

Navigating Enterprise AWS Cloud Migration: Security, Failures, and Optimization

Dinesh Boinpally

Northwest Missouri State University, USA

Abstract: Enterprise cloud migration to Amazon Web Services (AWS) represents a transformative journey that organizations undertake to enhance scalability, agility, and operational efficiency. An in-depth exploration of AWS migration challenges reveals critical insights into security considerations, common failure patterns, and optimization strategies that shape successful cloud transformations. Through detailed examination of real-world implementations, the content identifies key factors contributing to migration failures, including insufficient planning, skills gaps, and cost management oversights. The discussion emphasizes the importance of implementing robust security frameworks, maintaining compliance standards, and adopting cloud-native practices throughout the migration lifecycle. Post-migration optimization emerges as a crucial phase, encompassing cost management, performance tuning, and security enhancement strategies. The integration of cloud-native technologies, including containerization, serverless architectures, and Dev Ops practices, demonstrates significant impact on migration success. By highlighting practical challenges and effective solutions, this technical article provides valuable guidance for organizations pursuing AWS cloud adoption while maintaining security, efficiency, and operational excellence.

Keywords: Cloud Migration Security, Enterprise AWS Transformation, Cloud-Native Integration, Migration Optimization, Dev Ops Implementation.

INTRODUCTION

As organizations increasingly embrace digital transformation, enterprise-scale migrations to Amazon Web Services (AWS) have become a critical strategic initiative. According to Deloitte's comprehensive analysis, the cloud migration market has shown remarkable growth, with the percentage of companies using cloud services projected to rise from 41% in 2020 to 90% by 2025. This unprecedented shift is driven by various factors, including the need for enhanced scalability, improved disaster recovery capabilities, and reduced total cost of ownership (TCO). The research indicates that the cloud computing market achieved a significant milestone, reaching \$411 billion in 2020 and demonstrating a compound annual growth rate of 16% (Stewart, D. *et al.*, 2020).

The journey to cloud adoption encompasses complex challenges that extend beyond technical considerations. Research by eG Innovations reveals that organizations face distinct challenges in both migration and modernization phases. While cloud migration primarily focuses on relocating existing applications and data to cloud infrastructure with minimal changes, modernization involves fundamental architectural transformations to leverage cloud-native capabilities. This distinction is crucial, as approximately 65% of organizations initially opt for a "lift and shift" approach, only to later realize the need for comprehensive modernization to fully capitalize on cloud benefits (Kumar, N. 2024).

The complexity of enterprise cloud transformation is further emphasized by Deloitte's findings, which show that 90% of organizations accelerated their cloud adoption plans in response to the global pandemic. However, this acceleration has led to significant challenges, with organizations reporting that security (47%), governance (42%), and compliance (36%) remain their top concerns during cloud migration initiatives (Stewart, D. *et al.*, 2020). The technical landscape has evolved to address these challenges, with cloud service providers offering specialized tools and services for different migration approaches, including rehosting, replatforming, and refactoring.

Contemporary cloud migration strategies must account for the evolving nature of enterprise applications. According to eG Innovations' analysis, successful cloud transformations require a holistic approach that encompasses both technical and organizational changes. This includes considerations for application performance monitoring, cost optimization, and security compliance. The research indicates that organizations implementing comprehensive monitoring solutions during migration experience 43% fewer performance-related issues and achieve 38% faster problem resolution times (Kumar, N. 2024). Looking ahead, the cloud migration landscape continues to evolve, with Deloitte projecting that by 2025, more than 85% of organizations will adopt a cloud-first principle when making new technology investments. This trend is accompanied by a significant shift toward

multi-cloud strategies, with 93% of enterprises already employing multiple cloud services to optimize their operations and reduce vendor lock-in (Stewart, D. *et al.*, 2020). The integration of artificial intelligence and machine learning capabilities further enhances the value proposition of cloud adoption, enabling organizations to leverage advanced analytics and automation capabilities.

