International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V5I3P104
Eureka Vision Publication | Volume 5, Issue 3, 38-46, 2024

Original Article

Navigating Security and Compliance in the Modernization of Legacy Systems: Strategies for a Resilient Future

Vijayasekhar Duvvur,
Software Modernization Specialist, 3i Infotech Inc, USA.

Abstract - As organizations increasingly recognize the need to modernize their legacy systems, the intersection of security and compliance becomes a critical focal point. Legacy systems, often built on outdated technologies, are inherently vulnerable to modern cyber threats. While modernization offers a pathway to enhanced security and operational efficiency, the process itself can introduce new risks if not managed carefully. This article explores the intricate balance between modernization, security, and compliance, offering a comprehensive guide to navigating these challenges. We delve into the key risks associated with legacy system modernization, provide actionable strategies for ensuring compliance, and highlight best practices for achieving a secure and resilient IT environment. By prioritizing security and compliance throughout the modernization journey, organizations can not only mitigate risks but also build a foundation for long-term success in an increasingly digital world.

Keywords - Legacy Systems, Modernization, Security Compliance, Cybersecurity, Data Protection, Risk Management.

1. Introduction

Legacy systems have long been the backbone of many organizations, supporting critical operations and housing vast amounts of sensitive data. However, as the threat landscape evolves, these systems, often built on outdated technologies and lacking modern security features, are becoming increasingly vulnerable to cyberattacks. Modernization, the process of updating or replacing these legacy systems, presents a unique opportunity to enhance security, improve efficiency, and ensure compliance with current regulations. Yet, the modernization process is fraught with challenges, particularly when it comes to maintaining security and compliance during the transition.

This article examines the complexities of modernizing legacy systems while ensuring security and compliance. We will explore the risks associated with modernization [1], discuss strategies for mitigating these risks, and provide best practices for achieving a secure and compliant modernized system. By understanding these dynamics, organizations can navigate the modernization process more effectively, ensuring that their systems are not only up-to-date but also resilient against future threats.

Modernization is not merely a technical upgrade; it represents a fundamental transformation of an organization's IT infrastructure to meet current and future demands. However, this transformation must be underpinned by a strong commitment to security and compliance. Without these elements, modernization efforts can introduce new risks, undermine trust, and fail to deliver the intended benefits. Below, we explore in greater detail why security and compliance are critical to the success of modernization initiatives.

1.1 Mitigating Cyber Risks

Legacy systems are often riddled with vulnerabilities that make them prime targets for cybercriminals. These systems were typically designed in an era when cybersecurity threats were less sophisticated, and as a result, they lack the advanced security features found in modern solutions. For example, legacy systems may rely on outdated encryption standards, weak password policies, or insufficient access controls, all of which can be easily exploited by attackers. Modernization provides an opportunity to address these vulnerabilities, but only if security is prioritized throughout the process.

By integrating robust security measures, such as encryption, multi-factor authentication, and intrusion detection systems, into the modernized system, organizations can significantly reduce their exposure to cyber risks [8]. Failure to prioritize security during modernization can result in a system that is just as vulnerable as the legacy system it replaced, if not more so.

