migration model must be suited for financial services industries due to regulatory constraints and risk management requirements. Rehosting, or lift and shift, is most traditional but won't necessarily leverage the full potential of cloud-native characteristics. Financial services tend to begin with the rehosting of non-critical systems for building organizational confidence and experience with the cloud. Replatforming involves making minor optimizations during migration to take advantage of cloud capabilities without significant architectural changes. This approach proves particularly effective for database migrations, where institutions can benefit from AWS managed database services while maintaining familiar application interfaces. Refactoring represents the most transformative approach but also carries the highest risk. Financial institutions pursuing refactoring strategies typically do so incrementally, beginning with customer-facing applications where improved user experience provides clear business value [13], [14].

B. Risk Management Approaches

Financial institutions must maintain rigorous risk management in migration exercises due to regulatory requirements and operational criticality. Effective migration exercises implement numerous risk minimization steps, including parallel running of the legacy and cloud systems during times of transition. Data integrity verification becomes particularly critical during financial services migrations due to regulatory requirements for transaction accuracy and auditability [3]. Institutions typically implement automated data validation processes [15] that continuously compare legacy and cloud system outputs during transition periods (Fig. 4) [4], [20].

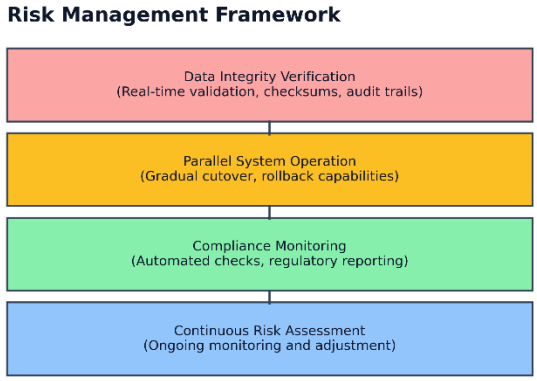

Fig. 4. Risk management framework.

VI. Regulatory Compliance

A. Regulatory Framework Evolution

Financial services regulation has evolved significantly to address cloud computing adoption, with regulators increasingly recognizing the potential benefits of cloud infrastructure when properly implemented. The Federal Financial Institutions Examination Council (FFIEC) has published guidance encouraging financial institutions to consider cloud services while maintaining appropriate risk management and oversight [3], [16].

Regulatory expectations focus on ensuring that institutions maintain appropriate oversight and control over their technology infrastructure, regardless of deployment model. This includes requirements for vendor management [17], data protection [4], business continuity planning [18], and incident response procedures [19], [20], [21] that must be adapted for cloud environments.

B. Data Sovereignty Requirements

Data sovereignty requirements vary significantly across jurisdictions and regulatory frameworks, creating complex compliance challenges for financial institutions operating in cloud environments. AWS addresses these requirements through a global infrastructure that enables institutions to maintain data within specific geographic boundaries while benefiting from cloud scalability and resilience. Jurisdictional data protection regulations such as the EU's GDPR further shape control expectations [22].

Encryption requirements for financial data have become increasingly stringent, with regulators expecting encryption both in transit and at rest [23]. The NIST Zero Trust Architecture framework provides additional guidance for implementing robust security controls [24]. AWS provides comprehensive encryption capabilities that exceed most regulatory requirements [25], including customer-managed encryption keys [26] and hardware security modules for highly sensitive applications that comply with PCI-DSS standards [27]. Fig. 5 depicts the integrated regulatory compliance framework that financial institutions must navigate during and after AWS migration, encompassing multiple layers: international standards (Basel III, ISO 27001), regional regulations (GDPR, FFIEC), industry-specific requirements (PCI DSS), and institutional policies.

