The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 85-91
DOI 10.37547/tajet/Volume07Issue08-10

Check for updates

Risk Management and Compliance Strategies for Legacy IT Infrastructure

Yurii Shevchuk
Senior Full Stack Engineer and Cybersecurity Specialist, DataArt
New York, United State

OPEN ACCESS

SUBMITED 24 July 2025
ACCEPTED 27 July 2025
PUBLISHED 12 August 2025
VOLUME Vol.07 Issue 08 2025

CITATION

Yurii Shevchuk. (2025). Risk Management and Compliance Strategies for Legacy IT Infrastructure. The American Journal of Engineering and Technology, 7(8), 85–91. https://doi.org/10.37547/tajet/Volume07Issue08-10

Abstract: This article examines strategies for risk management and regulatory compliance in the context of modernizing legacy IT infrastructure. The relevance of the topic arises from the growing need to integrate new technological solutions in environments characterized by limited flexibility, high maintenance costs, and technical debt—factors that contribute to operational, technical, and regulatory risks. The study analyzes the current state of legacy infrastructure, identifies key threats and vulnerabilities, and develops methodological approaches including modular migration, AI-driven analytics, the adoption of cloud technologies, and the integration of advanced security measures to ensure compliance with regulatory frameworks such as GDPR and HIPAA.

The scientific novelty lies in proposing a new perspective on integrating strategic planning, change management, and modern security technologies to reduce operational costs and improve business resilience. This perspective emerged through a critical review of existing literature. The author's hypothesis suggests that a comprehensive approach to modernizing legacy IT infrastructure—grounded in modular transition to cloud solutions and automated security monitoring—will lead to a reduction in risk and an increase in the efficiency of business processes.

The findings of this study may be of interest to IT management professionals, risk and compliance officers, and researchers seeking to integrate the latest analytical methods into the evaluation and modernization of inherited IT systems. The presented material is also expected to be useful to other scholars developing theoretical models for managing complex IT environments, as well as to practitioners implementing strategies for mitigating operational and regulatory risks amid continuous technological and legal transformation.

Keywords: legacy IT infrastructure, risk management, regulatory compliance, cloud technologies, AI-driven analytics, modular migration, information security.

Introduction

The relevance of modernizing legacy IT infrastructure is driven by the rapid development of digital technologies, with the global digital transformation market having grown from $469.8 billion in 2020 to $1,009.8 billion by early 2025, reflecting an average annual growth rate of 16.5% [11]. Challenges related to technical debt, high maintenance costs of outdated systems, and the difficulty of integrating them with modern technologies necessitate the development of effective risk management and compliance strategies [1,2].

Contemporary literature on risk management and compliance strategies for IT infrastructure is characterized by a diversity of approaches that combine issues of technical modernization, data governance, and economic optimization. A number of studies, including works by Adepoju A. H. et al. [1], Kambala G. [2], Ponnusamy S., Eswararaj D. [9], and Eeti S., Renuka A. [10], propose comprehensive frameworks for migrating legacy systems to new architectural models, placing particular emphasis on seamless integration, scalability, and, as a result, the reduction of operational and information risks. This group of authors demonstrates that transitioning to cloud solutions and modern data models not only upgrades infrastructure but also creates mechanisms capable of meeting current security and regulatory compliance requirements.

Another research focus centers on developing strategies for data governance and quality. In this area, Adepoju A. H. et al. [3] propose a model aimed at reducing data redundancy and improving quality, directly impacting the mitigation of risks related to data breaches and errors. The study by Mishra S., Komandla V., and Bandi S. [7] introduces new paradigms in big data management through the concepts of Data Fabric and Data Mesh, which support more efficient data integration into corporate processes. Similarly, Machireddy J. R., Rachakatla S. K., and Ravichandran P. [8] justify the use of artificial intelligence and machine learning for building analytical systems that enable data-driven strategy development while maintaining compliance.