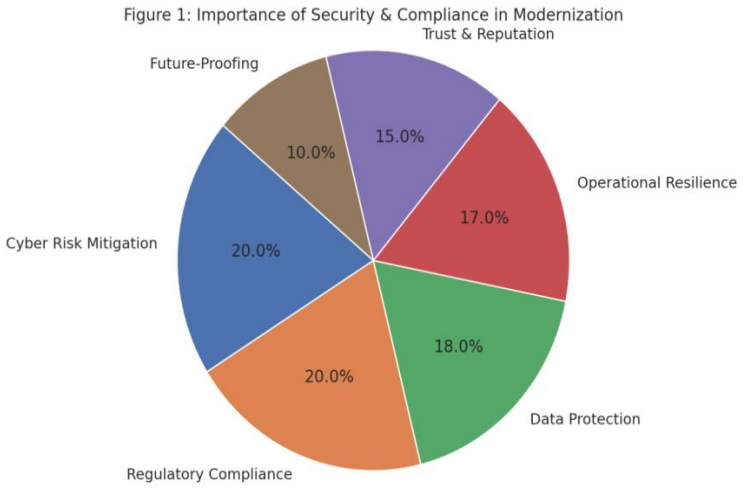

Figure 1. The Importance of Security and Compliance in Modernization

1.2 Regulatory Compliance

Organizations today operate in a highly regulated environment, with a growing number of laws and standards mandating specific security controls and data protection measures. Regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) require organizations to implement stringent security practices to protect sensitive data. Non-compliance with these regulations can have severe consequences, including hefty fines, legal action, and operational disruptions. Modernization offers an opportunity to align IT systems with these regulatory requirements, but it requires careful planning and execution. Organizations must ensure that the modernized system incorporates the necessary controls to meet compliance standards, such as data encryption, access controls, and audit trails. By doing so, they can avoid the financial and reputational damage associated with non-compliance.

1.3 Data Protection

Modernization often involves the migration of sensitive data from legacy systems to new platforms. This data may include customer information, financial records, intellectual property, and other critical assets [14]. Ensuring the security of this data during migration is paramount, as any breach or loss can have devastating consequences. Data breaches can result in financial losses, legal liabilities, and irreparable damage to an organization's reputation. Moreover, customers and partners expect their data to be handled securely, and any failure to do so can erode trust. During modernization, organizations must implement robust data protection measures, such as encrypting data both at rest and in transit, enforcing strict access controls, and conducting regular integrity checks. By prioritizing data protection, organizations can safeguard sensitive information and maintain the trust of their stakeholders.

1.4 Operational Resilience

A secure and compliant modernized system is inherently more resilient to cyber threats, reducing the risk of downtime and ensuring business continuity. Legacy systems are often fragile and prone to failure, particularly when subjected to cyberattacks or other disruptions. Modernization provides an opportunity to build a more robust and resilient IT infrastructure [9] that can withstand these challenges. For example, modern systems often include features such as automated backups, disaster recovery plans, and real-time monitoring, all of which contribute to operational resilience. Additionally, by addressing security vulnerabilities and ensuring compliance with regulatory requirements, organizations can reduce the likelihood of cyber incidents that could disrupt operations. In today's fast-paced business environment, where downtime can result in significant financial losses and damage to reputation, operational resilience is a critical consideration in any modernization effort.

1.5 Building Trust and Reputation

In an era where data breaches and cyberattacks are increasingly common, organizations must demonstrate a commitment to security and compliance to build and maintain trust with customers, partners, and regulators. A secure and compliant modernized system sends a strong message that the organization takes data protection seriously and is committed to safeguarding sensitive

information. This can enhance the organization's reputation and provide a competitive advantage in the marketplace. Conversely, a failure to prioritize security and compliance during modernization can lead to breaches, regulatory penalties, and a loss of trust, all of which can have long-term negative impacts on the organization's brand and bottom line.

1.6 Future-Proofing the Organization

Modernization is not just about addressing current challenges; it is also about preparing for the future. The threat landscape is constantly evolving, with new cyber threats emerging on a regular basis. Similarly, regulatory requirements are becoming increasingly stringent, with new laws and standards being introduced to address emerging risks. By prioritizing security and compliance during modernization, organizations can build a system that is not only secure and compliant today but also adaptable to future challenges. This future-proofing ensures that the organization remains resilient in the face of evolving threats and regulatory changes, reducing the need for costly and disruptive upgrades down the line.

