SAMA spotlight | ITGF | IT risk management

Kingdom of Saudi Arabia | 19 February 2023

keypoint

In November 2021, the Saudi Central Bank (SAMA) issued a circular on IT governance frameworks as part of its cybersecurity rules and instructions - with four intertwined domains: IT governance and leadership; IT risk management; IT operations management; and systems change management.

SAMA's risk-based IT risk management framework prescribes IT principles - a main set of IT controls - and control requirements - mandated IT controls which provide additional direction. Where control requirements cannot be implemented, SAMA licensees are expected to apply compensating controls, formally accept any ensuing risk and request a formal waiver from that control from SAMA. The IT risk management domain includes four focus areas:

- Managing IT risks
- Risk identification and analysis
- Risk treatments
- Risk reporting, monitoring and profiling

Principles/expectations
▪ IT risk management processes defined, approved, implemented, communicated and aligned with ERM processes
▪ Assets identified, recorded and maintained
▪ Controls and risks analysed based on likelihood of occurrences and resulting impact
▪ IT risks associated with IT assets treated based on applicable criteria
▪ IT risks treated according to defined treatment plans and effectively reviewed, monitored and reported

Work products and other outcomes:

- IT risk management process
- IT risk treatment plan
- IT key risk indicators
- IT risk assessment results
- IT risk register
- IT risk profile

Contact us:

Srikant Ranganathan
Senior Director
srikant.ranganathan@keypoint.com
+966 50 063 8273

Tom Gilbert
Director
tom.gilbert@keypoint.com
+966 53 250 9866

Darrshan Manukulasooriya
Senior Manager | IT Consulting
darrshan.m@keypoint.com
+966 55 395 1254

Muhammad Nauman Chisty
Assistant Manager | IT Consulting
nauman.chisty@keypoint.com
+966 13 845 9237

Yusuf Nooruddin
Assistant Consultant | IT Consulting
yusuf.nooruddin@keypoint.com
+966 13 845 9232