The Security Imperative in Cloud Migration

Security remains the foremost concern for enterprises undertaking AWS migrations, with recent data from UpGuard revealing unprecedented challenges in the cloud security landscape. The average cost of a data breach reached \$4.35 million in 2023, marking a 2.3% increase from the previous year. Organizations in the United States face even higher costs, averaging \$9.44 million per breach. These figures underscore the critical importance of robust security measures during cloud migration, particularly as remote work environments have increased the average cost of breaches by \$1.07 million (Tunggal, A. T. 2025). The shift from traditional on-premises infrastructure to cloud environments necessitates a fundamental reimagining of security architectures. According to Orca Security's 2024 State of Cloud Security Report, 80% of organizations operate in a multi-cloud environment, with 42% utilizing three or more cloud providers simultaneously. This complexity has led to significant security challenges, as 69% of security teams report spending excessive time on manual security tasks rather than addressing critical vulnerabilities. The research indicates that 49% of organizations have at least one publicly accessible workload containing sensitive information, highlighting the urgent need for improved security protocols (Sadon, S and Galea, D. 2024).

Identity and Access Management (IAM) complexities present significant challenges in cloud environments. UpGuard's analysis reveals that human error remains a leading cause of data breaches, accounting for 95% of cyber security incidents. The average time to identify and contain a breach has reached 277 days, with system

complexity and security team shortages contributing to extended response times. Organizations in highly regulated industries, such as healthcare and finance, face even greater challenges, with breach costs averaging \$10.93 million and \$5.97 million respectively (Tunggal, A. T. 2025). Cloud security posture management has become increasingly critical, as Orca Security's research shows that 87% of alert fatigue is caused by misconfigured cloud assets and excessive permissions. The study found that 78% of organizations have at least one neglected cloud asset with a known vulnerability that's been unaddressed for over 180 days. Furthermore, 55% of cloud assets are running on unsupported operating systems, while 36% of organizations have at least one critical public-facing vulnerability that remains unpatched (Sadon, S. and Galea, D. 2024).

The implementation of comprehensive security measures is further complicated by compliance requirements and data protection mandates. UpGuard's research indicates that organizations with fully deployed security AI and automation experienced significantly lower breach costs, saving an average of \$3.05 million compared to organizations without such capabilities. The study also reveals that healthcare organizations face the highest per-record cost of a breach at \$368, followed by financial services at \$364 per record, emphasizing the critical nature of sector-specific security considerations (Tunggal, A. T. 2025).

Cloud migration security strategies must evolve to address emerging threats, as evidenced by Orca Security's finding that 59% of organizations discovered sensitive data in previously unknown locations during cloud security assessments. The research highlights that 41% of cloud assets contain at least one high-severity security issue, while 26% of organizations have exposed at least one database to the internet. These findings emphasize the need for continuous security monitoring and risk assessment, particularly as 72% of security teams report challenges in prioritizing security alerts effectively (Sadon, S and Galea, D. 2024).

Table 1: Cloud Security Challenges and Impact Metrics (Tunggal, A. T. 2025; Sadon, S and Galea, D. 2024).

Security Aspect	Occurrence Rate (%)	Impact Level (%)	Time to Resolve (days)	Cost Impact (\$M)
Data Breaches	83	89	277	4.35
IAM Misconfigurations	66	72	90	3.05
Compliance Violations	76	63	45	3.86

Public Vulnerabilities	49	55	180	2.75
Security Policy Gaps	69	78	60	2.95

Learning from Migration Failures

Analysis of failed AWS migrations reveals several common patterns that organizations must address, with Fortinet's 2024 Cloud Security Report highlighting that 95% of organizations are moderately to extremely concerned about cloud security. The study reveals that 82% of organizations experienced at least one cloud security incident in the past year, while 76% report that cloud security challenges have become more difficult to address compared to the previous year. These findings emphasize the critical relationship between security considerations and successful cloud migrations (Harris, F. 2024).