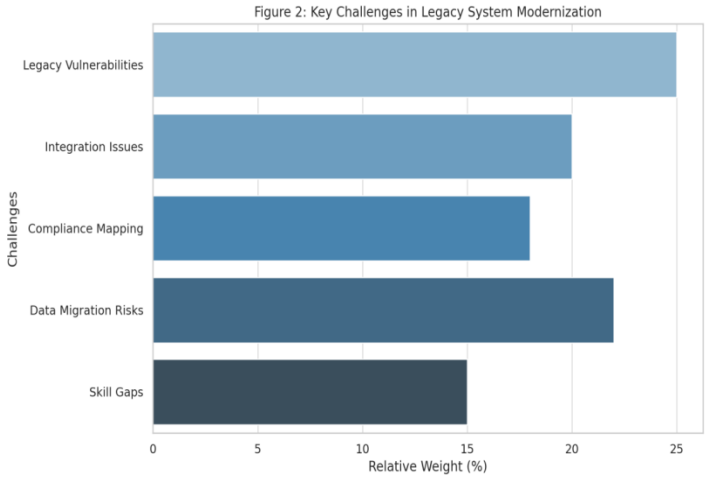

Figure 2. Key Challenges in Legacy System Modernization

Modernizing legacy systems while maintaining security and compliance is a complex and multifaceted endeavor. Organizations must navigate a range of challenges that can complicate the modernization process. Below, we delve deeper into each of these challenges, providing a more detailed understanding of the obstacles organizations face and why they are so critical to address.

2. Inherent Vulnerabilities in Legacy Systems

Legacy systems were often designed and implemented in an era when cybersecurity threats were less sophisticated and less prevalent. As a result, these systems typically lack the advanced security features that are standard in modern IT solutions. One of the most significant issues is the use of outdated software and hardware that are no longer supported by vendors. Without regular security patches or updates, these systems are exposed to known vulnerabilities that can be easily exploited by cybercriminals. Additionally, legacy systems often rely on weak or outdated encryption standards, or in some cases, no encryption at all, leaving sensitive data vulnerable to interception and theft. Furthermore, legacy systems may have inadequate access controls, allowing unauthorized users to gain access to critical systems and data. These inherent vulnerabilities must be addressed during modernization to ensure the new system is secure and resilient against modern cyber threats.

2.1 Integration Complexity

Integrating modernized systems with existing infrastructure is a significant challenge, particularly when it comes to ensuring that security controls are consistently applied across the entire environment. Legacy systems often operate in isolation, using proprietary protocols and technologies that are incompatible with modern solutions. This incompatibility can create gaps in security when integrating new systems with old ones. For example, modern systems may use advanced authentication mechanisms like multi-factor authentication (MFA), while legacy systems may still rely on simple username and password combinations. Ensuring that these systems work together seamlessly without compromising security requires careful planning and configuration management. Additionally, integrating modern cloud-based solutions [2] with on-premises legacy systems can introduce further complexity, as organizations must ensure that data flows securely between different environments and that security policies are uniformly enforced.

2.2 Compliance Mapping

Aligning modernization efforts with relevant compliance requirements is a complex task, especially for organizations that must adhere to multiple regulations and standards. Legacy systems were often designed before many of today's regulatory requirements were in place, meaning they may not have built-in controls to meet current compliance standards. For example, regulations like the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) mandate specific data protection measures that may not have been considered when the legacy system was originally developed. During modernization, organizations must map these compliance requirements to the new system, ensuring that all necessary controls are implemented. This process can be particularly challenging when dealing with overlapping or conflicting regulations, requiring organizations to carefully balance compliance with operational efficiency.

2.3 Data Security Risks During Migration

Data migration is a critical component of modernization, but it also introduces significant risks. Legacy systems often contain vast amounts of sensitive data, including customer information, financial records, and intellectual property. Moving this data from legacy systems to modern platforms requires robust security measures to ensure its confidentiality, integrity, and availability. One of the primary risks during migration is the potential for data breaches, as data is often more vulnerable when it is in transit between systems. Additionally, data corruption or loss can occur if the migration process is not carefully managed. Organizations must implement strong encryption for data both at rest and in transit, enforce strict access controls to limit who can access the data during migration, and perform regular integrity checks to ensure the data remains accurate and complete. Failure to adequately secure data during migration can result in significant financial and reputational damage.

