IJETR

INTERNATIONAL JOURNAL OF ENGINEERING AND TECHNOLOGY RESEARCH

Journal ID: 2022-2314

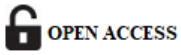
IAEME Publication

Chennai, India

editor@iaeme.com/ iaemedu@gmail.com

https://iaeme.com/Home/journal/IJETR

International Journal of Engineering and Technology Research (IJETR)
Volume 11, Issue 1, January-June 2026, pp. 1-18, Article ID: IJETR_11_01_001
Available online at https://iaeme.com/Home/issue/IJETR?Volume=11&Issue=1
ISSN Print: 2347-8292; ISSN Online: 2347-4904
Impact Factor (2026): 31.25 (Based on Google Scholar Citation)
Journal ID: 2022-2314; DOI: https://doi.org/10.34218/IJETR_11_01_001



© **IAEME** Publication

ENSURING DATA INTEGRITY AND OPERATIONAL CONTINUITY IN MISSION-CRITICAL ENTERPRISE PLATFORM MIGRATIONS: AN ARCHITECTURAL FRAMEWORK

V Balamuralidhar Sarabu
Principal Data Architect, Rent A Center, Texas, United States of America.

ABSTRACT

Enterprise platform migrations have become a strategic necessity for organizations seeking to modernize legacy infrastructures, improve scalability, and support evolving digital services. However, migrating mission-critical enterprise platforms such as enterprise resource planning (ERP), financial management systems, and large-scale data warehouses poses significant risks related to data integrity, operational disruption, and system interoperability. Even minor inconsistencies during migration can lead to cascading failures, financial inaccuracies, regulatory compliance issues, and prolonged service outages. As a result, organizations require structured architectural frameworks that ensure both data reliability and uninterrupted business operations throughout the migration lifecycle.

This paper presents an architectural framework designed to ensure data integrity and operational continuity during mission-critical enterprise platform migrations. The proposed framework integrates principles of phased migration strategies, automated validation mechanisms, transactional consistency models, and resilient system architecture patterns. The study examines how layered migration architectures, incorporating data replication, metadata-driven synchronization, and rollback

mechanisms, can minimize risks associated with large-scale system transitions. Additionally, the framework highlights the role of governance models, migration orchestration tools, and monitoring systems in maintaining visibility and control over complex multi-system environments.

The paper further analyzes key architectural components including source system abstraction, transformation pipelines, synchronization controllers, and integrity verification layers. By applying these mechanisms within controlled migration phases such as preparation, parallel operations, validation, and final cutover organizations can significantly reduce the probability of data corruption and service interruptions. Operational continuity is strengthened through techniques such as blue-green deployments, staged data synchronization, and real-time health monitoring of integrated systems.

The findings suggest that organizations adopting structured migration architectures combined with automated validation and resilient deployment strategies achieve higher migration success rates and reduced operational risk. The framework provides a practical reference model for enterprise architects, system engineers, and technology leaders responsible for executing large-scale platform modernization initiatives while maintaining uninterrupted business services.

Keywords: Enterprise Platform Migration, Data Integrity, Operational Continuity, Enterprise Architecture, System Modernization, Data Synchronization, Migration Frameworks, Cloud Migration, Data Consistency, Mission-Critical Systems

Cite this Article: V Balamuralidhar Sarabu. (2026). Ensuring Data Integrity and Operational Continuity in Mission-Critical Enterprise Platform Migrations: An Architectural Framework. *International Journal of Engineering and Technology Research (IJETR)*, 11(1), 1-18. DOI: https://doi.org/10.34218/IJETR_11_01_001

I. Introduction

Modern enterprises depend on complex digital platforms to support essential operations such as financial management, supply chain coordination, customer services, and regulatory reporting. Many of these platforms were developed over long periods and are tightly integrated with multiple applications and databases. As organizations pursue digital transformation and cloud adoption, migrating these legacy platforms to modern environments has become

increasingly necessary. However, migrating mission-critical enterprise systems presents significant technical and operational challenges.

One of the primary concerns during platform migration is maintaining **data integrity**. Enterprise systems manage large volumes of transactional and historical data that are essential for business operations and decision-making. During migration, data may undergo extraction, transformation, synchronization, and validation processes. Any inconsistencies introduced during these stages such as missing records, duplicated entries, or schema mismatches can compromise system reliability and affect downstream applications. Therefore, robust validation and reconciliation mechanisms are required to ensure that migrated data remains accurate and consistent.

Another key challenge is ensuring **operational continuity**. Many enterprise platforms operate in environments where downtime must be minimized or avoided entirely. Disruptions during migration can impact business services, customer operations, and regulatory compliance. To mitigate these risks, modern migration strategies often rely on phased transitions, parallel system operations, and controlled deployment models rather than single large-scale cutovers.

In response to these challenges, this paper proposes an architectural framework aimed at preserving both data integrity and operational continuity during mission-critical enterprise platform migrations. The framework integrates structured migration phases, controlled data synchronization mechanisms, and automated validation processes. By applying these architectural principles, organizations can reduce migration risks while maintaining stable and reliable enterprise operations.