Equally significant is the technology-driven approach to IT environment transformation. Khang A. and Sivaraman K. A. [4] examine tools and applications in the fields of big data, cloud computing, and the Internet of Things (IoT), illustrating how these technologies support the modernization of legacy systems and the creation of more flexible infrastructure. Likewise, Onoja J. P., Ajala O. A., and Ige A. B. [5] explore the potential of artificial intelligence to transform community engagement processes. Although their focus is on social development, their work suggests that such innovative approaches can be adapted to enhance compliance and risk management within IT systems.

Finally, the economic aspects of modernization are examined in the work of Abbey A. B. N. et al. [6], where economic frameworks are developed to optimize procurement strategies in both public and private sectors. The approach, based on the optimization of resource allocation, aims to reduce financial and operational risks associated with the transition from legacy systems to modern IT solutions.

Statistical data illustrating the dynamics of digital transformation are provided in source [11], published on the enterpriseappstoday website. Sources [11, 12], whose information is published on the websites: netwrix and businessstudio, were used in analyzing the ways of calculating the effectiveness of using risk management strategies in ensuring compliance for legacy IT infrastructure.

A review of the presented works reveals inconsistencies in how the prioritization of different aspects of risk management is evaluated. Some authors emphasize technological modernization and the development of migration frameworks, while others focus on data governance and analytical solutions. At the same time, the economic dimension remains insufficiently integrated with technical aspects, pointing to the need for interdisciplinary approaches in the development of comprehensive strategies. Furthermore, issues related to information security, regulatory compliance, and the integration of compliance requirements into migration processes remain underexplored, despite their critical importance in contemporary IT infrastructure management.

The aim of the study is to justify strategies for risk management and regulatory compliance in the modernization of legacy IT infrastructure.

The scientific novelty lies in proposing a new perspective on integrating strategic planning, change management, and modern security technologies to reduce operational costs and improve business resilience, as identified through literature analysis.

The author's hypothesis suggests that implementing a comprehensive strategy—based on modular transition to cloud solutions, systematic risk management, and strict adherence to regulatory standards—can reduce operational costs and enhance business resilience even during significant technological renewal of legacy IT infrastructure.

The research applies a methodology that includes qualitative analysis of academic and professional literature as well as the use of analytical tools to evaluate the effectiveness of the proposed measures.

1. Analysis of the condition of legacy IT infrastructure and its associated risks

Modern organizations operating on legacy IT systems face a range of technical, operational, and regulatory challenges resulting from technical debt, limited flexibility, and difficulties integrating such systems with modern technologies. These systems are often built on outdated programming languages and platforms (e.g., COBOL, mainframes) and are characterized by low scalability, high maintenance costs, and limited capacity for functional upgrades [1,3]. Their rigidity makes adaptation to current business processes problematic, leading to reduced operational efficiency and increased business risk.

Legacy systems are frequently the result of years of accumulated functionality layered onto outdated architectural foundations. As a result, they are defined by the following characteristics:

Technical debt and limited flexibility. Systems developed decades ago typically have rigid and complex architectures, making adaptation to evolving business requirements difficult [1].

Integration challenges. The absence of modern interfaces and data exchange standards creates barriers to integrating with newer applications, resulting in fragmentation of the IT environment.

High maintenance costs. Legacy systems demand significant financial and human resources to remain operational, as component replacement or architectural overhaul is often expensive and resource-intensive [2].

To better understand how these risks affect legacy IT infrastructure, Table 1 outlines the key risk indicators.