Insufficient planning and assessment emerge as primary contributors to migration failures. According to DuploCloud's analysis, 78% of organizations cite inadequate planning as the primary reason for failed cloud migrations. The research indicates that companies frequently underestimate the complexity of their existing infrastructure, with 65% of organizations failing to conduct comprehensive application dependency mapping before migration. This lack of preparation leads to extended downtimes, with the average migration taking 30% longer than initially planned. Furthermore, 71% of organizations report discovering critical dependencies only after beginning their migration efforts, resulting in significant project delays and cost overruns (Gaydos, B. 2024).

The skills gap and cultural resistance present formidable challenges in cloud adoption. Fortinet's research reveals that 83% of organizations face significant challenges in hiring and retaining cloud security professionals. The study indicates that 80% of organizations now use two or more cloud providers, further complicating the expertise required for successful migrations. Security teams are particularly strained, with 72% of organizations reporting that cloud security responsibilities are shared between multiple teams, leading to coordination challenges and potential security gaps. The research also shows that 74% of organizations struggle to maintain consistent security policies across their cloud environments (Harris, F. 2024). Cost management oversights

continue to plague cloud migration projects, with Duplo Cloud's analysis showing that 68% of organizations exceed their initial migration budgets. The study reveals that improper resource allocation accounts for 45% of cost overruns, while inadequate monitoring and optimization strategies contribute to an additional 32% of unexpected expenses. Organizations frequently underestimate the complexity of data transfer costs, with 57% reporting significant unexpected charges related to cross-region data movement. The research indicates that 63% of companies fail to implement proper cost optimization strategies during the initial migration phase, leading to sustained inefficiencies in cloud resource utilization (Gaydos, B. 2024).

Security considerations significantly impact migration success rates, as Fortinet's analysis shows that 93% of organizations are concerned about misconfigurations in their cloud environments. The study reveals that 75% of organizations have experienced incidents related to cloud misconfigurations, while 69% report challenges in maintaining consistent security controls across hybrid and multi-cloud environments. Additionally, 78% of organizations identify the complexity of cloud security tools and solutions as a significant challenge, with 66% struggling to achieve visibility across their cloud infrastructure (Harris, F. 2024). The impact of organizational readiness on migration success cannot be understated. Duplo Cloud's research indicates that 73% of organizations face significant challenges due to resistance to change within their IT teams. The study shows that companies with established change management processes are 2.5 times more likely to complete their migrations successfully. Furthermore, 69% of organizations report that lack of executive support and clear ownership of migration initiatives contributes to project failures. The research emphasizes that successful migrations require a combination of technical expertise, organizational alignment, and comprehensive planning, with organizations implementing formal migration frameworks experiencing 45% fewer disruptions during their cloud transition (Gaydos, B. 2024).

Table 2: Cloud Migration Failure Patterns and Organizational Impact (Harris, F. 2024; Gaydos, B. 2024).

Failure Pattern	Organizations Affected (%)	Project Delay (months)	Cost Overrun (%)	Recovery Time (weeks)
Inadequate Planning	78	6.5	47	12
Skills Gap	76	4.5	35	8
Cultural Resistance	73	4.8	32	6
Security Issues	75	3.2	28	10
Cost Management	68	5.1	45	4

Post-Migration Optimization Strategies

Post-migration optimization has become a critical focus for organizations leveraging AWS environments, with Arkitech Group's 2024 ESR Report revealing that enterprises typically overspend between 15% to 25% on cloud services due to suboptimal resource allocation. The study indicates that organizations implementing systematic optimization strategies achieve average cost reductions of 32% within the first year post-migration. Furthermore, enterprises that adopt comprehensive cloud financial operations (FinOps) practices report an average improvement of 28% in their cloud cost efficiency, with some organizations achieving up to 40% reduction in their monthly cloud spending through strategic resource management (Arkitech Group. 2024).