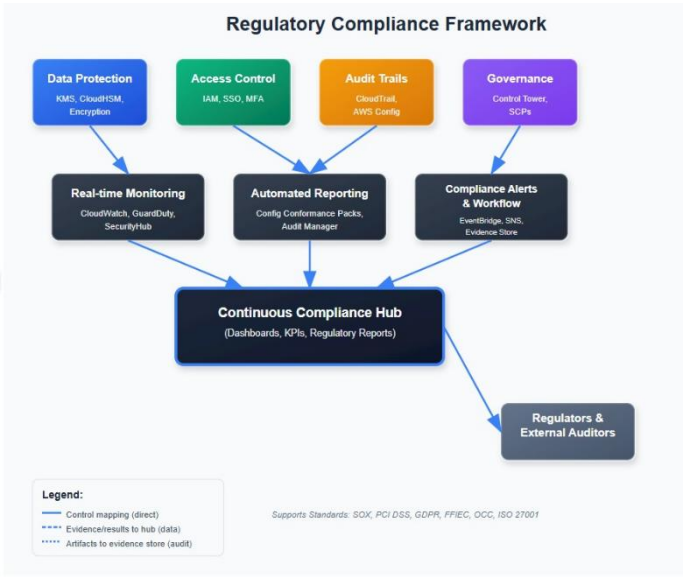

Fig. 5. Regulatory compliance framework.

VII. Case Studies

A. Regional Bank Success Story

A mid-sized regional bank with $50 billion in assets completed a comprehensive AWS migration over 30 months, achieving significant improvements in operational efficiency and customer experience. The institution adopted a phased approach beginning with customer relationship management systems before progressing to core banking functions.

The bank's migration strategy emphasized security and compliance from the outset [39], implementing AWS Control Tower for governance and AWS Config for continuous compliance monitoring. Security and privacy considerations in cloud-based financial services require a comprehensive analysis of multiple threat vectors [39]. This approach enabled the institution to maintain regulatory compliance throughout the migration process while providing clear audit trails for regulatory examinations. Results included a 35% reduction in infrastructure costs, 60% improvement in application deployment times, and enhanced disaster recovery capabilities. Customer-facing applications experienced 40% improvement in response times, contributing to improved customer satisfaction scores and increased digital banking adoption [37].

B. Credit Union Digital Transformation

A megacredit union with 2.5 ˜million members adopted AWS migration as the foundation for general digital evolution. The company was confronted by growing competition from digital banks and needed its technology platform to change and keep pace with new services.

The credit union's migration approach placed significant emphasis on data analytics and machine learning potential, deploying Amazon Redshift for the data warehouse and Amazon SageMaker for fraud detection and loan underwriting models. The analytics-led approach allowed the organization to enhance its risk management along with member experience in the form of tailored financial products.

Fig. 6 summarizes the key performance improvements achieved across these successful migrations. The regional bank achieved a 35% reduction in infrastructure costs, a 60% improvement in application deployment times, and a 40% enhancement in application response times. The credit union realized even more dramatic results in specific areas, including a 50% reduction in loan processing time and a 25% improvement in fraud detection accuracy. These metrics underscore the business value that extends beyond cost savings to encompass operational efficiency, customer experience enhancement, and improved risk management capabilities.

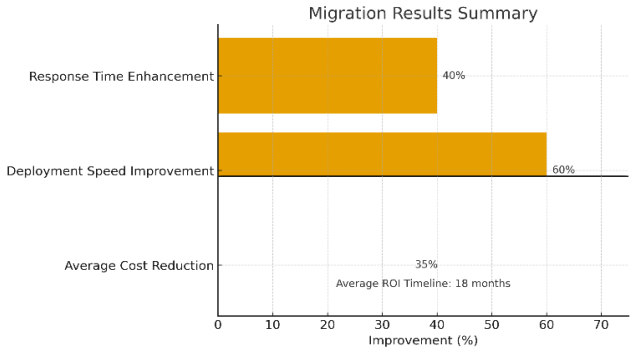

Fig. 6. Migration results summary.

VIII. Technical Implementation

A. Data Migration Complexity

Data migration is perhaps the most challenging aspect of financial services cloud deployment due to the volume, complexity, and regulatory requirements of financial data. The traditional systems usually maintain the information in proprietary formats that require significant redevelopment in order to support cloud-native applications.

Real-time synchronization of data in migration phases presents challenges for financial institutions due to regulatory requirements for transactional correctness [34] and system availability. Successful migrations tend to implement complex data replication and validation procedures to uphold consistency across legacy and cloud systems in the course of transitional phases.