Table 1. Key Risk Indicators for Legacy IT Infrastructure [1]

Indicator	Description	Business impact
Technical debt	Accumulated technological obsolescence limiting scalability and upgrades	Reduced performance, increased downtime
Limited flexibility	Inflexible architecture hindering the implementation of new features and integration	Delays in innovation, inability to respond quickly to market changes
Integration issues	Lack of modern APIs and data exchange standards	Fragmented IT environment, difficulties in system-to-system data synchronization
High maintenance costs	Significant expenditures to support and update outdated systems	Decreased profitability, reallocation of resources from growth to maintenance
Information security risks	Insufficient data protection, lack of modern encryption and access control	Increased vulnerability to cyberattacks, risk of confidential data breaches
Regulatory non-compliance risk	Inability to update systems in line with evolving standards and regulations	Legal penalties, fines, reputational damage

In turn, in order to calculate the annual expected damage before and after the implementation of risk management measures, the following formula should be used:

$$ALE = SLE \times ARO \ (1),$$

where:

SLE (Single Loss Expectancy) is the expected loss from a single incident;

ARO (Annual Rate of Occurrence) - expected frequency of incident occurrence per year [12].

Thus, legacy IT infrastructure represents a collection of systems characterized by high levels of technical debt, limited flexibility, and integration challenges. These features generate substantial risks at both technical and operational levels and lead to additional regulatory complications. A comprehensive assessment of the state of outdated systems and identification of key risks are essential prerequisites for the development of effective risk management and compliance strategies, which, in turn, support business resilience amid rapidly evolving technological environments.

2. Risk management strategies for modernization and migration

The use of AI-driven analytics and cloud technologies enhances the accuracy of risk forecasting and facilitates timely adjustment of management strategies [2]. The initial stage involves a comprehensive assessment of existing risks using tools for analyzing technical debt, identifying system dependencies, and evaluating the potential impact of each component on the overall performance of the IT infrastructure. This process includes the following core steps:

System mapping and grouping. Identifying and documenting the architectural features of legacy systems allows organizations to determine their relevance to business processes, forming the basis for prioritizing migration tasks [1].

Risk forecasting using AI-driven analytics. The application of predictive models to evaluate the effects of migration processes enables the early detection of potential bottlenecks and real-time adjustment of migration strategies [5,8].

Phased migration approach. Dividing the overall migration effort into smaller, manageable stages reduces the likelihood of system failures and allows for iterative feedback and adjustments at each implementation phase.

Implementation of monitoring and control mechanisms. Continuous tracking of performance metrics, security compliance, and regulatory alignment enables swift responses to emerging issues [1,7].

To improve risk management efficiency, it is recommended to integrate these measures into a unified strategic model that encompasses the technical, organizational, and regulatory dimensions of modernization. This approach enables rapid identification of vulnerabilities, minimizes risk impacts on operational activity, and reduces the cost of maintaining outdated infrastructure.

In the context of risk management during the migration of legacy systems, several strategies supported by research can be outlined [1,2]:

Modular migration and refactoring. Applying a phased transition, in which systems are decomposed into independent modules, reduces the impact of changes on the entire infrastructure. This method lowers the risk of system-wide failures and simplifies integration with newer technologies [1].

AI-driven forecasting and prioritization. Machine learning algorithms are used to assess component criticality and predict their impact on performance, enabling the creation of an optimized migration plan with minimal risk [2].

Cloud solutions and API integration. The adoption of modern cloud platforms allows for scalable flexibility, while the use of APIs facilitates seamless integration between legacy and modern systems, significantly reducing operational risks [2,9].

Strategic planning and change management. Engaging key stakeholders, delivering training programs, and implementing continuous monitoring systems help reduce internal resistance and increase organizational adaptability.

For clarity and organization, these approaches are summarized in Table 2.

