SAUDI ARABIAN MONETARY AUTHORITY (SAMA) CYBERSECURITY FRAMEWORK – APPROACH DOCUMENT

NETWORK INTELLIGENCE
Global cybersecurity provider

INTRODUCTION

Saudi Arabian Monetary Authority established a Cybersecurity Framework to enable Financial Institutions regulated by **SAMA** ("the Member Organisations") to effectively identify and address risks related to cybersecurity. To maintain the protection of information assets and online services, the Member Organisations must adopt the framework.

OBJECTIVES

The objectives of the framework are as follows:
.

- To create a common approach for addressing cybersecurity within the Member Organisations.
- To achieve an appropriate maturity level of cybersecurity controls within the Member Organisations.
- To ensure cybersecurity risks are properly managed throughout the Member Organisations.

SCOPE

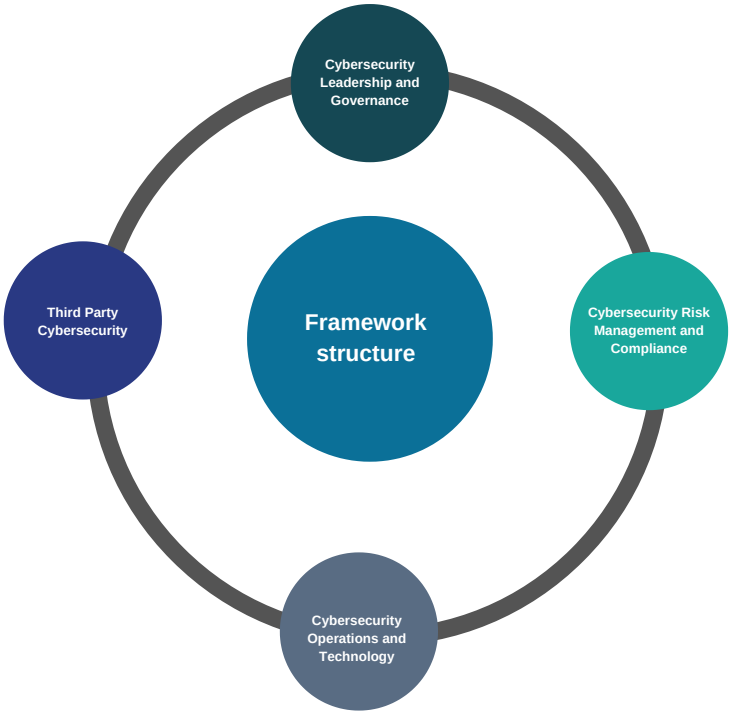
The Framework provides cybersecurity controls which are applicable to the information assets of the Member Organisation, including:

- Electronic information.
- Physical information (hardcopy).
- Applications, software, electronic services and databases.
- Computers and electronic machines (e.g., ATM).
- Information storage devices (e.g., hard disk, USB stick).
- Premises, equipment and
- communication networks (technical infrastructure)

