keypoint

In March 2022, the Saudi Central Bank (SAMA) issued a circular on cyber threat intelligence (CTI) principles as part of the threat management section of its cyber security framework (CSF). SAMA recognises that cyberattacks are an increasingly significant challenge to its licensees, with threat actors (TAs) continuously evolving. CTI enables targets - including regulators and the organisations they regulate - to collect, analyse and share data on cyber threats. A better understanding of existing and emerging cyber threats empowers the proactive anticipation of attacks and protects critical information assets.

SAMA CTI principles	Core	Strategic	Operational	Technical/tactical
Overview	Production and sharing of threat intelligence	TAs' intent and motivations	TAs' operations, behaviours and techniques	Technical elements /components of cyber attacks
Develop:	▪ Roles and responsibilities ▪ Threat intelligence plans ▪ Standard operating procedures (SOPs) ▪ Information classification process	• Requests for information (RfIs)	▪ Attack chain methodology	▪ Mechanisms to collect indicators of compromise (IoCs) ▪ Monitoring policy and procedures ▪ Process flows to aggregate IoC process

Assessing CTI maturity:

Assess current practice against SAMA's CTI maturity framework

Gap assessment

Policy update

Use findings from gap assessment to update CTI policies across all four SAMA CTI domains

Maturity assessment

Assess maturity of both current and to be CTI frameworks

Contact us:

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

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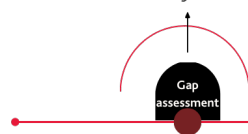tom.gilbert@keypoint.com
+966 53 250 9866

Sagar Rao
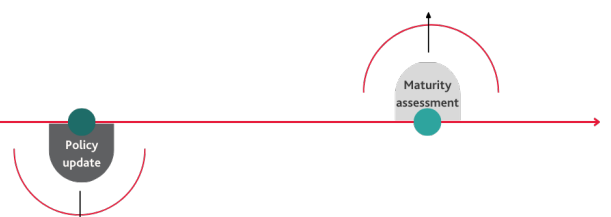Manager | IT consulting
sagar.rao@keypoint.com
+966 55 739 6033

Aditya Brijpuria
InfoSec SME | IT consulting
aditya.brijpuria@keypoint.com
+966 13 845 9232