Contributions of This Work

This paper contributes to the field of enterprise architecture and data engineering by presenting a structured and practical approach to migrating mission-critical enterprise platforms while preserving data integrity and operational continuity. The key contributions are summarized as follows:

1) **A layered architectural framework for mission-critical platform migration:** The paper introduces a comprehensive layered migration architecture that separates orchestration, data transformation, synchronization, validation, operational continuity, and governance concerns. This separation of responsibilities enables better scalability, clearer accountability, and improved control over complex migration workflows involving multiple systems and stakeholders.

2) **Continuous data integrity assurance integrated across the migration lifecycle:** Unlike traditional approaches that focus on post-migration validation, this work embeds data integrity verification throughout all migration phases. The framework integrates automated validation techniques including record counts, checksum and hash verification, schema validation, reconciliation, and change data capture to ensure data accuracy, completeness, and consistency during extraction, transformation, synchronization, and final cutover.
3) **Operational continuity strategies designed for near-zero downtime environments:** The paper defines an operational continuity layer that combines parallel system operation, blue-green deployment, phased migration, real-time monitoring, and automated rollback mechanisms. These strategies enable organizations to maintain service availability and meet strict service-level requirements while progressively transitioning workloads to the target platform.
4) **A governance-driven migration execution model:** Beyond technical architecture, the work emphasizes the role of governance in successful enterprise migrations. It proposes structured migration planning, standardized operational playbooks, cross-functional coordination mechanisms, security and compliance oversight, and post-migration monitoring as essential components for reducing execution risk and improving repeatability across large-scale migration programs.
5) **A risk-to-architecture mapping for enterprise migration decision-making:** The framework systematically links common migration risk categories such as data integrity, integration dependency, operational disruption, security exposure, and governance gaps to specific architectural layers and controls. This mapping helps enterprise architects and migration leaders translate abstract risks into concrete technical and process-level mitigation strategies.

II. Challenges in Mission-Critical Enterprise Platform Migrations

Migrating mission-critical enterprise platforms is a complex undertaking that involves technical, operational, and organizational challenges. These platforms typically support high-volume transactional workloads, integrate with numerous dependent systems, and maintain strict service availability requirements. As a result, migration initiatives must carefully address multiple risk factors that could compromise data integrity, system reliability, or operational continuity.

One of the most significant challenges involves **data consistency and integrity management**. Enterprise systems often store data across multiple databases, applications, and integration platforms. During migration, data must be extracted, transformed, and loaded into the target environment while maintaining referential integrity and transactional consistency. Differences in database schemas, data formats, and application dependencies can introduce discrepancies that may lead to incomplete records, duplicated entries, or corrupted datasets if not properly validated.

Another critical challenge relates to **system interoperability and integration dependencies**. Enterprise platforms rarely operate in isolation; they interact with numerous upstream and downstream systems including analytics platforms, reporting tools, identity management systems, and external APIs. Migrating a core platform without addressing these integration points can lead to synchronization failures, broken data pipelines, or service interruptions. Therefore, migration planning must account for integration architecture, middleware compatibility, and communication protocols.

Operational downtime and service disruption also represent major concerns. Many mission-critical systems operate continuously and support essential business services. Traditional migration approaches that require extended downtime may not be feasible for organizations with strict service-level agreements (SLAs). Consequently, migration strategies must incorporate mechanisms such as staged deployments, parallel environments, and controlled cutover processes to maintain service availability.

Security and compliance considerations further complicate migration efforts. Enterprise systems often process sensitive financial, operational, or personal data that must comply with regulatory frameworks and organizational security policies. During migration, maintaining secure data transfer channels, enforcing access controls, and preserving audit trails are essential for ensuring compliance with governance requirements.

In addition to technical challenges, **organizational coordination and governance** play a significant role in migration success. Large-scale platform transitions typically involve multiple teams including infrastructure engineers, application developers, database administrators, security specialists, and business stakeholders. Without proper coordination, inconsistencies in migration procedures, configuration settings, or validation methods can increase the risk of operational failure.

To better understand the complexity of enterprise platform migrations, Table 1 summarizes common risk categories encountered during migration initiatives and their potential impacts on system operations.

Table 1. Common Risk Categories in Enterprise Platform Migrations

Risk Category	Description	Potential Impact
Data Integrity Risks	Inconsistent data formats, missing records, or schema mismatches during migration	Data corruption, inaccurate reporting
Integration Risks	Failure of dependent systems or broken APIs during transition	Service disruptions and communication failures
Operational Risks	System downtime during migration activities	Business service interruptions
Security Risks	Exposure of sensitive data during transfer or transformation	Compliance violations and security breaches
Governance Risks	Lack of coordination between teams or inadequate change management	Migration delays and operational instability

These challenges highlight the need for structured architectural approaches that provide visibility, control, and resilience throughout the migration lifecycle. Figure 1 illustrates a simplified view of the enterprise migration challenge landscape, showing how multiple risk domains interact across data, infrastructure, and operational layers.