2.4 Skill Gaps and Lack of Expertise

Many organizations lack the in-house expertise needed to navigate the complexities of modernization, particularly when it comes to security and compliance. Legacy systems often require specialized knowledge to understand their unique architecture, dependencies, and vulnerabilities. However, as these systems age, the pool of professionals with the necessary skills to maintain and modernize them shrinks. This skill gap can lead to delays in the modernization process, as organizations struggle to find qualified personnel to manage the transition. Additionally, the rapid evolution of cybersecurity threats and compliance requirements means that even experienced IT staff may lack the up-to-date knowledge needed to address modern challenges. Organizations may need to invest in training for existing staff or bring in external experts to fill these gaps, adding to the cost and complexity of the modernization effort.

To successfully modernize legacy systems while maintaining security and compliance, organizations must adopt a strategic and holistic approach. Modernization is not just about upgrading technology; it is about transforming the entire IT ecosystem in a way that addresses current vulnerabilities, meets regulatory requirements, and prepares the organization for future challenges. Below, we explore in greater detail the key strategies organizations should consider to ensure security and compliance throughout the modernization process.

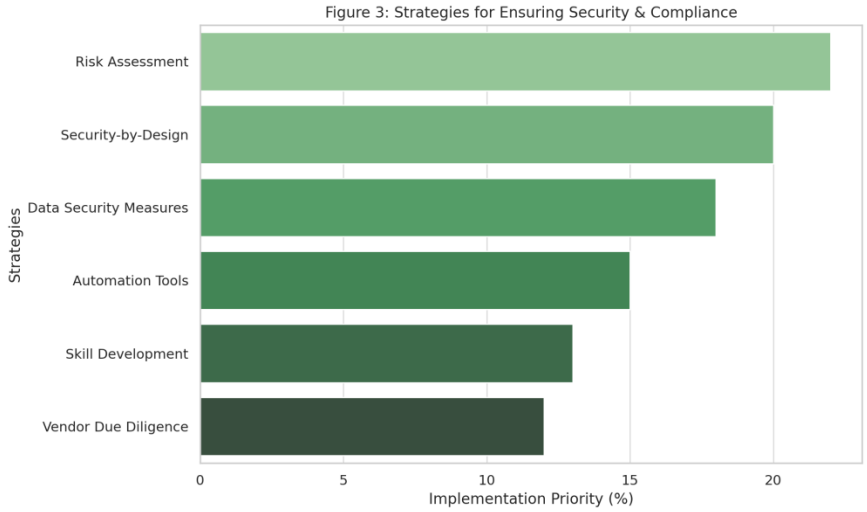

Figure 3. Strategies for Ensuring Security and Compliance During Modernization

3. Conduct a Comprehensive Risk Assessment

Before embarking on modernization, organizations must conduct a thorough risk assessment to identify potential security vulnerabilities and compliance gaps. This assessment serves as the foundation for the entire modernization effort, providing a clear understanding of the risks that need to be addressed. The risk assessment should begin with a detailed analysis of the legacy systems, evaluating their current state and identifying vulnerabilities such as outdated software, weak encryption, and inadequate access controls. This analysis should also consider the system's architecture, dependencies, and any third-party components that may introduce additional risks [11].

In addition to assessing the technical aspects of the legacy systems, organizations must also evaluate the regulatory and industry standards that apply to their operations. This includes identifying the specific security controls mandated by regulations such as GDPR [13], HIPAA [12], or PCI DSS and mapping these requirements to the vulnerabilities identified in the legacy systems. By doing so, organizations can ensure that the modernized system will meet all necessary compliance requirements.