Resource utilization optimization emerges as a primary focus area, with Granica's analysis showing that 67% of organizations struggle with properly sizing their cloud resources. The research reveals that implementing automated right-sizing recommendations leads to an average cost reduction of 35% across compute resources, while organizations utilizing advanced capacity planning tools report 41% improvements in resource utilization rates. Additionally, companies employing AI-driven optimization tools achieve a 23% reduction in unnecessary cloud spending and maintain an average resource utilization rate of 78%, significantly higher than the industry average of 45% (Granica. 2024).

Performance optimization strategies have evolved significantly, as Arkitech's research indicates that 84% of organizations now prioritize application performance monitoring post-migration. The study shows that companies implementing comprehensive monitoring solutions reduce their mean time to detection (MTTD) by 56% and achieve a 47% improvement in application response times. Organizations leveraging cloud-native performance optimization tools report an average reduction of 38% in performance-related

incidents, while those implementing automated scaling policies experience 42% fewer capacity-related outages (Arkitech Group. 2024).

Security and compliance optimization has become increasingly critical, with Granica's analysis revealing that 91% of organizations face challenges in maintaining security posture across their cloud environments. The research shows that companies implementing automated security controls achieve a 63% reduction in security incidents and a 45% improvement in compliance audit outcomes. Organizations utilizing integrated security and compliance platforms report 52% faster threat detection and response times, while those implementing continuous compliance monitoring reduce their audit preparation time by 67% (Granica. 2024). Cost allocation and governance frameworks demonstrate significant impact on optimization success, according to Arkitech's findings. Organizations implementing comprehensive tagging strategies achieve 44% better cost visibility and reduce unattributed cloud spending by 51%. The research indicates that companies utilizing automated governance controls experience 37% fewer policy violations and maintain 89% better alignment with budgetary constraints. Furthermore, enterprises implementing cross-functional FinOps teams report 33% more accurate budget forecasting and achieve 29% higher returns on their cloud investments (Arkitech Group. 2024).

Cloud architecture optimization presents ongoing opportunities for improvement, with Granica's study showing that 76% of organizations benefit from regular architecture reviews. The research reveals that companies conducting quarterly architecture assessments identify an average of 12 major optimization opportunities per review, leading to potential cost savings of 25-30%. Organizations implementing infrastructure as code (IaC) practices achieve 48% faster deployment times and maintain 56% better consistency in their cloud environments. Additionally, enterprises

utilizing cloud-native services report 39% lower operational costs compared to those maintaining lifted-and-shifted applications (Granica. 2024).

Table 3: Cloud Optimization Outcomes and Performance Improvements (Arkitech Group. 2024; Granica, 2024).

Optimization Area	Cost Reduction (%)	Performance Gain (%)	Implementation Time (months)
Resource Utilization	35	67	3
Security Controls	28	82	2
Operational Efficiency	42	71	4
Application Performance	31	78	3
Infrastructure Cost	45	65	2

Best Practices for Successful AWS Migration

Comprehensive planning has evolved significantly as organizations adapt to the changing cloud landscape, with Cogent Infotech's 2024 predictions highlighting that 87% of enterprises are now implementing hybrid cloud-edge strategies in their migration planning. The research reveals that organizations are increasingly focusing on edge computing capabilities, with 73% of companies planning to distribute their workloads between cloud and edge locations by 2025. This shift has led to a 45% increase in the complexity of migration planning, as companies must now consider both cloud and edge infrastructure in their assessment strategies. The study indicates that enterprises implementing comprehensive planning approaches that incorporate edge computing considerations achieve 52% better performance outcomes and 38% improved data processing efficiency (Cogent Infotech 2024).

