Saudi Central Bank issues IT Governance Framework

Simon Stokes - Senior Counsel - Digital & Data
 - Riyadh

At the end of 2021 the Saudi Central Bank (SAMA, formerly known as the Saudi Arabia Monetary Authority) issued its own information technology governance framework (Framework) for those organisations regulated by SAMA (Member Organisations). This is designed to enable Member Organisations to effectively identify and address risks related to IT. In this article, we provide a brief overview of the Framework and implications for Member Organisations subject to it.

Vision 2030 and financial technology

Saudi Arabia's Vision 2030 program anticipates the growth of financial technology and the move to a cashless society. A goal was set to increase electronic payments to 70% of all transactions by 2025. In 2021 SAMA announced that Saudi Arabia had the highest adoption of contactless payments through near-field communication (NFC) in the Middle East and North Africa – at 94% this adoption was also higher than the EU average and ahead of Hong Kong and China.

This is an impressive achievement and highlights the digital transformation that has taken root across the financial services sector in Saudi Arabia. Yet the widespread application of information technology (IT) to financial services is not without its risks.

Technology risk and the need for good governance

Cybersecurity threats are ever-present and hackers get ever more sophisticated. There is also the increasing use of cloud technology. Adoption of cloud technology brings benefits – access to cutting edge technology, cost efficiencies, and so on. But concerns have been raised about the resilience of cloud technology – if a major data centre provider

goes offline for any reason this could have a severe impact on a bank's operations, for example. Finally, not all digital transformation projects are successful – IT projects can fail to deliver and there have been some well-publicised failures internationally.

At the heart of the successful adoption and use of IT is good IT governance. This can help manage risk, ensure the resilience of IT systems, effectively manage change, and ensure legal compliance.

SAMA IT Governance Framework

Background

At the end of 2021 SAMA issued its own IT governance framework for its Member Organisations. This Framework is designed to enable Member Organisations to effectively identify and address risks related to IT. The Framework has the following objectives:

- creating a common approach for addressing IT risks
- achieving an appropriate maturity level of IT controls
- ensuring IT risks are properly managed

The Framework also specifies principles and requirements for initiating, implementing, maintaining, monitoring and improving IT governance controls within Member Organisations. The Framework is not stand-alone – it sits alongside SAMA's *Cyber Security Framework* and *Business Continuity Management Framework* as well as other SAMA requirements and circulars, including in relation to outsourcing and cybersecurity.

Target audience

The Framework states that its target audience is senior and executive management, business owners, owners of information assets, CIOs and those involved in defining, implementing and reviewing IT controls within Member Organizations.

Organizations that must comply

The Framework is applicable to Member Organizations regulated by SAMA. Member Organisations are responsible for implementing and complying with the Framework. SAMA is the owner of the Framework and is responsible for providing any required interpretation.

SAMA will review (and update, if required) the Framework periodically to assess its effectiveness, including addressing emerging IT threats and risks. Member Organizations can also request an update to the Framework, and SAMA will review the requested update, and adjust the next version of the Framework if appropriate.

How to achieve compliance

The Framework is 'risk' or 'principle' based. It specifies key IT governance principles and objectives that Member Organisations must adopt and achieve. The list of mandated control requirements provides additional direction and will need to be considered by Member Organizations in achieving the relevant objectives. When a certain control requirement cannot be adopted, the Member Organization needs to consider applying alternative and compensatory controls, following an internal risk acceptance process and obtaining a formal waiver from SAMA. The Framework sets out how to request a waiver in such circumstances.

The implementation of the Framework is subject to periodic self-assessment, performed by the Member Organization based on a questionnaire. The self-assessments will be audited by SAMA to determine the level of compliance and the IT maturity level of the Member Organization.

Key aspects of the Framework

The Framework has four aspects:

- IT governance and leadership
- IT risk management
- IT operations management
- System change management

Each of these domains then has subdomains focusing on a specific IT governance topic, for which the Framework identifies a principle and related control requirements. The Framework needs to be implemented in light of the principle along with its associated control requirements.

Many of the principles and controls will be familiar to those working in IT and largely relate to:

- management and organisational matters (such as the adoption of IT controls including IT policies, standards and procedures and use of key performance indicators (KPIs) and key risk indicators (KRIs))
- risk assessment and management

- technology (including secure computer code reviews and testing)

Legal aspects of the Framework

In addition, some of the principles and controls have a distinctly "legal" flavour to them. These include:

- **Regulatory compliance** – relevant regulations including data privacy need to be identified, communicated within the organisation and complied with. The controls here include the maintenance of an up-to-date log of relevant legal, regulatory and contract requirements together with their impact and required actions.
- **Manage service level agreements (SLAs)** – contract terms and conditions governing the roles, relationships, obligations and responsibilities of internal stakeholders and third parties need to be formally agreed, developed and managed. This applies to both internal and external SLAs. Where an organisation uses a third party service provider there needs to be a formal SLA in place meeting a range of requirements.
- **Change requirement definition and approval** – changes to information assets need to be defined, documented and approved by the relevant asset owner prior to implementing the change. The controls here include a formal change control process. This will have a contractual dimension where a third party vendor is involved.
- **System acquisition** – a process must be put in place to ensure the risks of any system acquisition (including related vendor service levels) are adequately assessed and mitigated before acquiring the system. The controls here include the need for a defined and approved set of system requirements (both functional and non-functional), an initial feasibility study (to assess both the requirements of the new system and its conformity with regulatory requirements) and a detailed implementation plan. These controls are common sense – they will help avoid later legal disputes if properly incorporated into the system acquisition contract.

Conclusion

The SAMA IT Governance Framework supplements the existing financial services IT regulatory framework in Saudi Arabia. It represents best practice – to comply will require a top down commitment and the involvement of stakeholders from IT Security, IT Operations, Procurement, Legal and Regulatory Compliance. Legal compliance and good contract management and drafting underpin a number of aspects of the Framework. It also highlights recent.

> *"The SAMA IT Governance Framework supplements the existing financial services IT regulatory framework in Saudi Arabia. It represents best practice – to comply will require a top down commitment and the involvement of stakeholders from IT Security, IT Operations, Procurement, Legal and Regulatory Compliance. Legal compliance and good contract management and drafting underpin a number of aspects of the Framework. It also highlights recent developments in Saudi Arabia such as the new data privacy law and the need for IT risk management processes to procure new and emerging technologies such as AI and blockchain."*

For further information, please contact http://Simon Stokes.