Mitigating risk

Banking risk management has been significantly altered by the pandemic. Similar to the changing nature of the coronavirus, the risk profile evolved as consumer behavior and the economy changed. Several practices, like business continuity planning; governance, risk and compliance technologies; and technology risk management have become crucial to banking internal controls.

Business continuity management

The pandemic laid bare the need for banks to practice sound—but flexible—business continuity planning (BCP). Flexibility proved key—there are notable differences between traditional business continuity planning and pandemic planning. In particular, many banks' BCPs were not prepared for the duration of the shock to their business model brought on by the pandemic. Insuring continuity of functions such as deposit and lending services, ATMs and payment and settlement services only covered a bank for the initial shock. The lasting effects of the lockdown forced banks to enact continuity plans for more complex functions like counterparty exposure management, financial market operations and workforce management.

In addition to flexibility, a key metric for business continuity success is a bank's level of cross-functionality in its operations. Particularly, banks that used risk mitigation practices that broke silos within its operations proved the most resilient. Pre-pandemic silo breaking allowed for greater communication between departments as the crisis ramped up.

GRC technologies

As banks re-evaluate their internal control models to new risks, many are finding their models would benefit from greater cross-functionality and the implementation of governance, risk and compliance (GRC) technologies.

> As banks re-evaluate their internal control models to new risks, many are finding their models would benefit from greater cross-functionality and the implementation of governance, risk and compliance (GRC) technologies.

GRC technology-enabled products and services integrate, facilitate, streamline and maximize the efficiency and value of an organization's GRC strategy. Specifically, they provide configurable controls monitoring, access controls/segregation of duties (SOD) analysis, automation of access authorization, periodic attestation of system privileges and transaction analysis.

However, without proper planning, companies may not be using GRC technologies to their full potential. Tools designed to monitor and analyze GRC processes can become nothing more than a repository for documents, failing to support the comprehensive GRC program the company intended. Meanwhile, tools are often implemented in silos and a lack of process leads to conflicting opinions and efforts between business units.

With hindsight of the banking sector's internal controls failures during the pandemic, banks would be best served by diagnosing their organization's unique issues and building custom roadmaps as they reform their defense systems and implement new technologies.

GRC deliverables and accelerators:

- *GRC program implementation roadmap:* A clear path for the future is critical to the timely and transparent execution of program activities.
- *GRC data rationalization and data migration:* Data rationalization and cleaning, as well as a data migration strategy, enable a consistent and repeatable process for the onboarding of all data.
- *Testing strategy and evaluation criteria:* This includes prioritization of requirements, use cases and fit-gap analysis to provide a link between the business requirements and business process design.
- *Deployment and post-production support plan:* A successful implementation does not stop after go-live. A proactive approach to post-production support accelerates adoption of the solution and resolution of implementation issues.
- *People and change:* An effective communication, training, and implementation adoption monitoring ensures that the organization gets the full benefit of the investment.

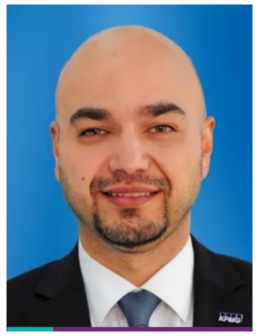
Technology risk management

The dual forces of the pandemic and technological advancement brought new risks to banks. Remote work exposed organizations to cybersecurity risks which were exploited by cybercriminals. In 2019 and 2020, intrusions threatening organizations grew 400% globally, according to CrowdStrike. That figure, in part, explains technology risk. New technologies—such as those allowing remote work—create vulnerabilities, especially soon after their implementation before governance is perfected. The remote work/cyber risk paradigm extends to other technologies, such as those facilitating digitalization in the banking sector.

Banks need to make sure technology risks are managed. Emerging technologies related to banking digitalization and fintech have increased the focus on technology risk management.

In addition to digitalization technology risk, IT risks such as security, outsourcing and disaster recovery are now at the forefront of risk management functions. C-suite executives are demanding that their information technology departments provide better insight on IT processes and controls, as well as greater anticipation and management of risks.

Artificial intelligence, cognitive computing, internet of things (IoT) and robotics are the top four technologies that will drive business transformation in the coming years. Future technology risk professionals will have to decipher the risks of new emerging technology and develop an agile technology risk framework with enough flexibility to respond to new risks. Some companies are taking steps to follow through on this objective. For example, we see clients using data analytics, continuous auditing and monitoring to change the way that they manage technology risk.



Mohammed Abudalo
Advisory Leader
E: mabudalo@kpmg.com

The path towards security beyond compliance

The benefits of strong cyber security are clear, but the path to get there is often fuzzy in large organizations. they will need to:

1. *Focus on embedding pragmatic remote working security controls* to deal with threats, including education of employees.
2. *Act to secure cloud* and other ad-hcc collaboration environments and seek assurance on security controls of managed services providers.
3. *Review and enhance business continuity management frameworks,* covering larger, more frequent and globally simultaneous events
4. *Test robustness of the banks' cyber resilience* and *optimize controls* while reducing cost of ownership.
5. *Plan to migrate to a security operating model* that enables higher levels of automation.