Technology governance in an evolving regulatory landscape

The advent of new and disruptive technologies like AI, cloud computing, decentralized ledger systems, machine learning, big data analytics, and high-speed connectivity has posed unprecedented opportunities and risk challenges to financial systems around the world.[13]

Central banks around the world internalize these changes by introducing laws, regulations, and policies to govern and provide a resilient environment to foster digital financial growth. They also recognize the urgency of looming IT and cybersecurity threats accompanying wider technology penetration in the financial services sector.

While digital transformation is vital for Saudi Arabia to accelerate economic growth, it comes with increased cybersecurity risks, especially when digital platforms are developed rapidly and adopted for sensitive activities. Preempting the rising trends in disruptions and risks, while balancing Saudi Arabia's commitment to economic development, will challenge the financial sector as it transforms.

SAMA has embraced the evolving FinTech landscape and is acting as a guardian and catalyst for financial growth and stability. SAMA understands the necessity of in-depth IT governance and regulatory compliance to bring a balance between FinTech adoption and IT risk management. Consequently, SAMA has published regulatory frameworks and policies to maintain a resilient cyber-secure environment that ensures business continuity. Collectively, the IT governance landscape will help the Kingdom achieve monetary and financial growth and stability in line with Vision 2030 and the Financial Sector Development Program (FSDP).

Preempting the rising trends in disruptions and risks, while balancing Saudi Arabia's commitment to economic development, will challenge the financial sector as it transforms.

IT governance

Technological innovation and advancement in finance exposes the financial sector to evolving risks. Due to these developments, IT governance has grown in prominence to balance the utilization of advanced technology with identifying and mitigating IT risks.

In this regard, SAMA is actively working with its member organizations to elevate their maturity across well-defined controls by year-end. The IT Governance Framework seeks to support member organizations on the effective and efficient use of technology to achieve their goals and manage risks associated with IT. For the holistic implementation of IT governance rules and guidelines across the organizations, this framework will be implemented in conjunction with other frameworks related to Open Banking, cybersecurity and business continuity.[14]

It is an opportune time for banks to reflect and look beyond compliance but rather towards the business value unlocked by the initiatives needed to confirm with the new IT Governance Framework. Financial institutions are adopting initiatives such as establishing an enterprise architecture practice, adopting a comprehensive Technology Risk Management Framework, developing a robust Software Development Life Cycle (SDLC), and instilling an independent Quality Assurance function. These accelerate digital transformation, improve their customers' experience, enable quicker, safer adoption of emerging technologies, and allow for better use of their data. The initiatives are paramount for banks to offer differentiated products and flourish as the financial sector transforms digitally.

Open Banking Initiative

The Saudi Central Bank envisages Open Banking as an opportunity to achieve financial inclusion and development of the financial sector in the country. Through Open Banking initiatives, SAMA provides a FinTech ecosystem to leverage data associated with account information and financial transactions to develop innovative, secure, and inclusive financial products and services.

In the first half of 2022, the Saudi Central Bank is planning to go live with Open Banking with the support of market participants.[15] The Open Banking ecosystem aims to spur economic growth with the participation of the private sector in line with Saudi Arabia's Vision 2030.

Cybersecurity

The fast-growing digital economy has accelerated the need for a robust cybersecurity structure in the financial sector. With this realization, Saudi Arabia is promoting the development of cyberthreat-resilient infrastructure and processes through cybersecurity laws, regulations, programs, and awareness campaigns.

SAMA has issued a Cybersecurity Framework that addresses the principles and guidelines for regulated entities to establish cybersecurity governance and build a resilient cybersecurity system with adequate preventive and detective controls.[16] SAMA recognizes the importance of maintaining confidentiality, integrity, and availability of financial services during technological disruptions and growing cyber threats. With the support of associated organizations, SAMA ensures that critical data, information, hardware, software applications, communication networks, premises, people, and overall operational infrastructure remain safe and secure.

Business Continuity Management

A well-connected and technology-led digital economy requires the continuity and availability of financial operations and services 24/7, without any disruption. The continuity of financial services is crucial for maintaining every other socioeconomic sector.

In 2017, SAMA introduced a Business Continuity Management Framework (BCMF) to ensure the continuous availability of financial services in the Kingdom during stable and disruptive times. This Framework establishes resilience among organizations to detect, prevent, and mitigate any potential threat and to continue the provision of critical financial services to its key stakeholders.[17] This framework includes Business Continuity Management best practices to ensure a minimum level of resilience is maintained by member organizations.

Future prospects

In the years ahead, disruptive financial technologies can bring forth a revolution in conducting business activities worldwide. Information Technologies are continuously evolving and dynamically changing the governance and regulatory compliance landscape.

The world is grappling with decentralized currencies and payment methods using blockchain technologies. At the same time, new cyber threats are evolving fast with increasingly malicious intentions. Remote work culture and decentralized financial systems with unhindered accessibility to organizational infrastructure have brought data and information security into focus. Therefore, continuous and more intensive efforts are required to safeguard the digital environment and achieve Vision 2030.

It is recommended for Saudi Arabia to ensure strict compliance to IT regulations in an ever-evolving digital landscape, which necessitates a specialized workforce that is well-versed in all facets of IT governance. Sustainable development will depend on innovation and transformation, which require a governed environment for conducting business.

Fadi Al Sheikh
Head of IT Strategy, Architecture & Enablement
E: falsheikh@kpmg.com