

In the era of artificial intelligence (AI)-enabled digital transformation, organizations frequently underestimate the significance of application security and controls. Consequently, this oversight has led to a notable increase in application-related audit findings, heightened risk exposure, internal fraud incidents, and missed opportunities for reducing the cost of compliance with automation.

Internal controls and audit risks of a cloud implementation

Key risks associated with digital transformation

Technology transformation

Business transformation

Cybersecurity

Expanded digital presence can cause increased exposure to cyberattacks and cyber

threats and

fraud

 Vulnerabilities in new technologies and applications can be exploited by malicious actors and fraudsters.

fraud.

- Phishing, ransomware, and other cyber threats can disrupt business operations and lead to data breaches.
- Insufficient monitoring and detection mechanisms, without Al-enhanced threat detection and fraud prevention, can allow malicious activities to go unnoticed.

Technology integration and interoperability

- Integrating new digital solutions with legacy systems can be difficult.
- Lack of interoperability between different technologies can lead to inefficiencies and increased operational complexity.
- Fragmented data silos can arise, preventing seamless data flow and analytics. Al can facilitate better data integration and analytics across systems.
- High costs and resource requirements for customizing and maintaining integrations between disparate systems can be reduced by Al-driven automation and efficiency improved.

Data privacy and compliance

- Handling large volumes of sensitive data increases the risk of data breaches.
- Noncompliance with data protection regulations (e.g., General Data Protection Regulation and California Consumer Privacy Act) can lead to hefty fines and legal consequences.
- Complexities may exist in how to manage data across different jurisdictions with varying regulations.
- Insufficient data encryption and access controls, which can be bolstered by Al-driven compliance checks, can result in unauthorized data access and loss of customer trust.

Operational disruptions

- Integration of new digital systems can cause disruptions in existing operations.
- Downtime or failures in critical systems can affect business continuity and service delivery.
- Lack of proper testing and validation of new systems can lead to unexpected failures and operational issues.
- Dependence on third-party vendors for digital solutions can create additional risks if they face outages or security breaches. Al can enhance predictive maintenance to foresee and prevent potential disruptions.

Change management and employee resistance

- Employees may resist changes due to fear of the unknown or lack of understanding.
- Inadequate change management processes can lead to decreased productivity and morale.
- There might be insufficient training and support for employees who need to adapt to new digital tools and processes.
- Misalignment between digital transformation goals and employee expectations can hinder successful adoption.
 Al can help personalize training programs to improve adoption rates.

Periodic evaluations





Program workstream

Proactive Trusted Application management strategy

To meet risk and compliance requirements effectively, we recommend implementing a proactive Trusted Application management strategy. This entails establishing a dedicated Trusted Application security and controls team with specialized expertise for conducting assessments at critical junctures during your implementation process. Additionally, leveraging Al-driven solutions can enhance these strategies by providing business-centric enablement, real-time monitoring, predictive analytics, and automated compliance checks for more robust security and control measures.

Critical stages throughout your implementation process require evaluation of your security and controls strategy, design, and utilization of automation opportunities

Iteration 1 (Design)

Iteration 2 (SIT)

Iteration 3 (UAT)

Iteration 4 (Post-Hypercare)

Our KPMG Trusted Application approach

KPMG provides customized support tailored to your implementation journey. Whether your organization needs assistance in designing and implementing Trusted Applications or requires a review for timely challenge resolution and refinement of control designs, we are here to help. Our commitment is to assist you at every stage of your journey, leveraging our Trusted Application solutions to enable robust risk and compliance management.

By focusing on risk and control considerations throughout the project lifecycle, you can address risks and redesign controls earlier, achieving cost savings and increased efficiency. KPMG has extensive experience collaborating with organizations during system implementations. We can adopt a collective approach to enhance efficiencies for your transformation project.

By focusing on risk and control considerations throughout the project lifecycle, you can address risks and redesign controls earlier, achieving cost savings and increased efficiency.

Potential benefits

User empowerment and security balance

Achieves an effective balance between application user empowerment and security, enabling users to more fully leverage the application's capabilities while the organization's confidential data and vital operations remain meticulously protected.



Deepening insights

Enhances insights into financial reporting's internal control impacts and helps ensure the integrity of underlying financial data.



Proactive issue identification

Quickly identifies potential audit/control issues and automated controls, helping to reduce surprises and enhancing test efficiency.



Streamlined audit planning

Keeps audit documentation updated with information technology changes and new processes for more streamlined audit planning and testing



Timely issue resolution

Enables management to promptly address project and control issues, safeguarding project timelines and objectives.



Cost-effective solutions

Identifies avenues for implementing more effective, cost-efficient automated application controls and highlights potential risks.

KPMG has extensive experience collaborating with organizations during system implementations. We can adopt a collective approach to enhance efficiencies for your transformation project.

Contact us



Mick McGarry Principal and Protection Offering Leader, KPMG LLP hmcgarry@kpmg.com 214-578-2225

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us:



kpmg.com

Subscribe

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

DASD-2024-15820