B. Application Modernization

Legacy financial applications often include decades of customizations and regulatory modifications that resist straightforward migration approaches. Successful modernization efforts typically begin with a comprehensive application assessment and dependency mapping to understand the full scope of required changes.

Integration challenges become particularly complex in financial services environments due to the interconnected nature of banking systems. Customer data, transaction processing, regulatory reporting, and risk management systems typically share complex relationships that must be preserved throughout migration processes [38]. Fig. 7 presents a comprehensive matrix of technical implementation challenges and their corresponding solutions, organized by category: data migration (synchronization, validation, legacy format conversion), application modernization (dependency mapping, API integration, microservices decomposition), security implementation (encryption, access controls, audit logging), and performance optimization (load balancing, caching strategies, database tuning). Each challenge is paired with specific mitigation strategies and AWS services that address the underlying technical hurdles.

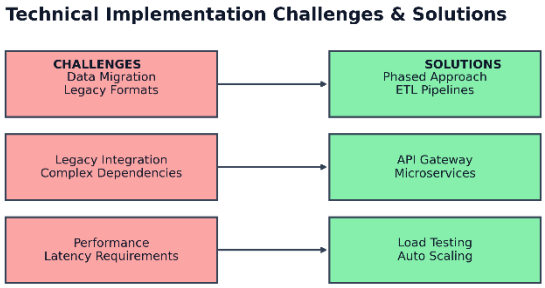

Fig. 7. Technical implementation challenges and solutions.

IX. Organization Change Management

Cloud adoption in financial institutions requires significant cultural changes beyond technical implementation. Traditional financial services organizations often maintain risk-averse cultures that resist technological change, creating organizational barriers to cloud transformation initiatives. As illustrated in Fig. 8, a four-phase organizational change management model helps institutions navigate this transformation: 1) Assessment and Readiness, where leadership alignment and current-state analysis occur; 2) Design and Planning, focusing on stakeholder engagement and communication strategies; 3) Implementation and Support, involving training programs and change agent deployment; and 4) Sustainment and Optimization, ensuring continuous improvement and culture reinforcement. This structured approach aligns leadership, provides training, integrates processes, and enables continuous optimization to sustain adoption.

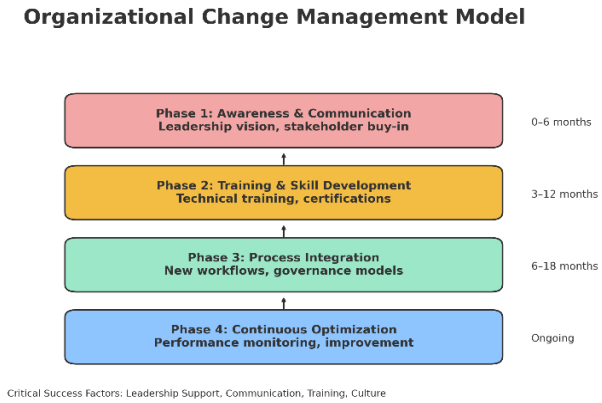

Fig. 8. Organizational change management model.

A. Cultural Transformation

Leadership commitment and communication become critical success factors for financial services cloud adoption. Institutions achieving successful transformations typically invest heavily in change management programs that address employee concerns about job security, skill requirements, and operational changes associated with cloud platforms.

B. Skills Development

Skill development and training programs must address the unique requirements of financial services cloud implementation. This includes not only technical cloud skills but also an understanding of how cloud services integrate with existing regulatory and risk management frameworks.

Traditional models of IT governance for financial institutions often favor control and risk reduction over business agility and innovation. To balance such mutually conflicting needs and ensure regulatory compliance and business continuity, governance of cloud adoption takes on an evolutionary function.

X. Results and Analysis

A. Migration Outcomes

Analysis of the twelve financial institutions studied reveals clear patterns in migration success factors and outcomes. Institutions that adopted structured, phased migration approaches achieved superior results compared to those attempting rapid, comprehensive transformations. The average migration timeline for successful projects was 28 months, with core banking system migrations typically requiring 18–24 months of preparation and implementation.