Table 2. Key risk management strategies for legacy system migration [1,2,5,10]

Strategy	Description	Advantages
Modular migration and refactoring	Decomposing the system into independent modules followed by phased updates	Reduces the impact of changes on the entire system, simplifies integration
AI-driven forecasting and prioritization	Applying machine learning algorithms to assess component criticality and predict risks	Increases the accuracy of risk assessment, enables rapid response to potential issues
Cloud solutions and API integration	Implementing cloud platforms and modern APIs to integrate new and legacy systems	Scalability flexibility, reduced operational costs, improved interoperability
Strategic planning and change management	Developing a clear migration plan with stakeholder involvement, staff training, and ongoing monitoring	Minimizes resistance to change, ensures continuity of business processes

In order to calculate the efficiency of security investment, the following formulas should be used:

$$ROSI = \frac{ALE_{before} - ALE_{after} - C_{invest}}{C_{invest}} \text{ (2)},$$

where:

ALE_{before} – annual expected damage before the implementation of measures.

ALE_{after} – annual expected damage after implementation of measures.

C_{invest} – costs of implementation of risk management measures.

If the obtained result is positive, it indicates that the costs are recouped by reducing losses [12].

Also as part of the assessment it is necessary to calculate the risk reduction ratio, which can be calculated using the following formula:

$$A = P \times I \text{ (3)},$$

where:

P – maximum probability found in the list of risk causes.

I – the maximum force of influence found in the list of risk consequences [13].

The implementation of comprehensive risk management strategies—encompassing modular migration, AI-driven analytical assessment, integration of cloud-based solutions, and proactive change management—helps mitigate the negative impact of migration processes on business operations. These approaches not only reduce technical and operational risks but also contribute to regulatory compliance, which is a key factor in maintaining IT infrastructure resilience in the context of ongoing technological evolution.

3. Ensuring regulatory compliance and integrating security measures

Modernizing legacy IT infrastructure entails not only updating technological components but also ensuring compliance with current regulatory standards and integrating advanced security measures. The transition to next-generation architectures requires a holistic approach to data protection, access management, and continuous security monitoring, particularly relevant in the face of escalating cyber threats and tightening regulatory frameworks such as GDPR, HIPAA, and ISO/IEC 27001 [1,4].

One of the core challenges of legacy systems is their inability to adapt to modern cybersecurity and regulatory requirements. These systems often lack support for contemporary encryption methods, access control, and audit capabilities, which increases the risk of data breaches and regulatory violations. Accordingly, modernization initiatives must integrate mechanisms that enable:

Continuous security monitoring and auditing. Ongoing system surveillance and regular audits facilitate timely detection of vulnerabilities and allow for migration adjustments as needed.

Encryption and access control integration. The use of advanced encryption algorithms and the implementation of multi-factor authentication and role-based access control systems reduce the risk of unauthorized data access.

Compliance automation. Leveraging cloud-based solutions with built-in compliance functions (e.g., automated log collection and analysis, regular security policy updates) reduces operational risks and minimizes the human factor [1,2].

Incorporating these measures is increasingly critical in light of modern legal and security standards. The implementation of advanced security controls not only protects an organization's informational assets but also ensures transparency during the migration process, enhancing trust among clients and partners [1].

The following table summarizes key measures for ensuring regulatory compliance and integrating security mechanisms during the modernization of legacy systems.

Table 3. Measures to ensure compliance with regulatory requirements and integration of security measures [1,6]

Measure	Description	Advantages
Continuous monitoring and auditing	Deployment of automated monitoring systems, routine auditing, and log analysis to detect security issues	Enables rapid identification and resolution of vulnerabilities, increases process transparency
Modern encryption methods	Utilization of AES, RSA, and other advanced encryption standards for protecting data in transit and at rest	Ensures high-level data protection, reduces the risk of breaches
Multi-factor authentication and access control	Implementation of MFA systems and role-based access control for safeguarding critical systems	Reduces likelihood of unauthorized access, enhances system change management
Automated compliance systems	Integration of cloud platforms with built-in policy updates, compliance reporting, and regulatory controls	Ensures legal compliance, lowers operational costs associated with manual compliance

Thus, ensuring regulatory compliance and integrating security measures constitute a multifaceted process that requires a systematic approach when modernizing legacy IT infrastructure. The implementation of advanced encryption technologies, multi-factor authentication, and automated monitoring systems enables the reduction of information security risks while maintaining adherence to regulatory requirements. This approach supports the development of a resilient and secure IT environment capable of effectively sustaining business processes in a rapidly evolving technological landscape.