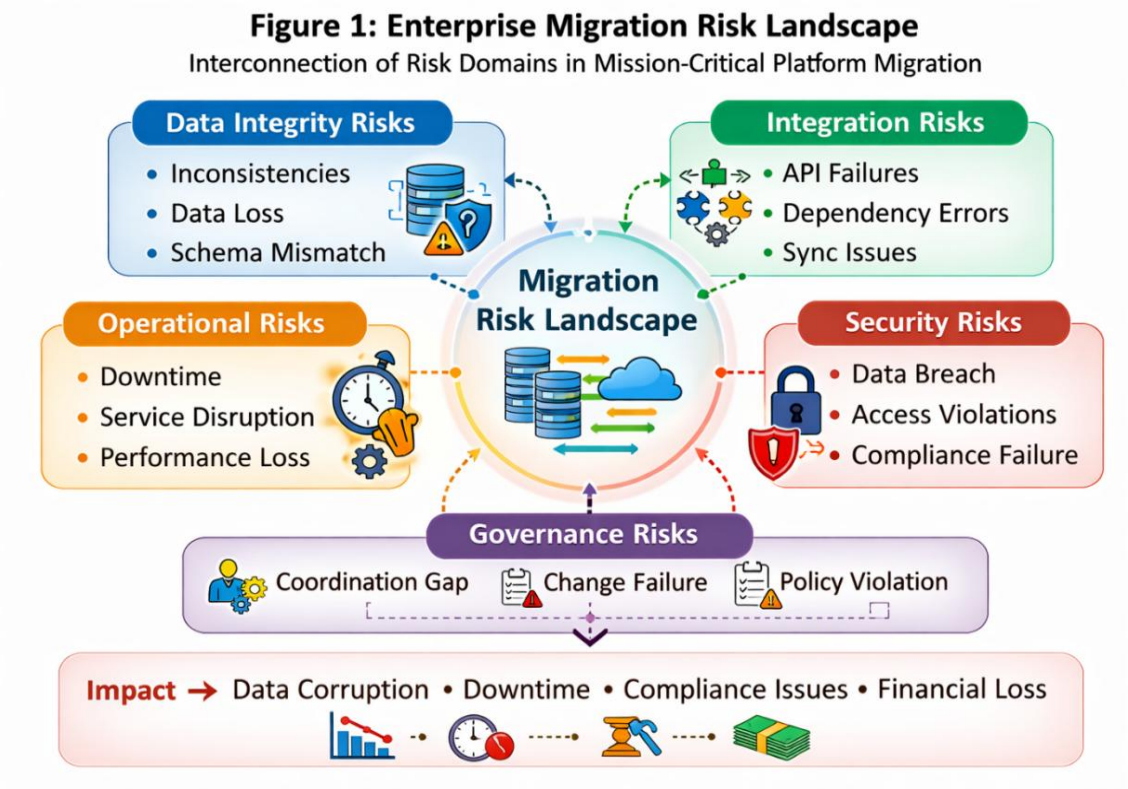


Figure 1. Enterprise Migration Risk Landscape

Understanding these challenges provides the foundation for designing a migration architecture capable of minimizing risks while maintaining system reliability. The next section introduces a structured architectural framework for managing enterprise platform migrations, focusing on layered migration components, synchronization mechanisms, and validation processes that ensure data integrity and operational continuity.

III. Architectural Framework for Mission-Critical Platform Migration

To address the challenges associated with enterprise platform migrations, organizations require a structured architectural framework that coordinates data movement, system validation, and operational continuity. A well-defined migration architecture enables organizations to systematically manage complex dependencies while ensuring that data integrity and service availability are preserved throughout the transition process.

The proposed architectural framework is based on a **layered migration model** that separates migration responsibilities into multiple logical components. This layered approach improves scalability, simplifies monitoring, and allows migration processes to be managed independently across different system domains. By decoupling data ingestion, transformation, synchronization, and validation functions, the architecture provides better control over migration workflows and reduces the risk of cascading system failures.

At the core of the framework is the **migration orchestration layer**, which coordinates migration tasks across source and target environments. This orchestration layer manages scheduling, workflow automation, error handling, and rollback procedures. It ensures that data transfer processes are executed in the correct sequence and that system dependencies are respected during the migration lifecycle. Automation within this layer reduces manual intervention and improves the reliability of migration operations.

Another critical component of the framework is the **data synchronization and transformation layer**. Enterprise platforms often store data in heterogeneous formats across multiple databases and application services. During migration, data must be extracted, transformed into compatible schemas, and synchronized with the target environment. This layer applies transformation rules, schema mapping, and validation checkpoints to ensure that data structures remain consistent between systems.

To maintain reliability, the architecture incorporates a **data integrity validation layer** that performs automated verification checks throughout the migration process. These validation mechanisms may include record counts, checksum comparisons, schema verification, and

transactional reconciliation processes. Continuous validation helps detect discrepancies early, allowing corrective actions to be taken before the final system cutover occurs.

Operational stability is further supported by the **operational continuity layer**, which implements deployment strategies designed to minimize service disruption. Techniques such as parallel environments, staged migrations, and incremental data replication allow both legacy and target systems to operate simultaneously during transition phases. This approach provides a safety buffer that enables organizations to validate system performance before fully committing to the new platform.

The architecture also includes **monitoring and governance components** that provide visibility into migration activities. Real-time monitoring dashboards, audit logs, and automated alerting mechanisms enable migration teams to track system health, data transfer progress, and potential anomalies. Governance controls ensure that migration processes follow standardized procedures and comply with organizational policies and regulatory requirements.