Finally, the risk assessment should prioritize risks based on their potential impact and likelihood. This prioritization allows organizations to focus their efforts on addressing the most critical [3] vulnerabilities first, ensuring that the modernization process delivers the greatest security and compliance benefits.

3.1 Adopt a Security-by-Design Approach

Security should be integrated into every stage of the modernization process, from the initial planning phase through to implementation and beyond. This security-by-design approach ensures that security considerations are not an afterthought but are instead a core component of the modernization effort. One of the key elements of this approach is the adoption of secure development practices. Developers must follow secure coding principles, and security testing should be conducted throughout the development lifecycle to identify and address vulnerabilities early in the process.

Threat modeling is another critical component of the security-by-design approach. By identifying potential threats and vulnerabilities associated with the chosen modernization approach, organizations can develop targeted mitigation strategies to address these risks. This proactive approach to threat management helps ensure that the modernized system is resilient against both current and emerging threats.

The design of the modernized system architecture must also prioritize security. This includes incorporating features such as data encryption at rest and in transit, access controls based on the principle of least privilege, and robust authentication mechanisms. By designing the system with security in mind from the outset, organizations can reduce the risk of introducing new vulnerabilities during the modernization process.

3.2 Implement Robust Data Security Measures

Data security is a critical concern during modernization, particularly during the data migration phase. Legacy systems often contain vast amounts of sensitive data, including customer information, financial records, and intellectual property. Ensuring the security of this data during migration is essential to preventing breaches and maintaining customer trust.

One of the first steps in securing data during migration is data classification. By classifying data based on its sensitivity, organizations can prioritize security measures and ensure that the most critical data receives the highest level of protection. Encryption is another essential measure, as it protects data both at rest and in transit, minimizing the risk of unauthorized access even if a breach occurs.

Access controls are also crucial during data migration. Organizations must implement strict access controls to ensure that only authorized personnel can access sensitive data during the migration process. This includes enforcing the principle of least privilege, which limits access to only those individuals who need it to perform their specific tasks.

Finally, organizations must perform regular data integrity checks throughout the migration process. These checks ensure that the data remains accurate and complete, reducing the risk of data corruption or loss. By implementing these robust data security measures, organizations can safeguard sensitive information and ensure a smooth and secure migration process.

3.3 Leverage Automation and Advanced Security Tools

Automation and advanced security tools can play a key role in ensuring security and compliance during modernization. One of the most valuable tools in this regard is automated vulnerability scanning. These tools can scan the modernized system and its underlying infrastructure for known vulnerabilities, configuration errors, and weak encryption practices. By identifying these

issues early in the process, organizations can address them before they become significant security risks. Another critical tool is a Security Information and Event Management (SIEM) system. SIEM systems centralize log collection and analysis from the modernized system and other security tools, enabling real-time monitoring for suspicious activity. This facilitates faster detection of potential security incidents and allows organizations to respond more effectively to threats.

Compliance management software is another valuable tool for organizations undergoing modernization. These tools can automate many of the tasks associated with compliance, such as gap analysis, risk assessment, and regulatory change management. By streamlining these processes, organizations can ensure that they remain compliant with relevant regulations while reducing the administrative burden on their IT teams.

3.4 Invest in Training and Skill Development

Modernization requires a skilled workforce capable of managing the complexities of security and compliance. Many organizations lack the in-house expertise needed to navigate these challenges, particularly when it comes to modernizing legacy systems. To address this gap, organizations must invest in training and skill development for their employees.

Comprehensive security training is essential for all employees, not just those directly involved in the modernization process. This training should cover best practices [4] for data protection, password hygiene, and phishing awareness, helping to create a culture of security within the organization. Role-based training is also important, as it ensures that employees understand their specific responsibilities in maintaining security and compliance.

Phishing simulation exercises can further enhance employee awareness and preparedness for cyberattacks. By conducting regular simulations, organizations can identify areas where additional training or awareness campaigns are needed and ensure that employees are equipped to recognize and respond to potential threats.