Conclusion

The analysis of legacy systems revealed their lack of flexibility and high maintenance costs, which result in operational and informational risks. The study proposed strategies to mitigate these risks, including modular migration, the use of AI algorithms for forecasting and prioritization, as well as the adoption of cloud solutions and modern data protection methods such as encryption and multi-factor authentication.

Despite the findings, the study presents limitations related to industry-specific contexts. It is recommended that future research expand the empirical base by incorporating data from diverse sectors and conducting long-term monitoring of the effectiveness of the proposed measures. The results confirm the hypothesis that a comprehensive and integrated approach to modernizing legacy IT infrastructure leads to a significant reduction in risk, enhances business resilience, and creates competitive advantages in a rapidly changing technological environment.

References

1. Adepoju A. H. et al. Framework for migrating legacy systems to next-generation data architectures while ensuring seamless integration and scalability //International Journal of Multidisciplinary Research and Growth Evaluation. – 2024. – Vol. 5 (6). – pp. 1462-1474.
2. Kambala G. The Role of Cloud Computing in Modernizing Legacy Enterprise Systems: A Case Study Approach. – 2023. – Vol. 12 (7). – pp.9039-9054.
3. Adepoju A. H. et al. A data governance framework for high-impact programs: Reducing redundancy and enhancing data quality at scale //Int J Multidiscip Res Growth Eval. – 2023. – Vol. 4 (6). – pp. 1141-1154.
4. Khang A., Sivaraman K. A. Big data, cloud computing and IoT: Tools and applications/edited //J. Future Revol. Comput. Sci. Commun. Eng. – 2023. – Vol. 4 (4). – pp. 599-602.
5. Onoja J. P., Ajala O. A., Ige A. B. Harnessing artificial intelligence for transformative community development: A comprehensive framework for enhancing engagement and impact //GSC Advanced Research and Reviews. – 2022. – Vol. 11 (3). – pp. 158-166.
6. Abbey A. B. N. et al. Developing economic frameworks for optimizing procurement strategies in public and private sectors //J Bus Finance Res. – 2023. – Vol. 2(1). - pp.19-26.
7. Mishra S., Komandla V., Bandi S. A new pattern for managing massive datasets in the Enterprise through Data Fabric and Data Mesh //Journal of AI-Assisted Scientific Discovery. – 2021. – Vol. 1 (2). – pp. 236-59.
8. Machireddy J. R., Rachakatla S. K., Ravichandran P. Leveraging AI and machine learning for data-driven business strategy: a comprehensive framework for analytics integration //African Journal of Artificial Intelligence and Sustainable Development. – 2021. – Vol. 1 (2). – pp. 12-35.
9. Ponnusamy S., Eswararaj D. Navigating the modernization of legacy applications and data: Effective strategies and best practices //Asian Journal of Research in Computer Science. – 2023. – Vol. 16 (4). – pp. 239-256.
10. Eeti S., Renuka A. Strategies for Migrating Data from Legacy Systems to the Cloud: Challenges and Solutions //TIJER (The International Journal of Engineering Research. – 2021. – Vol. 8 (10). – pp. 1-11.
11. Digital Transformation Statistics and Facts. [Electronic resource] Access mode: https://www.enterpriseappstoday.com/stats/digital-transformation-statistics.html (date of request: 03/18/2025).
12. How to Calculate Return on Security Investment . [Electronic resource] Access mode: https://blog.netwrix.com/2018/08/07/how-to-calculate-return-on-security-investment/ (date of request: 03/31/2025).
13. Risk analysis and assessment . [Electronic resource] Access mode: https://www.businessstudio.ru/help/docs/current/doku.php/ru/manual/risk_management/risk_assessment (date of request: 03/31/2025).