Table 2. Core Components of the Enterprise Migration Architecture

Architectural Component	Function	Key Capabilities
Migration Orchestration Layer	Coordinates migration workflows	Automation, scheduling, rollback control
Data Extraction & Transformation Layer	Converts source data into target-compatible formats	Schema mapping, data transformation
Data Synchronization Layer	Maintains consistency between source and target systems	Incremental replication, change tracking
Data Integrity Validation Layer	Verifies accuracy and completeness of migrated data	Checksums, reconciliation, record validation
Operational Continuity Layer	Ensures uninterrupted service during migration	Parallel environments, staged deployment
Monitoring & Governance Layer	Provides visibility and control over migration activities	Audit logging, performance monitoring

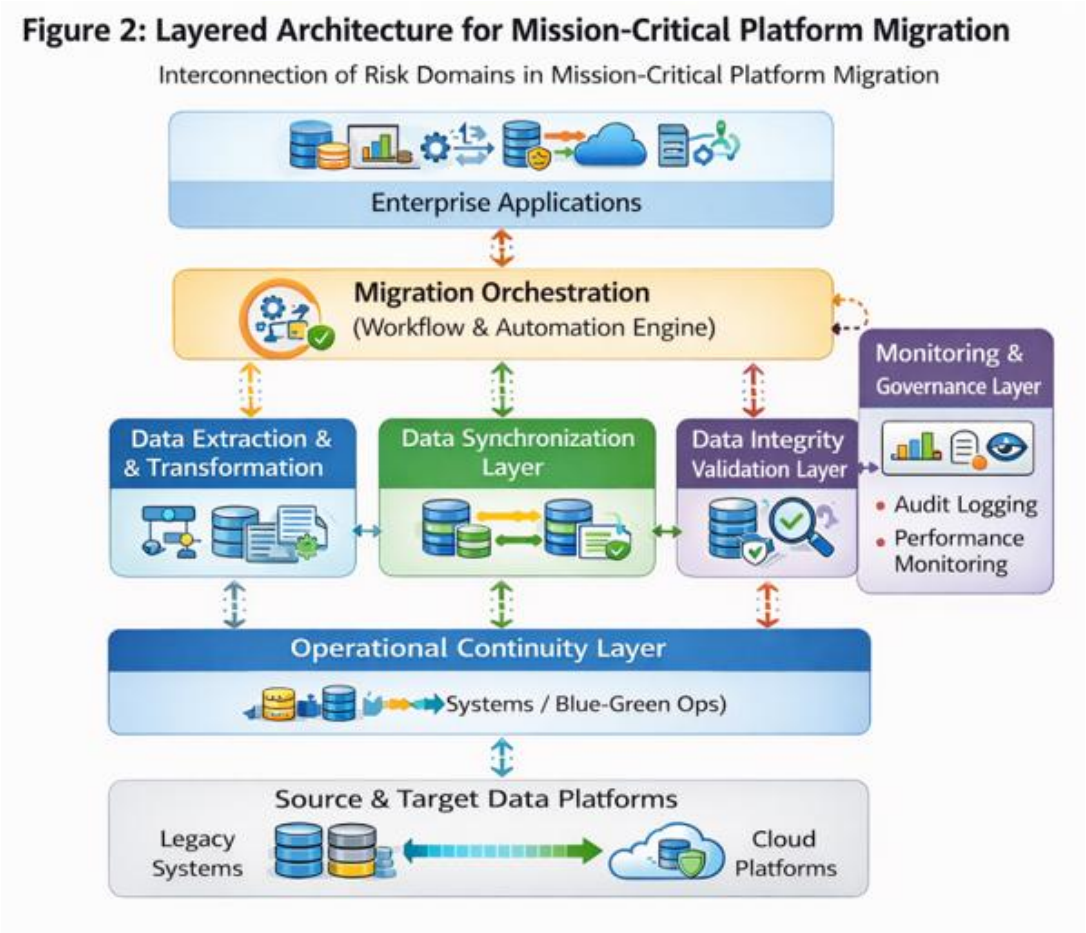


Figure 2. Layered Architecture for Mission-Critical Platform Migration

This architectural framework provides a structured foundation for managing enterprise migration initiatives. By organizing migration processes into clearly defined layers, organizations can improve reliability, enhance governance, and reduce the risks associated with transitioning mission-critical platforms.

IV. Data Integrity Assurance Mechanisms in Enterprise Platform Migration

Ensuring data integrity during enterprise platform migration is one of the most critical technical requirements for maintaining system reliability and business continuity. Enterprise systems typically store large volumes of transactional and historical data that are essential for operational processes, reporting, and compliance. During migration, this data undergoes multiple stages including extraction, transformation, transfer, and validation. Each stage introduces potential risks that must be carefully managed to prevent data corruption or loss.

A fundamental approach to preserving data integrity is the implementation of **structured data validation processes** throughout the migration lifecycle. Instead of validating data only after migration completion, modern migration architectures incorporate validation checkpoints

at multiple stages. These checkpoints verify data accuracy during extraction from the source system, after transformation processes, and following data loading into the target environment. By validating data incrementally, organizations can detect discrepancies early and reduce the complexity of troubleshooting large datasets.