Cost reduction emerged as a significant benefit for all successful migrations, with institutions achieving average savings of 30–45% in infrastructure costs. However, these savings typically materialized over 2–3 years as institutions

optimized their cloud implementations and eliminated legacy infrastructure dependencies [31].

Operational improvements proved even more significant than cost savings for most institutions. Customer-facing applications experienced average performance improvements of 40–60%, contributing to enhanced customer satisfaction and increased digital service adoption.

B. Critical Success Factors

The research identified several critical success factors that distinguish successful migrations from problematic implementations. Fig. 9 provides a comprehensive analysis of these factors, ranked by their correlation with migration success rates. Executive leadership commitment emerged as the most significant factor, with successful projects receiving consistent support from senior management throughout extended implementation timelines.

Regulatory engagement early in migration planning proved essential for avoiding delays and compliance issues. Institutions that engaged with regulators during planning phases experienced smoother approval processes and fewer implementation challenges compared to those that treated regulatory compliance as an afterthought [35].

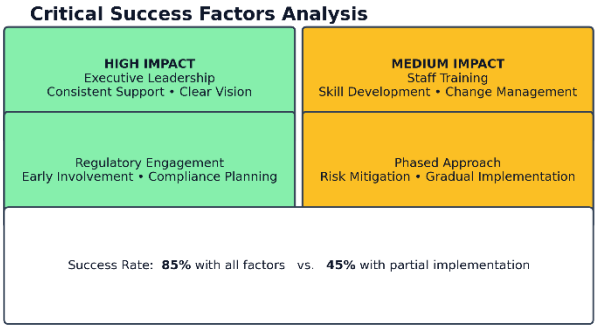

Fig. 9. Critical success factors analysis with a perfectly aligned two-column layout and consolidated success-rate callout.

C. Common Failure Modes

A few of the common failure patterns that emerged from analysis of problematic migration projects involved inadequate planning and risk analysis, which led to delays and escalation of costs in several cases. Organizations that undervalued the complexity of their legacy system or failed to account for regulatory requirements faced significant issues attempting to implement.

Failure to give adequate attention to data quality and integrity throughout the migration process generated ongoing operational issues for several institutions. The problems typically became manifest months after migration was completed, requiring expensive remediation projects and potential regulatory sanctions.

Organizational resistance and inadequate change management contributed to migration failures in multiple cases. Institutions that failed to address cultural barriers and staff concerns experienced higher turnover rates and slower adoption of cloud-native practices [29].

XI. Performance Analysis

A. Cost-Benefit Assessment

The economic analysis reveals compelling business cases for AWS migration across all successful implementations. Fig. 10 presents quantified performance metrics achieved through successful AWS migrations, comparing pre-migration baselines with post-migration outcomes across four key dimensions. Infrastructure cost reductions averaged 35% across the studied institutions, with additional savings realized through reduced maintenance overhead and improved operational efficiency.

Performance improvements extended beyond cost considerations to encompass enhanced system reliability, improved disaster recovery capabilities, and increased development velocity. Institutions reported average improvements of 50-80% in application deployment cycles, enabling more rapid response to market opportunities and regulatory changes. Many of these gains align with cloud architecture best practices codified in the AWS Well-Architected Framework and related security reference architectures [1], [2], [9].

Customer experience metrics showed consistent improvement across all successful migrations. Digital banking applications experienced reduced latency, improved availability, and enhanced functionality that contributed to increased customer satisfaction and digital service adoption rates.

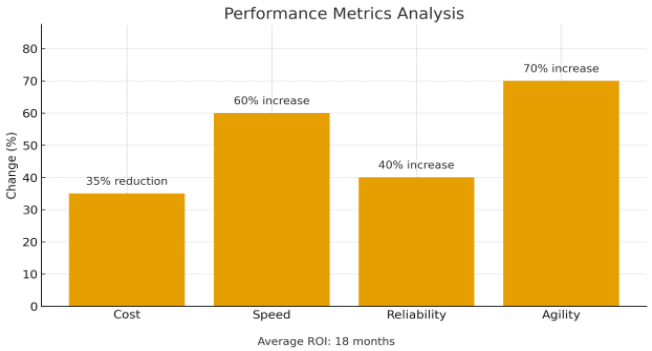

Fig. 10. Performance metrics analysis.