3.5 Engage with Third-Party Vendors Carefully

Many modernization efforts involve third-party vendors or cloud service providers, particularly when organizations are moving to cloud-based solutions. While these partnerships can provide valuable expertise and resources, they also introduce additional risks. Organizations must ensure that third-party vendors adhere to the same security and compliance standards that they apply internally.

This begins with conducting thorough security due diligence on potential vendors. Organizations should evaluate the vendor's security practices, compliance posture, and incident response capabilities to ensure that they meet the organization's standards. Contractual requirements are also critical, as they provide a legal framework for enforcing security and compliance obligations. These requirements should address data security, access controls, incident reporting, and regulatory compliance.

Finally, organizations must conduct regular assessments of the security posture of third-party vendors and cloud service providers [16, 17, 18]. This ongoing monitoring ensures that vendors maintain adequate security controls and continue to comply with relevant regulations throughout the duration of the partnership.

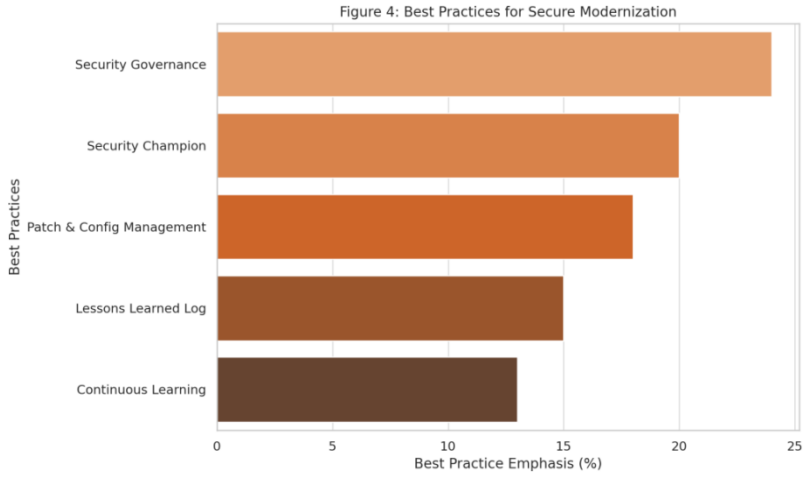

Figure 4. Best Practices for Secure and Compliant Modernization

While the strategies outlined earlier provide a roadmap for ensuring security and compliance during legacy system modernization, organizations must also adopt a set of best practices to solidify their efforts. These best practices go beyond risk mitigation and compliance checks; they establish a foundation for long-term security and operational resilience. Below, we explore these best practices in greater detail, emphasizing their importance and how they contribute to a successful modernization process.

4. Establish a Security Governance Framework

A robust security governance framework is essential for ensuring that security and compliance are embedded into the organization's culture and operations. This framework should begin with the development of clear and comprehensive security policies and procedures. These policies should outline the organization's approach to data security, access control, incident response, and vulnerability management. They should also be tailored to the specific requirements of the modernized system and aligned with relevant compliance frameworks.

In addition to policies, the governance framework should clearly define roles and responsibilities for security within the modernization project. This includes assigning ownership for tasks such as security assessments, vulnerability management, and compliance reporting. By clearly defining who is responsible for what, organizations can ensure that security considerations are not overlooked or neglected.

Finally, the governance framework should foster a culture of security awareness throughout the organization. This involves establishing clear communication channels for security-related issues and encouraging employees to report suspicious activity or potential security breaches. A strong security culture ensures that everyone in the organization understands the importance of security and compliance and is actively engaged in maintaining them.

4.1 Appoint a Security Champion

Modernization projects are complex and multifaceted, often involving multiple teams and stakeholders. To ensure that security and compliance remain a priority throughout the process, organizations should appoint a dedicated security champion or team. This individual or team should possess a deep understanding of security best practices, compliance regulations, and the specific risks associated with the chosen modernization approach.