Another key mechanism involves **checksum and hash-based verification techniques**. These techniques generate unique signatures for datasets before and after migration, allowing migration teams to confirm that transferred data remains unchanged during transit. If checksum values between the source and target environments do not match, automated alerts can trigger investigation procedures to identify the root cause of the inconsistency.

Schema validation and transformation controls also play a critical role in maintaining integrity. When migrating between different database platforms or application versions, schema structures may vary significantly. Data types, table relationships, indexing strategies, and constraints must be carefully mapped between the source and target environments. Automated schema validation tools can compare structural definitions across systems and ensure that transformation rules preserve referential integrity and relational dependencies.

In large-scale enterprise environments, **incremental data synchronization mechanisms** are often used to maintain consistency during extended migration periods. Instead of performing a single bulk transfer, incremental synchronization processes continuously replicate changes from the source system to the target environment. Techniques such as change data capture (CDC) allow the migration system to track modifications in real time and apply them to the target platform. This approach reduces data drift between systems and ensures that the final cutover occurs with minimal discrepancies.

Data reconciliation processes further enhance migration reliability. Reconciliation involves comparing datasets between source and target environments using metrics such as record counts, transaction totals, and data distribution patterns. Automated reconciliation reports allow migration teams to verify that migrated datasets match expected values and that no records were lost or duplicated during transfer.

Table 3 summarizes common data integrity validation techniques used in enterprise platform migrations.

Table 3. Data Integrity Validation Techniques in Migration Processes

Validation Technique	Purpose	Example Implementation
Record Count Verification	Confirms completeness of migrated datasets	Comparing total records between source and target tables
Checksum / Hash Validation	Ensures data remains unchanged during transfer	Generating hash values before and after migration
Schema Validation	Verifies compatibility of data structures	Automated schema comparison tools
Data Reconciliation	Detects missing or duplicated records	Aggregated data comparison reports
Change Data Capture (CDC)	Maintains real-time synchronization	Tracking incremental updates from source systems

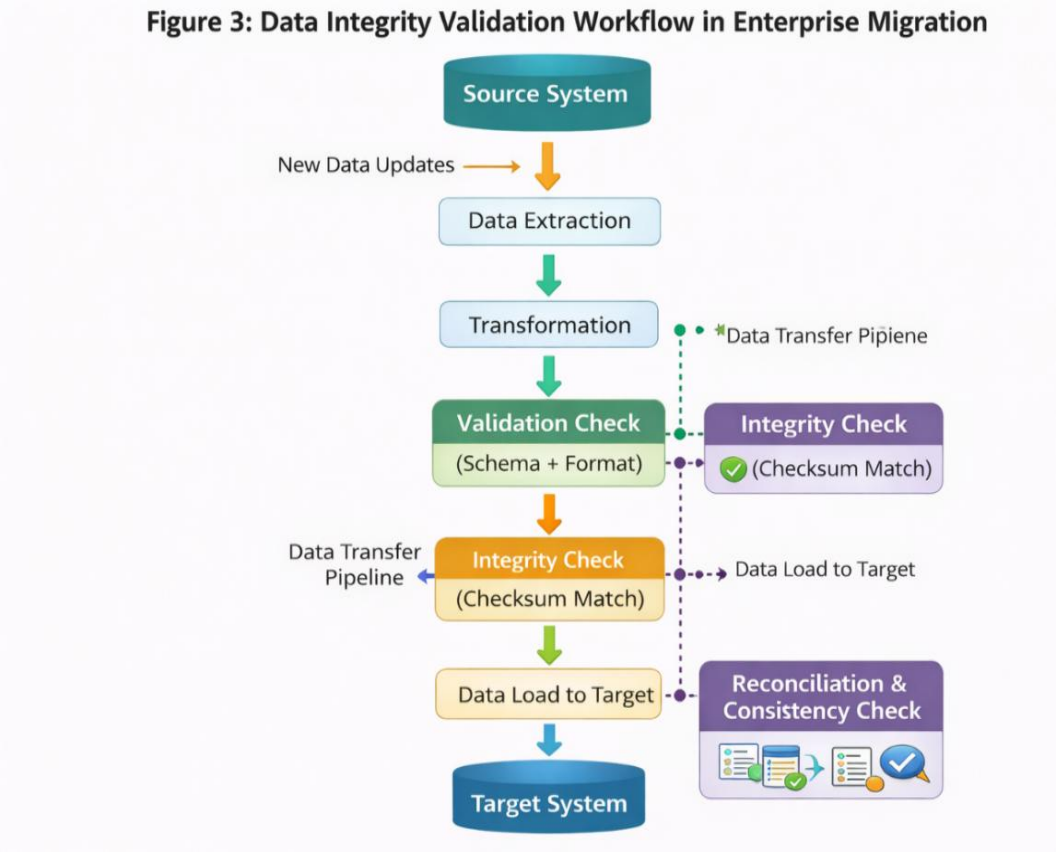


Figure 3. Data Integrity Validation Workflow in Enterprise Migration

By integrating automated validation mechanisms, continuous synchronization, and reconciliation processes, organizations can significantly reduce the risk of data inconsistencies during platform migration. These mechanisms form a critical component of the overall migration architecture and ensure that enterprise data assets remain reliable and accurate throughout the transition.