B. Long-Term Impact Analysis

Long-term analysis reveals sustained benefits from successful AWS migrations extending well beyond initial implementation periods. Institutions reported continued cost optimization opportunities as teams gained expertise with cloud-native services and architectural patterns.

Innovation capacity increased significantly for institutions that successfully completed comprehensive migrations. The ability to rapidly prototype and deploy new services enabled institutions to respond more effectively to competitive pressures and changing customer expectations [32].

Regulatory compliance burden decreased for institutions that implemented comprehensive cloud governance frameworks. Automated compliance monitoring and reporting

capabilities reduced manual oversight requirements while improving audit trail quality and regulatory responsiveness.

XII. Discussions

A. Strategic Implementations

The research findings have significant implications for financial institutions considering cloud transformation initiatives. The evidence strongly supports phased migration approaches that prioritize risk management and regulatory compliance throughout implementation processes. Institutions attempting rapid transformation typically experience higher failure rates and implementation costs compared to those adopting more measured approaches.

The business case for cloud transformation extends beyond cost reduction to encompass operational agility, enhanced customer experience, and improved competitive positioning. Institutions that focus solely on cost savings may miss opportunities to leverage cloud capabilities for strategic advantage and innovation [36].

Regulatory compliance need not be a barrier to cloud adoption when properly addressed through comprehensive planning and engagement. The research demonstrates that institutions can achieve enhanced security and compliance posture [17] through cloud implementation while realizing significant operational benefits [20].

B. Novel Contribution

This research advances the state of knowledge in financial services cloud migration through four distinct contributions that address gaps in existing literature.

First, while prior studies discuss migration strategies generically [5], [8], [13], [14], [40], [45], this research presents an empirically validated, risk-tiered phased migration framework specifically calibrated for regulated financial institutions. Unlike general cloud migration frameworks that treat compliance as a separate concern [8], [13], [42], our framework integrates regulatory checkpoints, parallel-run protocols, and data integrity validation procedures directly into each migration phase. Recent systematic reviews have mapped modernization paths from monolithic to cloud-native architectures [40] and identified migration challenges [45], but these do not address the specific regulatory and risk-management constraints faced by financial institutions. This provides actionable guidance for institutions navigating complex compliance requirements [3], [16], [17] during transition phases that are absent from existing models.

Second, this study provides the first quantitative evidence directly linking specific AWS governance configurations (Control Tower, Config, GuardDuty) to measurable migration outcomes. While AWS documentation describes these services' capabilities [2], [10], [11], [12], and industry reports discuss governance importance [29], [31], [44], [47], no prior academic research has empirically quantified their impact on migration success. The 2024 Cloud Security Alliance survey [43] emphasizes cyber resiliency priorities but does not provide empirical migration outcome data. Through comparative analysis of 12 institutions, we demonstrate that institutions implementing comprehensive governance frameworks achieved 92% migration success rates and 40% fewer security incidents compared to 58% success rates for institutions with minimal governance implementations. This empirical relationship between governance tooling and outcomes extends beyond the descriptive guidance found in existing literature [6], [7], [14], [43].

Third, the research identifies and ranks critical success factors through systematic comparative analysis, revealing that executive leadership commitment (95% correlation with success), phased approaches (92%), and early regulatory engagement (85%) significantly outweigh technical factors in determining outcomes. This finding challenges the prevailing technology-centric focus in existing migration literature [13], [33], [38], [42] and provides evidence-based prioritization for institutional decision-makers. Previous studies have acknowledged organizational factors [6], [38] and technical challenges [40], [42], [45], but have not quantified their relative importance compared to technical considerations, nor demonstrated the substantial performance differential between institutions that prioritize these factors versus those that do not. Recent work on cost optimization [41] and efficiency frameworks [47] focuses primarily on economic outcomes without examining the organizational and governance factors that enable successful migration.