The security champion plays a critical role in advocating for security within the project team. They collaborate with developers, system administrators, and other stakeholders to ensure that security is integrated seamlessly into every stage of the modernization process. This includes participating in design discussions, reviewing code for security vulnerabilities, and ensuring that security testing is conducted throughout the development lifecycle.

The security champion is also responsible for communicating security risks and compliance requirements to project stakeholders. They develop reports that track progress on addressing security concerns and maintaining compliance, providing transparency and accountability throughout the modernization process. By having a dedicated security champion, organizations can ensure that security and compliance remain a central focus, even as the project evolves and new challenges arise.

4.2 Maintain Updated Security Controls

Security is not a one-time effort; it requires ongoing attention and maintenance. As part of the modernization process, organizations must implement a robust patch management strategy to ensure that the modernized system and its underlying infrastructure remain secure. This includes deploying security patches and updates in a timely manner, particularly for critical vulnerabilities that could be exploited by attackers.

In addition to patch management, organizations should implement robust configuration management practices. This involves ensuring that all components of the modernized system are configured securely and consistently, minimizing the risk of misconfigurations that could introduce vulnerabilities. Configuration management should be an ongoing process, with regular reviews and updates to address emerging threats and changes in the system environment.

Regular security reviews are also essential for maintaining updated security controls. These reviews should be conducted periodically to identify and address any emerging security threats or vulnerabilities. They can be performed internally by the organization's IT team or by qualified external security professionals. By conducting regular reviews, organizations can ensure that their security controls remain effective and up-to-date in the face of evolving threats.

4.3 Document Lessons Learned

Modernization projects often encounter unexpected challenges and obstacles, particularly when it comes to security and compliance. To ensure that these challenges are not repeated in future projects, organizations should maintain a detailed log of lessons learned. This documentation should include a description of the challenges encountered, the steps taken to address them, and the outcomes of those efforts.

The lessons learned log serves as a valuable resource for future IT projects, providing insights into what worked well and what did not. It can also help identify areas for improvement in the organization's overall security posture. For example, if a particular vulnerability was overlooked during the modernization process, the lessons learned log can highlight the need for more thorough risk assessments in future projects.

In addition to documenting challenges, organizations should also document successful strategies and best practices. This information can be used to develop standardized processes and procedures for future modernization efforts, ensuring that security and compliance are consistently prioritized.

4.4 Stay Informed and Invest in Skills Development

The cybersecurity landscape is constantly evolving, with new threats and vulnerabilities emerging on a regular basis. To stay ahead of these challenges, organizations must proactively stay informed about the latest security trends and developments. This includes subscribing to security advisories from trusted sources, participating in industry forums, and attending cybersecurity conferences and events.

Staying informed also involves keeping up-to-date with changes in regulatory requirements. Compliance is not a static goal; it requires ongoing attention to ensure that the organization remains aligned with the latest regulations and standards. By staying informed about regulatory changes, organizations can ensure that their modernized system remains compliant and that they avoid potential fines or penalties.

In addition to staying informed, organizations must invest in ongoing security skills development for their IT staff. Modernization projects often require specialized knowledge and expertise, particularly when it comes to integrating security and compliance into the process. By providing training and development opportunities for their IT teams, organizations can ensure that they have the necessary skills to manage the security of the modernized system effectively.

This investment in skills development should extend beyond technical training. It should also include training on security best practices, compliance requirements, and incident response procedures. By equipping their IT staff with the knowledge and skills they need, organizations can build a more resilient and secure IT environment.

5. Conclusion

Modernizing legacy systems is a critical yet complex endeavor that requires a careful balance between technological advancement, security, and compliance. As organizations strive to update their outdated systems, they must navigate a landscape filled with inherent vulnerabilities, integration complexities, and evolving regulatory requirements. The modernization process offers a unique opportunity to enhance security, improve operational efficiency, and ensure compliance with current standards, but it also introduces new risks if not managed properly.

