Balancing Risk & Innovation

Compliance Risk Management in Digital Transformations

Rapid changes in technology and customer preferences have driven financial institutions ("institutions") to move from outdated, siloed systems to flexible and innovative core platforms. This shift aims to better align with market trends and expectations. In today's digital-first environment, institutions face mounting pressures to advance their digital strategies while navigating an ever-changing compliance risk management landscape.

Whether embarking on a single system replacement or a comprehensive overhaul of an institution's technology ecosystem, embedding compliance objectives within the overall program's criteria is essential to promote customer satisfaction, regulatory adherence, and organizational efficiency. Successful digital transformations require compliance risk management to be integrated into the strategy, processes, people, and technology involved. An institution's second line of defense is a critical partner, collaborating with diverse subject matter professionals to design and implement technology architectures that effectively mitigate Compliance Risk.

By adopting the following practices, institutions can effectively balance the complexities of digital transformation with compliance risk requirements, ultimately achieving sustainable returns on their investments. As discussed below, engaging compliance professionals early in the process establishes a compliance-by-design posture, efficient operating routines, and continuous alignment with regulatory expectations to support the institution's long-term strategic goals.

Strategy

A well-defined digital transformation strategy, including compliance risk management objectives, should be established before any project begins. Three critical elements of this strategy are the intake process, impact assessment, and the compliance interaction model:

Intake Process

An established intake process supports the consistent implementation of change management activities and systematically evaluates each proposed digital transformation initiative from inception. The intake process should gather the comprehensive scope of the initiative to inform the risk profile of the project, identifying potential changes to the business, operations, systems, and technology, as well as any key internal stakeholders and other considerations.

Impact Assessment

An impact assessment can then be performed to identify the potential effects the project will have on the institution's current systems, operations, and risk profile, including the laws, rules, and regulations impacted. The assessment's results can help determine overall impact as well as assist with identifying the resources needed to monitor and execute the successful implementation. With a clear understanding of these data points, institutions can be proactive and develop a comprehensive plan for compliance risk management integration across the digital transformation implementation.

Compliance Interaction Model

Depending on the compliance risks involved, the level of the second line of defense's involvement in the project can range from providing occasional advisory support to being embedded within development teams. Whether the model calls for providing ad hoc advice or working closely with business and technology leaders, it is essential to have sufficient representation from the institution's second line of defense to manage complex compliance risks throughout the project.

Intake Process

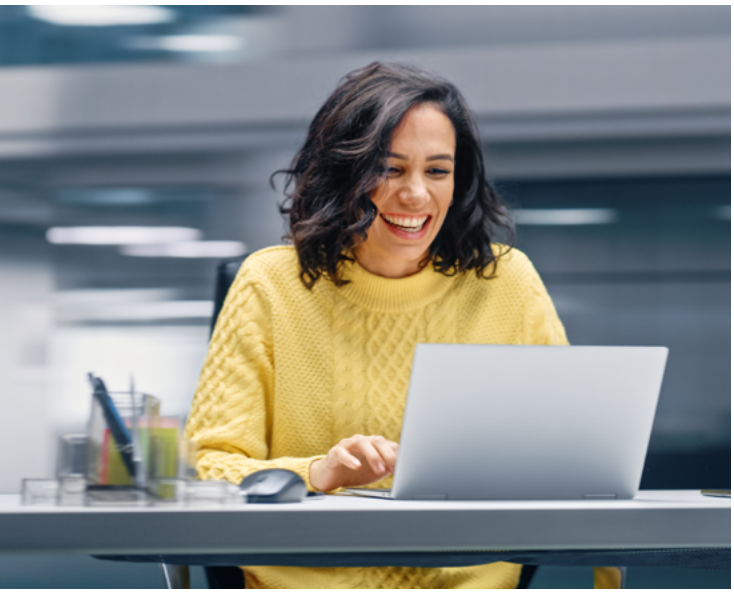
Outline the scope of the transformation, define the risk profile, and identify stakeholders.

Impact Assessment

Define potential effects across systems, operations, and other areas.

Compliance Interaction Model

Plan for the Compliance Function's role in the transformation and target state.



Process

Processes to manage compliance risks related to digital transformation projects should be scalable, effective, and pragmatic. A standardized framework should be used to support consistency across teams.

