Regulatory and compliance

Technology-driven governance, risk and compliance

Bankers in Saudi Arabia faced one of their most challenging years of risk management in 2020. Similar to the changing nature of the coronavirus, the risk profile evolved as different aspects of peoples' lives and the economy were impacted by the pandemic. Authorities in Saudi Arabia worked to mitigate risks as they arose, but moving forward banks are expected to prepare themselves for a future without such unprecedented government support.

Business continuity management

The pandemic laid bare the need for banks to practice sound and flexible business continuity planning. Flexibility proved key – there are notable differences between traditional business continuity planning and pandemic planning. In particular, many banks' business continuity plans (BCPs) were not tested for the duration of the shock to their business model brought on by the pandemic. Ensuring 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 in 2020 was a bank's level of cross-functionality baked into 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.

Three lines of defense model

As banks evaluate their internal control models with hindsight of 2020, many are finding their models would benefit from greater cross-functionality and the implementation of government, risk, and compliance (GRC) technologies.

Tracking the ongoing methodological changes to internal risk controls has been the evolution of the Institute of Internal Auditor's (IIA) three lines of defense (3LoD) model, which was broadly instituted following the 2008-09 financial crisis. The 3LoD model, which encompasses internal controls into a first line of defense of front-line management, a second line usually within compliance and risk functions, and a third line in internal audit, has come under scrutiny for a number of shortfalls. Chiefly, organizations have found the model to be too limited and too restrictive.

In July 2020, an IIA working group renamed the 3LoD model to the "three lines model," which illustrates a widespread sentiment to change internal controls from a defensive operation to a key part of governance. This move came after organizations, already fragmented by operational separation brought on by the pandemic, failed to quickly and comprehensively respond to the pandemic. The IIA's change also follows a longer-running industry movement to enhance the cross-functionality of the 3LoD model, as illustrated by the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Internal Control – Integrated Framework. COSO's framework allows for combined assurance, which breaks down the barriers that were heightened by remote work and laid bare by the pandemic.

Liquidity risk

At the beginning of the pandemic, the major challenge for banks materialized as liquidity risk – the result of country lockdowns that caused deteriorating corporate revenues and drawdowns of credit facilities as well as national measures to ease payment pressures on individuals and businesses. SAMA stepped in and extended working capital finance to all corporates to address short-term liquidity requirements, a liquidity injection that was passed on to the corporates' banks.

> Particularly, banks that used risk mitigation practices that broke silos within its operations proved the most resilient.

As time went on, utilization of funds decreased and banks' positions improved, to the extent that liquidity is higher now when compared to pre-Covid-19 levels. LDR/SLR/NSFR ratios and overall cash positions have improved as a result. This liquidity is for good measure. Over the medium term, pressure is expected on liquidity management due to drawdowns, deferral in loan repayments together with stressed equity and bond markets.

Credit risk

As the crisis continued, banks and supervisors shifted their focus to credit quality and loan impairments. With many of their previous credit risk assessments turned on their heads by the pandemic, bankers in the Kingdom were often working with unreliable financial information on their obligors. This could not be solved by broad downgrades, as the pandemic did not affect all sectors equally. Resultingly, bank's internal ratings systems downgraded credit from corporate borrowers in sectors most impacted, such as tourism, hotels, and commodities.

For ongoing credit monitoring, credit risk departments are focusing on identifying the most relevant indicators to monitor, specifying the indicator changes that should trigger downgrades, and deciding when downgrades should be applied.

Market risk

In Saudi Arabia and all major oil-producing countries, market risk was driven up last year by record low oil prices. Combined with ongoing geopolitical risk in the region and global trade tensions, banks have operated within a dizzyingly complex market in 2020. Resultingly, asset prices have undergone unprecedented volatility, impacting trading books and increasing counterparty credit risk.

With analysts expecting a stabilization of oil prices in 2021, global supply chains repaired, and signs of regional geopolitical tensions easing, banks in the Kingdom are hopeful for decreased market risk moving forward.

Big questions remain for each of these risks. How long will government support for institutions and individuals last? What will happen to the price of oil as vaccination programs ease movement restrictions? Before any of these questions are answered, banks are preparing themselves through a number of internal control measures.

Risk mitigation through technology

Any bank's effort to increase the cross-functionality of their internal controls without GRC technologies falls short of the expectation. 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/SoD (Segretation of Duties) analysis, automation of access authorization, periodic attestation of system privileges, and transaction analysis.

However, without proper planning, banks 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.

Mohammad Abudalo
Risk and Compliance Lead
KPMG in Saudi Arabia

Mohammad Abudalo is specialized in GRC, internal audit and business process improvement, and has built his experience in these fields working with the firm in Jordan, Qatar, Bahrain and now Saudi Arabia. Aside from his work with financial institutions, he supported regional regulators to assess the progress in achieving the mandates of Federal Reserve and FATF workforce.