The significance of a security-first approach has become paramount, as IBM's analysis demonstrates that organizations implementing AI-driven security controls during migration experience 64% fewer security incidents. The study reveals that enterprises utilizing IBM Watson's AI capabilities for security assessment and monitoring achieve a 57% reduction in false positives and identify potential threats 3.2 times faster than traditional approaches. Organizations implementing automated security frameworks report a 43% improvement in compliance adherence and maintain 89% better visibility across their hybrid cloud environments. The research emphasizes that companies leveraging AI-powered security tools during migration reduce their security-related downtime by 51% and achieve 47% faster incident resolution times (Khan, T. and Henderson, D. 2024).

Edge computing integration has emerged as a critical consideration in migration strategies, with

Cogent Infotech reporting that 68% of organizations are now prioritizing edge-ready infrastructure in their migration planning. The study shows that companies implementing edge-aware monitoring systems achieve 41% better application performance and maintain 63% lower latency for critical applications. Furthermore, organizations that establish dedicated edge computing capabilities alongside their cloud infrastructure report 55% improved data processing efficiency and 49% better real-time analytics capabilities. The research indicates that enterprises incorporating edge computing considerations in their migration strategies experience 34% fewer data transfer-related issues and achieve 57% better overall system reliability (Cogent Infotech 2024).

IBM's comprehensive analysis emphasizes the importance of automated migration tools and AI-driven optimization, revealing that organizations utilizing automated assessment tools complete their migrations 2.5 times faster than those relying on manual processes. The study shows that enterprises implementing IBM's AI-powered migration assessment tools achieve 61% better accuracy in dependency mapping and reduce their migration planning time by 47%. Companies leveraging automated workflow optimization report 53% fewer migration-related disruptions and maintain 76% better consistency in their deployment processes. Additionally, organizations utilizing AI-driven performance monitoring during migration experience 44% fewer performance-related incidents and achieve 58% better resource utilization (Tasmiha Khan and Dina Henderson. 2024). The evolution of operational excellence in cloud migration has been significant, with Cogent Infotech's research showing that 79% of organizations are implementing advanced automation and orchestration tools. The study reveals that companies adopting edge-aware

operational practices achieve 46% better system reliability and maintain 71% higher availability rates. Organizations implementing comprehensive monitoring solutions that span both cloud and edge environments report 58% faster incident detection times and achieves 62% better visibility across their distributed infrastructure. The research also indicates that enterprises establishing clear operational metrics across their hybrid environments demonstrate 43% better alignment between technical capabilities and business requirements (Cogent Infotech. 2024).

Disaster recovery and business continuity planning have become increasingly sophisticated, as highlighted by IBM's findings. Organizations implementing AI-driven disaster recovery solutions achieve 69% faster recovery times and

maintain 83% better data consistency during recovery operations. The study shows that enterprises utilizing automated backup verification tools experience 55% fewer failed recovery attempts and achieve 71% better success rates in their recovery testing procedures. Companies implementing comprehensive business continuity frameworks that leverage AI for predictive analysis report 47% better risk mitigation capabilities and maintain 92% higher confidence in their recovery procedures. Furthermore, organizations utilizing IBM's advanced recovery tools demonstrate 64% better alignment with their established recovery time objectives and achieve 59% more efficient resource utilization during recovery scenarios (Khan, T. and Henderson, D. 2024).

Table 4. Cloud Migration Best Practices and Success Metrics (Cogent Infotech. 2024; Tasmiha Khan and Dina Henderson. 2024)

Practice Area	Success Rate (%)	Efficiency Gain (%)	Risk Reduction (%)	Time Saved (months)
Edge Computing	73	52	41	4.2
AI-Driven Assessment	64	57	53	3.8
Hybrid Infrastructure	87	46	38	3.1
Security Framework	82	61	64	2.5
Automated Monitoring	79	55	47	2.8

Integration of Cloud-Native Practices

The adoption of cloud-native practices has become increasingly critical for successful AWS migrations, with Flexera's 2024 State of the Cloud Report revealing that 87% of enterprises now have a multi-cloud strategy, while 72% are pursuing a hybrid cloud approach. The research indicates that container adoption continues to grow, with 95% of organizations either using or experimenting with containers in their development environments. Furthermore, the study shows that enterprises implementing cloud-native technologies report an average of 33% in cost savings through improved resource utilization, while 65% of organizations plan to increase their container usage in the coming year. Most notably, the report highlights that 84% of enterprises are now focusing on FinOps practices to optimize their cloud spending and resource allocation (Luxner, T. 2024).