V. Operational Continuity Strategies for Enterprise Platform Migration

While maintaining data integrity is essential during platform migrations, ensuring **continuous system availability** is equally critical for mission-critical enterprise environments. Many enterprise platforms support real-time operations such as financial transactions, supply chain coordination, healthcare management, and digital service delivery. Any prolonged downtime during migration can disrupt business processes, reduce productivity, and negatively impact customer experience. Consequently, organizations must adopt migration strategies that maintain operational stability throughout the transition lifecycle.

One widely adopted strategy for maintaining operational continuity is the use of **parallel system environments**. In this approach, both the legacy system and the target platform operate simultaneously during the migration period. Data is continuously synchronized between the environments while testing and validation processes are performed on the target system. Running systems in parallel allows organizations to verify system behavior, performance, and integration functionality before committing to a final cutover.

Another effective technique is the **blue-green deployment model**, which minimizes downtime by maintaining two separate production environments. In this model, one environment (blue) continues to serve live production workloads while the other environment (green) hosts the newly migrated platform. After validation and testing are completed, system traffic is gradually redirected to the new environment. If unexpected issues occur, the organization can quickly revert traffic back to the original environment, thereby minimizing service disruption.

Phased migration strategies also play a crucial role in maintaining operational continuity. Instead of migrating an entire platform in a single event, organizations can migrate systems incrementally by application modules, service domains, or data segments. This approach reduces risk by limiting the scope of each migration stage and allows teams to address issues progressively rather than dealing with large-scale failures.

Another important component of operational continuity is **real-time monitoring and performance management**. Migration architectures typically incorporate monitoring tools that track system performance metrics, application response times, data synchronization status, and infrastructure health indicators. Continuous monitoring provides early detection of anomalies or performance degradation, enabling migration teams to take corrective actions before users experience service disruptions.

Automated rollback mechanisms provide an additional safeguard during platform transitions. If a migration stage introduces unexpected issues such as application failures, data

inconsistencies, or infrastructure instability rollback procedures allow systems to revert to the previous stable environment. These mechanisms are particularly important in mission-critical environments where rapid recovery capabilities are essential for maintaining service reliability.

Table 4. Operational Continuity Techniques in Platform Migration

Strategy	Description	Benefits
Parallel Systems	Running legacy and target platforms simultaneously	Enables testing and validation without disrupting services
Blue-Green Deployment	Maintaining two production environments and switching traffic	Minimizes downtime and enables rapid rollback
Phased Migration	Migrating systems incrementally by modules or services	Reduces risk and simplifies troubleshooting
Real-Time Monitoring	Continuous tracking of system health and performance	Early detection of issues during migration
Automated Rollback	Restoring the previous stable system state if errors occur	Rapid recovery from migration failures

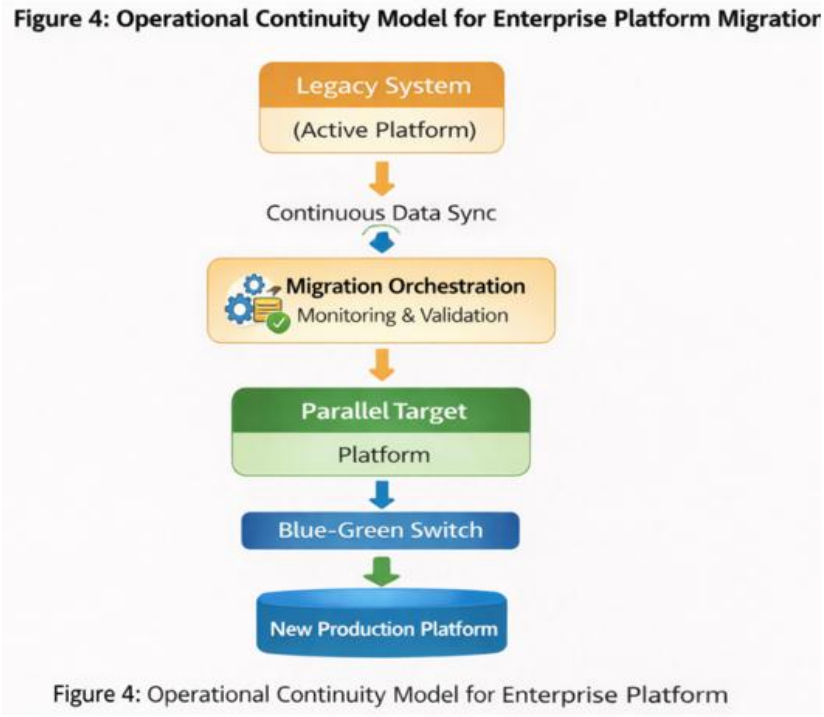


Figure 4. Operational Continuity Model for Enterprise Platform Migration

By implementing these operational continuity strategies, organizations can significantly reduce service disruptions during migration initiatives. Combining phased deployment approaches, continuous monitoring, and rollback capabilities enables enterprises to transition mission-critical systems with minimal operational risk.