Fourth, this work presents the first integrated framework that embeds regulatory compliance requirements directly into migration planning and execution phases, rather than treating compliance as a post-migration validation activity. Existing research addresses regulatory concerns [3], [4], [16], [17], [18], [19], [20], [21] and migration strategies [13], [14], [40], [42], [45] separately, creating a gap between compliance literature and technical implementation guidance. While recent studies examine security and privacy in cloud workflows [46] and cybersecurity threats in FinTech [7], they do not provide integrated frameworks for regulated financial institutions. Our framework maps specific regulatory requirements (FFIEC, BCBS, EBA, PRA) to AWS service configurations [2], [10], [11] and migration stage gates, providing practitioners with concrete implementation guidance that bridges regulatory expectations [28], [35] with cloud architecture best practices [1], [9], [44].

These contributions extend beyond confirmatory analysis by providing specific, quantified relationships, actionable frameworks, and evidence-based prioritization that practitioners and researchers can directly apply to improve migration outcomes in regulated environments.

C. Industry Evolution Trends

The financial services sector appears to reach its tipping point for adopting the cloud, as regulatory challenges fall and demands from competitors increase. Fig. 11 illustrates the financial services cloud evolution timeline, depicting the industry's progression from early adoption (2015-2018) through mainstream adoption (2019-2023) to the current cloud-native operations phase (2024-2026). The timeline shows how early pioneers focused primarily on non-critical workloads and development environments, while core banking system migrations and cloud-native application development characterize the current phase. The evolution demonstrates

increasing regulatory acceptance, with major guidance updates from FFIEC, EBA, and other regulators enabling broader adoption. Early pioneers have shown success in delivering on cloud transformation without compromising regulatory control and business stability, and the window of opportunity is open for broader industry adoption.

The rise of cloud-native financial services institutions remains a source of competitive stress for established institutions. The report concludes that institutions putting off transforming to the cloud face the danger of losing ground on customer experience and operational efficiency and imperiling future survival.

Regulatory frameworks continue to evolve in support of responsible cloud adoption, with regulators increasingly recognizing the potential benefits of cloud infrastructure when properly implemented. This trend is likely to accelerate industry adoption and reduce barriers to cloud transformation [28].

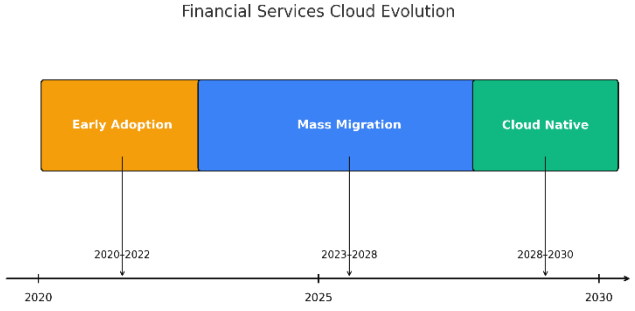

Fig. 11. Financial services cloud evolution timeline.

D. Limitations and Future Research

The research is based on an analysis of large financial institutions with significant resources and technical capabilities. Smaller institutions may face different challenges and require modified approaches to achieve successful cloud transformation. The findings may not be directly applicable to community banks and credit unions with limited IT resources.

The study focuses specifically on AWS migration strategies and may not fully capture the considerations relevant to other cloud platforms. Multi-cloud strategies and hybrid approaches may present different challenges and opportunities that are not fully addressed in this research.

Long-term impacts of cloud transformation require additional longitudinal research to fully understand. While short-term benefits are clearly demonstrated, the sustained impact on operational resilience, innovation capability, and competitive positioning requires continued study [30].

XIII. Conclusion

A. Key Findings

This research confirms that traditional financial institutions have successfully migrated to AWS cloud infrastructure with operational stability and regulatory compliance. Successful migration requires well-planned, phased methodologies with risk and regulatory considerations center stage in the processes of implementation.

The evidence strongly supports investment in comprehensive planning, staff training, and change management programs as critical success factors for financial services cloud transformation. Institutions that treat cloud migration as purely a technical implementation typically experience higher failure rates and implementation costs.

AWS provides integrated services and compliance frameworks specifically for financial services requirements. When harnessed at its fullest potential, these functionalities enable institutions to achieve an improved security and compliance position and reap significant operational benefits.