Containerization has emerged as a fundamental component of cloud-native transformation, with CNCF's State of Cloud Native Development Report indicating that the global cloud-native developer population has grown to 6.8 million, representing a 1.8x increase in just two years. The

analysis reveals that Kubernetes has become the de facto standard for container orchestration, with 5.6 million developers using Kubernetes worldwide. Organizations implementing container orchestration platforms report 47% faster application deployment cycles and achieve 53% better resource utilization. The research also shows that 4.6 million developers are now using container registries, demonstrating the widespread adoption of containerized development practices (Kulkarni, A. 2022).

The implementation of serverless architectures has shown significant growth, as Flexera's research demonstrates that 74% of enterprises are now using or experimenting with serverless computing. The study reveals that organizations leveraging serverless technologies experience an average reduction of 40% in operational overhead costs, while 61% report improved scalability for their applications. The analysis indicates that serverless adoption is particularly strong in enterprises with mature cloud practices, where 82% of organizations utilize serverless computing for at least one critical application. Additionally, the report shows that 69% of companies plan to

increase their serverless computing usage in the next year, driven by the benefits of reduced infrastructure management and improved cost efficiency (Luxner, T. 2024). Cloud-native development practices have become increasingly sophisticated, with CNCF's analysis showing that 60% of backend developers are now using containers as their primary deployment technology. The research indicates that organizations implementing microservices architectures experience 31% better application maintainability and achieve 42% faster feature delivery times. The study reveals that service mesh adoption has grown by 50% among cloud-native developers, while 27% of backend developers are actively using service mesh technologies in production environments. Furthermore, the analysis shows that 30% of developers are now working with both containers and serverless technologies, indicating a growing trend toward hybrid deployment approaches (Kulkarni, A. 2022). DevOps practices and automation have become central to cloud-native success, with Flexera's findings indicating that 90% of enterprises are implementing DevOps practices to some degree. The research shows that organizations with mature DevOps practices achieve 45% faster time to market for new features and maintain 56% better deployment success rates. The study reveals that 78% of enterprises are increasing their investment in automation tools and practices, while 71% report that automated deployment processes have significantly reduced their operational errors. Additionally, the report indicates that 83% of organizations consider DevOps expertise crucial for their cloud initiatives, with 67% planning to expand their DevOps teams in the coming year (Tanner Luxner. 2024).

The adoption of cloud-native technologies continues to evolve, as CNCF's research shows significant growth in the usage of complementary tools and practices. The study reveals that 54% of developers are using service mesh technologies, while 31% are implementing WebAssembly modules in their cloud-native applications. The analysis indicates that organizations implementing comprehensive observability solutions achieve 38% better system reliability and maintain 44% higher availability rates. The research also highlights that 41% of developers are now using GitOps practices for deployment management, while 36% have implemented chaos engineering practices to improve system resilience (Aditya Kulkarni. 2022).

CONCLUSION

The complexity of enterprise AWS cloud migration necessitates a strategic approach that balances technical requirements with organizational readiness and security considerations. Organizations achieving successful migrations demonstrate strong commitment to comprehensive planning, security-first implementations, and continuous optimization practices. The adoption of cloud-native technologies emerges as a fundamental driver of migration success, enabling improved scalability, reduced operational overhead, and enhanced development efficiency. Security remains paramount throughout the migration journey, with successful organizations implementing robust controls, maintaining compliance standards, and continuously enhancing their security posture. Post-migration optimization plays a vital role in realizing the full benefits of cloud adoption, encompassing resource utilization, cost management, and performance enhancement. The integration of DevOps practices and automation frameworks significantly impacts deployment efficiency and operational excellence. As cloud technologies continue evolving, organizations must maintain focus on security, optimization, and cloud-native adoption to maximize their AWS migration benefits while ensuring robust protection of critical assets and data. The establishment of clear success metrics, implementation of comprehensive monitoring solutions, and adoption of best practices in cloud security and operations ensure sustained success in cloud environments. Through careful consideration of these elements and commitment to continuous improvement, organizations can achieve transformative benefits from their AWS cloud adoption initiatives.