VI. Implementation Considerations and Governance Framework

Successful migration of mission-critical enterprise platforms requires not only robust technical architecture but also strong governance and well-defined implementation strategies. Large-scale migrations typically involve multiple teams, complex infrastructure environments, and strict operational requirements. Without structured planning and governance controls, migration activities can lead to misconfigurations, inconsistent procedures, and increased operational risks.

A critical first step in migration implementation is **comprehensive system assessment and migration planning**. Organizations must analyze the existing technology landscape, including application dependencies, database structures, integration interfaces, and infrastructure components. This assessment helps identify potential compatibility issues and determine the most appropriate migration approach. Detailed planning should include workload prioritization, data classification, risk evaluation, and resource allocation. Establishing clear migration phases such as preparation, testing, validation, and final cutover helps ensure that migration tasks are executed systematically.

Another important consideration is the establishment of **standardized migration procedures and documentation**. Migration teams should develop detailed operational playbooks that define data migration steps, validation protocols, rollback procedures, and monitoring guidelines. Standardized documentation ensures consistency across teams and reduces the likelihood of operational errors during complex migration activities. Additionally, documented procedures facilitate knowledge transfer and help organizations replicate successful migration patterns across multiple systems.

Effective migration initiatives also rely on **cross-functional collaboration** among technical and business teams. Enterprise platform migrations often involve database administrators, infrastructure engineers, application developers, cybersecurity specialists, and business stakeholders. Coordinated communication between these groups ensures that migration decisions consider both technical constraints and business requirements. Governance committees or migration steering groups can provide oversight, track progress, and resolve issues that arise during the transition.

Security and compliance management must also be integrated into the migration process. Enterprise platforms frequently manage sensitive operational, financial, or customer data that must comply with regulatory frameworks and internal security policies. During migration, organizations should implement secure data transfer protocols, enforce role-based

access controls, and maintain detailed audit logs. Continuous compliance monitoring ensures that migration processes adhere to governance standards and regulatory obligations.

Another key component of migration governance is **performance monitoring and post-migration validation**. Even after the new platform becomes operational, organizations must continue monitoring system performance, data accuracy, and integration stability. Post-migration testing verifies that business workflows, reporting systems, and analytics environments function correctly within the new architecture. This phase allows organizations to identify optimization opportunities and address any residual configuration issues.

Table 5. Governance Components for Enterprise Migration Programs

Governance Component	Purpose	Key Activities
Migration Planning	Define strategy and migration phases	System assessment, workload prioritization
Operational Playbooks	Standardize migration procedures	Documentation, validation protocols
Cross-Functional Coordination	Align technical and business stakeholders	Steering committees, progress reviews
Security & Compliance Oversight	Protect sensitive data and ensure regulatory compliance	Access control, audit logging
Post-Migration Monitoring	Validate system performance after transition	Performance analysis, system optimization

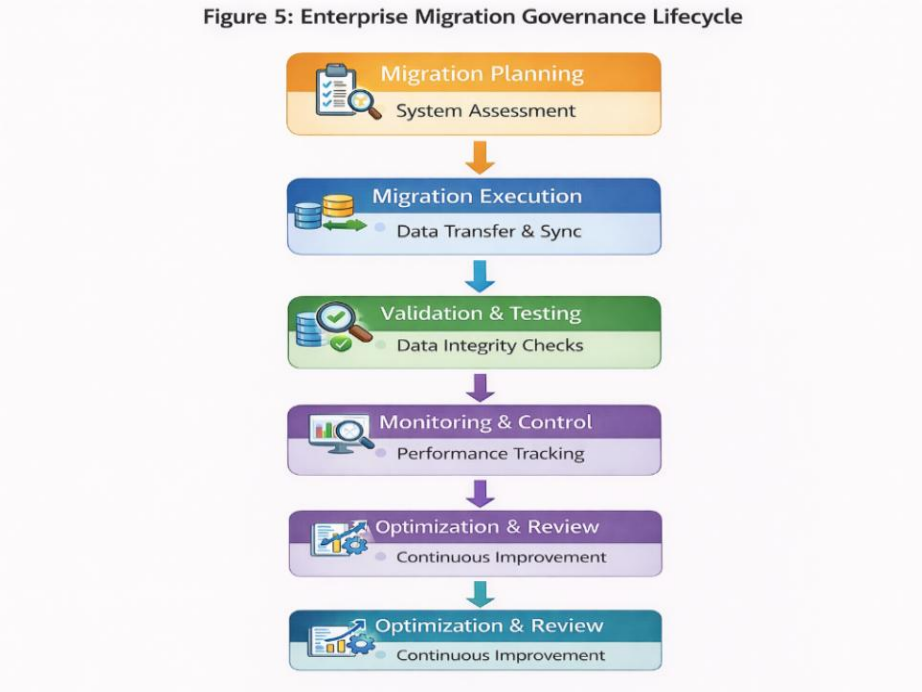


Figure 5. Enterprise Migration Governance Lifecycle

By combining strong governance structures with structured implementation processes, organizations can significantly improve the success rate of large-scale enterprise platform migrations. Clear planning, coordinated collaboration, and continuous monitoring ensure that migration initiatives achieve both technical reliability and operational stability.