By adopting a strategic approach that includes comprehensive risk assessments, a security-by-design mindset, robust data protection measures [7], and the use of advanced security tools, organizations can mitigate these risks and build a resilient IT infrastructure [5]. Additionally, investing in employee training, appointing a dedicated security champion, and maintaining updated security controls are essential best practices that contribute to the long-term success of modernization efforts [6].

The importance of security and compliance cannot be overstated. In an era where cyber threats are constantly evolving, and regulatory requirements are becoming increasingly stringent, organizations must prioritize these elements to protect sensitive data, maintain customer trust, and avoid costly penalties. Modernization is not just about upgrading technology; it is about future-proofing the organization, ensuring that it remains resilient in the face of emerging threats and regulatory changes [19, 20].

Ultimately, the journey to modernize legacy systems is challenging, but with careful planning, the right strategies, and a commitment to best practices, organizations can achieve a secure, compliant, and future-ready IT environment. By doing so, they not only mitigate risks but also lay the foundation for long-term success in an increasingly digital and interconnected world.

References

[1] NIST Special Publication 800-37: "Risk Management Framework for Information Systems and Organizations." *National Institute of Standards and Technology (NIST)*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[2] ISO/IEC 27001: "Information Security Management." *International Organization for Standardization (ISO)*. https://www.iso.org/isoiec-27001-information-security.html

[3] Cloud Security Alliance (CSA): "Security Guidance for Critical Areas of Focus in Cloud Computing."https://cloudsecurityalliance.org/research/guidance/

[4] OWASP Top Ten: "The Ten Most Critical Web Application Security Risks." *Open Web Application Security Project (OWASP)*.https://owasp.org/www-project-top-ten/

[5] Gartner Report: "Best Practices for Legacy System Modernization."*Gartner, Inc.* https://www.gartner.com

[6] McKinsey & Company: "Modernizing Legacy Systems: A Strategic Approach." https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights

[7] Forrester Research: "The State of Application Modernization in 2023." https://www.forrester.com

[8] IBM Security: "Data Protection and Privacy in the Cloud Era." https://www.ibm.com/security/data-protection

[9] Deloitte Insights: "Legacy System Modernization: Balancing Risk and Innovation."https://www2.deloitte.com/us/en/insights.html

[10] PwC Cybersecurity & Privacy: "Building a Secure and Compliant IT Infrastructure."https://www.pwc.com/gx/en/services/cybersecurity.html

[11] PCI DSS (Payment Card Industry Data Security Standard): "Requirements and Security Assessment Procedures."https://www.pcisecuritystandards.org/

[12] HIPAA (Health Insurance Portability and Accountability Act): "Security Rule and Compliance Guidelines."https://www.hhs.gov/hipaa/index.html

[13] GDPR (General Data Protection Regulation): "Official Guidelines and Compliance Resources." https://gdpr-info.eu/

[14] NIST Cybersecurity Framework (CSF): "Improving Critical Infrastructure Cybersecurity."https://www.nist.gov/cyberframework

[15] CIS Controls: "Center for Internet Security Critical Security Controls." https://www.cisecurity.org/controls/

[16] Microsoft Azure: "Best Practices for Securing Legacy Systems in the Cloud." https://azure.microsoft.com/en-us/resources/

[17] AWS Well-Architected Framework: "Security Pillar for Legacy System Modernization."https://aws.amazon.com/architecture/well-architected/

[18] Google Cloud: "Data Migration and Security Best Practices." https://cloud.google.com/security

[19] Red Hat: "Modernizing Legacy Applications with OpenShift." https://www.redhat.com/en/topics/modernization

[20] Cybersecurity and Infrastructure Security Agency (CISA): "Legacy System Modernization and Cybersecurity."https://www.cisa.gov/legacy-systems.