REFERENCES

1. Stewart, D., Okubo, N., Jehu, P., & Liu, M. "The cloud migration forecast: Cloudy with a chance of clouds—TMT Predictions 2021." *Deloitte Insights*, December 7 (2020).
2. Kumar, N. "Cloud migration vs modernization – What's the difference?," *eG Innovations*, (2024). [Online]. Available: <https://www.eginnovations.com/blog/cloud-migration-vs-modernization-whats-the-difference/>
3. Tunggal, A. T. "What is the Cost of Data Breach in 2023?," *UpGuard*, (2025). [Online]. Available: [https://www.upguard.com/blog/cost-of-data-breach#:~:text=In%202023%2C%20the%20average%20cost,\(US%24%204.35%20million\).](https://www.upguard.com/blog/cost-of-data-breach#:~:text=In%202023%2C%20the%20average%20cost,(US%24%204.35%20million).)

4. Sadon, S and Galea, D. "2024 State of Cloud Security Report Shows That More Risk Prioritization is Needed," *Orca.Security*, (2024). [Online]. Available: <https://orca.security/resources/blog/2024-state-public-cloud-report-risk-prioritization/>
5. Harris, F. "Key Findings from the 2024 Cloud Security Report," *Fortinet*, (2024). [Online]. Available: <https://www.fortinet.com/blog/industry-trends/key-findings-cloud-security-report-2024>
6. Gaydos, B. "Cloud Migration Strategies: Why You're Failing" *DuploCloud*, (2024). [Online]. Available: <https://duplocloud.com/blog/helpful-resources/cloud-migration-strategies-why-youre-failing/#:~:text=Why%20Cloud%20Migration%20Strategies%20Fail,inadequate%20testing%2C%20and%20insufficient%20budgeting.>
7. Arkitech Group, "Cloud Cost Optimization: Key Insights from the 2024 ESR Report," (2024). [Online]. Available: <https://blog.arkitechgroup.com/cloud-cost-optimization-key-insights-from-the-2024-esr-report>
8. Granica, "Cloud Optimization Trends: 2024 and Beyond," (2024). [Online]. Available: <https://granica.ai/resources/cloud-optimization-trends-grc>
9. Cogent Infotech, "2024 Predictions: Mass Migration From The Cloud To The Edge," (2024). [Online]. Available: <https://www.cogentinfo.com/resources/2024-predictions-mass-migration-from-the-cloud-to-the-edge>
10. Khan, T and Henderson, D. "Cloud migration best practices: Optimizing your cloud migration strategy," *IBM*, (2024). [Online]. Available: <https://www.ibm.com/think/insights/cloud-migration-strategy#:~:text=Use%20IBM%20Watson's%20AI%20or,flow%20of%20goods%20and%20services>
11. Luxner, T. "Cloud computing trends: Flexera 2024 State of the Cloud Report," *Flexera*, (2024). [Online]. Available: <https://www.flexera.com/blog/finops/cloud-computing-trends-flexera-2024-state-of-the-cloud-report/>
12. Kulkarni, A. "CNCF Publishes State of Cloud Native Development Report," *InfoQ*, (2022). [Online]. Available: <https://www.infoq.com/news/2022/01/cncf-state-of-cloud-native/>

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Boinpally, D. " Navigating Enterprise AWS Cloud Migration: Security, Failures, and Optimization." *Sarcouncil Journal of Multidisciplinary* 5.7 (2025): pp 38-45.