Key principles include:

Requirement Identification

Early involvement of skilled compliance professionals allows for the identification and integration of compliance requirements into the project scope. This minimizes potential timeline impacts and assures regulators of the commitment to compliance before and after implementation.

Traceability & Completeness

It is crucial to document how compliance risk was managed during the transformation. This includes key decisions as well as any recommendations made by compliance professionals and the disposition thereof. Project documentation should provide clear linkage and traceability to demonstrate that all regulatory requirements and internal policies are fully addressed and integrated into the new systems. The ability to prove the test strategy and scenarios were appropriate for the scope of development and impacted requirements is a core expectation for risk executives and regulators alike.

Operational Readiness

Ensuring operational readiness means the institution is prepared to handle new system functionalities and workflows seamlessly once the digital transformation goes live. This includes thorough testing of system capabilities throughout the development lifecycle and a well-defined plan to ensure changes are adopted in production. These activities should be embedded in the initiative as core milestones and include cross-team training, updates to policies, procedures, and customer-facing artifacts, enhancements to the compliance risk assessment, and documenting systemic controls as identified and/or designed through the transformation program. Additionally, organizations should establish clear success criteria and complaint trends that can be monitored to evaluate whether the program objectives and customer experience are meeting organizational targets.

People

Compliance professionals involved in digital transformation projects may need additional skills beyond their existing expertise to effectively support transformation efforts and sustainability. A skills assessment can identify necessary resources and training opportunities. Successful employees typically have a mix of compliance testing, project management, strategic thinking, communication, software development lifecycle knowledge, and understanding of institutional processes and technology.

The capacity of existing team members may also be stretched due to the pace and volume of change activities. Compliance support in digital transformations is not a part time role, organizations that successfully balance innovation speed with compliance risk mitigation often do so by dedicating full-time resources to transformation efforts.

Technology

Similar to the identification of automated processes and controls to support sustainable compliance, the second line of defense can play a strategic role in digital transformations to determine how the evolving technology architecture can enable an enhanced compliance program and compliance risk mitigation. There are generally three different ways that future focused financial institutions leverage transformation initiatives to enhance their control environment and design a sustainable compliance technology architecture:

System Configuration to Facilitate Compliance

Technology architecture can be configured for regulatory compliance through automated processes, such as accurately calculating interest rates and sending timely disclosures, which promotes adherence to regulatory standards and reduces human error. This automation streamlines compliance, provides audit trails as proof of adherence, reduces human error, and enhances consistency and reliability within the organization.

System Control Implementation

Advanced compliance management systems can encourage compliance through built-in controls such as system hard stops, edit checks, and permission management controls, preventing non-compliant transactions and unauthorized access or data modifications. These built-in controls establish that compliance policies are enforced consistently and prevent non-compliant activities from occurring within the system.

Downstream Data Flow Controls

Systems can generate exception reports that highlight anomalies or deviations from expected patterns, helping to detect potential non-compliance early and enabling organizations to pinpoint issues such as late submissions, data discrepancies, or unauthorized transactions. By establishing key thresholds and reports for regular review compliance professionals can identify potential risks and take corrective actions promptly, addressing any gaps in compliance to maintain adherence to regulatory standards.

Ultimately, leveraging these technological advancements can significantly strengthen the overall compliance framework, ensuring more effective risk management and operational efficiency.

How KPMG Can Help

KPMG has experience enabling compliance risk management within digital transformations in select engagements, based on client needs. Our team has assisted clients in various aspects of the technology implementation process, including strategy determination, process buildout, obligation identification and mapping, regulatory compliance testing, and post-implementation validation. Leveraging established assets, and a deep understanding of compliance expectations, KPMG is prepared to collaborate with you to design and deliver a solution tailored to your specific requirements. For further information on the topics discussed and to learn how KPMG has supported clients in their digital journeys, you are invited to contact our authors.

Contact us

Chad Polen
Partner, Advisory
T: 412-491-6006
E: cpolen@kpmg.com

Luke Friesen
Director, Advisory
T: 404-222-3223
E: lfriesen@kpmg.com

Amy Masters
Principal, Advisory
T: 412-208-6129
E: almasters@kpmg.com

Stephen Honeycutt
Director, Advisory
T: 980-280-5980
E: shoneycutt@kpmg.com

Contributed by Joshua Laguerre, Rita Tonleu, and Anna Huang

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

Learn about us: **kpmg.com**