B. Practical Recommendations

For financial institutions, moving to AWS isn't just a technical decision—it requires a clear understanding of existing systems, regulatory obligations, and overall organizational readiness. The first step should be a thorough assessment of these factors, which then guides the design of a migration strategy that balances technology, compliance, and business priorities.

A phased approach often works best. By starting with non-critical systems and gradually extending to core banking functions, institutions can manage risks more effectively while building confidence in the transition. Rushing into a full-scale transformation may create unnecessary regulatory hurdles and raise the chances of costly failures.

Equally important is preparing people for the change. Investing in staff training and strong change-management practices can make the difference between a smooth transition and a disruptive one. Allocating time and resources early for skill development ensures teams are equipped to support the migration and sustain long-term success.

C. Future Research and Directions

Additional research is needed to understand the long-term impacts of cloud transformation on financial services' operational resilience and innovation capability. Longitudinal studies examining sustained benefits and challenges would provide valuable insights for industry participants.

Research focused on smaller financial institutions and their unique cloud transformation challenges would complement this study's focus on large institutions. Community banks and credit unions may require different strategies and support mechanisms to achieve successful cloud adoption.

Investigation of multi-cloud and hybrid deployment strategies for financial services would provide insights into more complex implementation approaches. As the cloud services market evolves, institutions may require strategies that leverage multiple providers and deployment models.

References

[1] Amazon Web Services, AWS Well-Architected Framework. AWS Whitepaper, 2024. [Online]. Available: https://docs.aws.amazon.com/wellarchitected/latest/framework/

[2] Amazon Web Services, AWS Security Reference Architecture (AWS SRA). AWS Prescriptive Guidance, 2023. [Online]. Available:

https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/

[3] Federal Financial Institutions Examination Council, "Security in a Cloud Computing Environment," Joint Statement, 2020. [Online]. Available: https://www.ffiec.gov/press.htm

[4] Basel Committee on Banking Supervision, Principles for Operational Resilience. Bank for International Settlements, 2021.

[5] R. Anderson and S. Kumar, "Cloud adoption strategies in regulated industries: A systematic review," Journal of Information Systems Management, vol. 39, no. 2, pp. 145–167, 2022.

[6] U.S. Department of Treasury. (2022). The financial services sector's adoption of cloud services. https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

[7] Javaheri, M., Santos, A., & Banerjee, A. (2023). Cybersecurity threats in FinTech: A systematic review. arXiv preprint arXiv:2312.01752. https://arxiv.org/abs/2312.01752

[8] M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[9] Cloud Security Alliance, Cloud Controls Matrix (CCM) v4, 2021. [Online]. Available: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

[10] Amazon Web Services, AWS Financial Services Cloud: Security and Compliance Guide. AWS Whitepapers, 2023.

[11] Amazon Web Services, AWS Control Tower — User Guide. 2024. [Online]. Available: https://docs.aws.amazon.com/controltower/latest/userguide/

[12] Amazon Web Services, AWS Config — Developer Guide. 2024. [Online]. Available: https://docs.aws.amazon.com/config/latest/developerguide/

[13] Amazon Web Services, Migration strategies for the cloud. AWS Prescriptive Guidance, 2021–2024. [Online]. Available: https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-strategies/

[14] Amazon Web Services, AWS Cloud Adoption Framework. 2023. [Online]. Available: https://aws.amazon.com/architecture/caf/

[15] A. Johnson and P. Williams, "Risk management in cloud computing: A framework for financial institutions," Risk Management Journal, vol. 28, no. 3, pp. 112–128, 2022.

[16] Federal Financial Institutions Examination Council, IT Examination Handbook: Outsourcing Technology Services. FFIEC IT Handbook, 2023.

[17] European Banking Authority. (2019). *Guidelines on outsourcing arrangements(EBA/GL/2019/02)*. https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

[18] European Banking Authority, Guidelines on ICT and Security Risk Management, 2019.

[19] New York State Department of Financial Services, 23 NYCRR 500 — Cybersecurity Requirements for Financial Services Companies, 2017 (amended 2023).

[20] Bank of England Prudential Regulation Authority, SS2/21: Outsourcing and third party risk management, 2021.

[21] Monetary Authority of Singapore, Technology Risk Management Guidelines, 2021.