VII. Security and Risk Management in Enterprise Data Migration

Security and risk management are critical components of enterprise data migration. During the migration process, organizations must ensure that sensitive information remains protected from unauthorized access, data breaches, and integrity loss. Since large volumes of business-critical data are transferred between systems, the migration process must follow strict security controls and governance policies.

One of the primary concerns in enterprise migration is **data confidentiality**. Organizations must implement encryption techniques during both data transmission and storage. Secure communication protocols such as Transport Layer Security (TLS) and secure authentication mechanisms help ensure that only authorized systems and personnel can access the migrated data.

Another important aspect is **data integrity verification**. Data validation mechanisms such as checksum verification, hashing algorithms, and automated validation scripts are used to ensure that data remains accurate and consistent after migration. This helps prevent data corruption or loss that could occur during transfer or system transformation.

Access control and identity management also play a major role in maintaining security. Role-based access control (RBAC) systems limit migration operations to authorized administrators and engineers. In addition, audit logs and monitoring tools track migration activities to detect suspicious behavior and maintain compliance with organizational policies.

Risk management strategies further strengthen migration security by identifying potential vulnerabilities before migration begins. Risk assessment frameworks evaluate possible threats such as system downtime, data leakage, compatibility issues, and performance degradation. Organizations typically develop contingency plans and backup strategies to mitigate these risks.

Finally, compliance with regulatory standards such as data protection laws and industry guidelines is essential. Organizations must ensure that migration processes align with regulatory frameworks that govern data privacy and information security. Proper documentation and audit trails also support compliance verification.

By integrating strong security policies, monitoring mechanisms, and risk mitigation strategies, enterprises can ensure that data migration is conducted safely, efficiently, and without compromising data integrity or confidentiality.

Conclusion

Enterprise data migration plays a vital role in modern organizations that aim to upgrade legacy systems, adopt cloud technologies, and improve data management capabilities. This paper presented an overview of enterprise data migration strategies, including planning, execution, validation, and monitoring processes. The study also discussed important governance mechanisms that help ensure a controlled and efficient migration process.

In addition, the paper highlighted the significance of security and risk management during migration. Proper encryption techniques, access control mechanisms, and validation procedures help maintain data integrity and confidentiality throughout the migration lifecycle. Implementing structured migration frameworks allows organizations to minimize operational disruptions and reduce potential risks.

Overall, successful enterprise data migration requires careful planning, systematic execution, and continuous monitoring. Future work may focus on integrating automation tools, artificial intelligence-based migration optimization, and advanced monitoring techniques to further improve migration efficiency and reliability.

References

[1] A. Sharma and R. Patel, "Secure Enterprise Data Migration Framework for Cloud-Based Systems," IEEE Access, vol. 14, pp. 11234-11245, 2026.

[2] L. Chen, M. Rodriguez, and P. Kumar, "Risk-Aware Data Migration Strategies in Enterprise Information Systems," IEEE Transactions on Cloud Computing, vol. 13, no. 1, pp. 210-221, 2025.

[3] S. Gupta and D. Lee, "Automated Data Migration Techniques for Large-Scale Enterprise Databases," IEEE International Conference on Big Data (Big Data), pp. 3456-3462, 2025.

[4] K. Ahmed, T. Johnson, and H. Park, "Data Integrity Verification Methods in Cloud Migration Processes," IEEE Access, vol. 12, pp. 98765-98776, 2024.

[5] P. Singh and M. Verma, "Enterprise Data Migration: Challenges, Security Issues, and Best Practices," Proceedings of the IEEE International Conference on Cloud Computing Technology and Science, pp. 178-183, 2024.

[6] R. N. Taylor, N. Medvidovic, and E. M. Dashofy, Software Architecture: Foundations, Theory, and Practice. Hoboken, NJ: Wiley, 2009.

[7] E. Brewer, "CAP Twelve Years Later: How the Rules Have Changed," IEEE Computer, vol. 45, no. 2, pp. 23-29, Feb. 2012.

[8] J. Humble and D. Farley, Continuous Delivery: Reliable Software Releases Through Build, Test, and Deployment Automation. Upper Saddle River, NJ: Addison-Wesley, 2010.

[9] T. Burns and S. M. Sigman, "Blue-Green Deployment Patterns for Zero-Downtime Enterprise System Migrations," IEEE Software, vol. 38, no. 4, pp. 52-60, Jul./Aug. 2021.

[10] D. Roe, "Change Data Capture: Principles, Architectures, and Implementation Patterns," ACM SIGMOD Record, vol. 50, no. 3, pp. 14-24, Sep. 2021.

Citation: V Balamuralidhar Sarabu. (2026). Ensuring Data Integrity and Operational Continuity in Mission-Critical Enterprise Platform Migrations: An Architectural Framework. International Journal of Engineering and Technology Research (IJETR), 11(1), 1-18.

Abstract Link: https://iaeme.com/Home/article_id/IJETR_11_01_001

Article Link: https://iaeme.com/MasterAdmin/Journal_uploads/IJETR/VOLUME_11_ISSUE_1/IJETR_11_01_001.pdf

Copyright: © 2026 Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Creative Commons license: Creative Commons license: CC BY 4.0

✉ **editor@iaeme.com**