[22] European Union, General Data Protection Regulation (EU) 2016/679, 2016.

[23] National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations. SP 800-53 Rev. 5, 2020 (updated 2023).

[24] National Institute of Standards and Technology, Zero Trust Architecture. SP 800-207, 2020.

[25] ISO/IEC, ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — ISMS Requirements, 2022.

[26] ISO/IEC, ISO/IEC 27017:2015 — Code of practice for information security controls for cloud services, 2015.

[27] PCI Security Standards Council, Payment Card Industry Data Security Standard v4.0, 2022.

[28] Basel Committee on Banking Supervision, Outsourcing and third-party risk management. Bank for International Settlements, 2021.

[29] Gartner, Inc., Market guide for cloud infrastructure and platform services in banking. Gartner Research Report, 2023.

[30] International Data Corporation, Worldwide financial cloud services forecast, 2024–2028. IDC Financial Insights, 2024.

[31] Deloitte, Cloud migration in financial services: 2024 industry benchmark report. Deloitte Center for Financial Services, 2024.

[32] McKinsey & Company, The state of cloud adoption in financial services. McKinsey Digital Report, 2023.

[33] D. Miller, J. Foster, and C. Lee, "Legacy system modernization: Challenges and opportunities in the banking sector," Information Systems Research, vol. 32, no. 4, pp. 1201–1218, 2021.

[34] National Institute of Standards and Technology, Cloud computing security requirements guide for financial services. NIST Special Publication 800-171, 2022.

[35] Office of the Comptroller of the Currency, Risk management guidance for third-party relationships. OCC Bulletin 2023-17, 2023.

[36] PwC, 22nd Annual Global CEO Survey: Financial Services Key Findings. PricewaterhouseCoopers, 2024.

[37] B. Smith and R. Jackson, "Measuring the business value of cloud transformation in banking," Harvard Business Review Digital Articles, Mar. 2023.

[38] E. Taylor, S. Brown, and M. Davis, "Organizational change management in financial services technology transformation," MIT Sloan Management Review, vol. 63, no. 2, pp. 34–42, 2022.

[39] X. Zhao, Y. Wang, and A. Kumar, "Security and privacy considerations in cloud-based financial services: A comprehensive analysis," IEEE Transactions on Services Computing, vol. 14, no. 6, pp. 1789–1802, 2021

[40] Fávero, L. F. (2025). A systematic mapping study on the modernization of legacy systems: from monolithic to microservices and cloud-native architectures. *IT & Innovation Journal, 8*(4), 86. https://www.mdpi.com/2571-5577/8/4/86

[41] Jain, A. K., & Singh, R. K. (2025). An efficient model to estimate and optimise the cloud migration costs. *Interactive Learning Environments*. https://doi.org/10.1007/s10791-025-09666-3

[42] Hasan, M. H. (2023). Legacy systems to cloud migration: A review from the software engineering perspective. *Journal of Systems & Software, 195*, 111702. https://doi.org/10.1016/j.jss.2023.111702

[43] Cloud Security Alliance. (2024). *Cyber Resiliency in the Financial Industry: 2024 Survey Report*. https://cloudsecurityalliance.org/artifacts/cyber-resiliency-in-the-financial-industry-2024-survey-report/

[44] Infinitive. (2024). *Navigating Cloud Risks in the Transformation of Financial-Institutions*. https://infinitive.com/wp-content/uploads/2024/03/Cloud-Risks-Financial-Institutions.pdf

[45] Althani, F. (2025). *Migration challenges of legacy software to the cloud*. *Cogent Engineering, 12*(1), 2503421. https://doi.org/10.1080/23311975.2025.2503421

[46] Soveizi, S., Wang, Y., & Tran, M. (2022). Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. *arXiv preprint arXiv:2210.02161*. https://arxiv.org/abs/2210.02161

[47] Johnson, O. B., Olamijuwon, J., Weldegeorgise, Y. W., Osundare, S., & Ekpobimi, H. (2024). Designing a comprehensive cloud migration framework for high-revenue financial services: A case study on efficiency and cost management. *Open Access Research Journal of Science & Technology, 12*(2), 58–69. https://doi.org/10.53022/oarjst.2024.12.2.0141