SAMA FRAMEWORK STRUCTURE

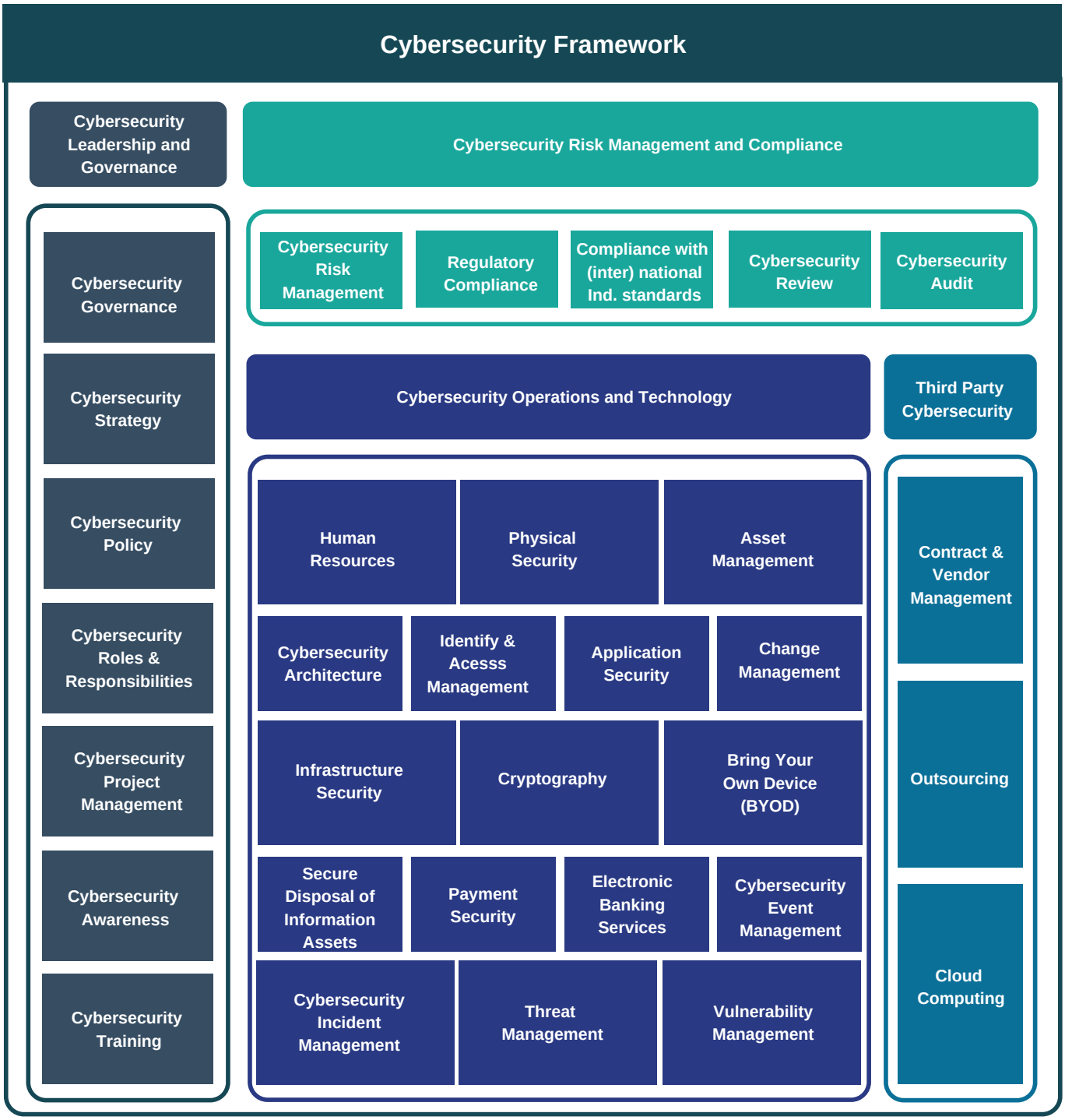
The Framework is structured around four main domains, namely:

- Cybersecurity Leadership and Governance.
- Cybersecurity Risk Management and Compliance.
- Cybersecurity Operations and Technology.
- Third-Party Cybersecurity.



SAMA FRAMEWORK METHODOLOGY

Following are the sub-domains that needs to be complied in order to adhere to SAMA cybersecurity framework.



CYBERSECURITY MATURITY LEVELS

The cybersecurity maturity level will be measured with the help of a predefined cybersecurity maturity model. The cybersecurity maturity model distinguishes 6 maturity levels (0, 1, 2, 3, 4 and 5), which are summarized in the table below. In order to achieve levels 3, 4 or 5, a Member Organisation must first meet all criteria of the preceding maturity levels.

Maturity Level	Definition & Criteria	Explanation
0 Non-existent	• No Documentation • There is no awareness or attention for certain cybersecurity control	• Cybersecurity controls are not in place. There may be no awareness of particular risk area or current plans to implement such cybersecurity controls
1 Ad-hoc	• Cybersecurity controls is not or partially defined. • Cybersecurity controls are performed in an inconsistent way. • Cybersecurity controls are fully defined.	• Cybersecurity control design and varies by department or owner. • Cybersecurity control design may only partially mitigate the identified risk and execution may be inconsistent.
2 Repeatable but informal	• The execution of the cybersecurity is based on an informal and unwritten, though standardised, practice.	• Repeatable cybersecurity control are in place. However, the control objectives and design are not formally defined or approved. • There is limited consideraton for a structured review or testing of a control.
3 Repeatable but informal	• Cybersecurity controls are defined, approved and implemented in a structure and formalised way. • The implementation of cybersecurity controls can be demostrated.	• Cybersecurity policies, standards and procedures are established. • Compliance with cybersecurity documentation ie. policies, standards and procedures is monitored preferably using a governance, risk and compliance tool (GRC). • key performance indicators are defined, monitored and reported to evaluate the implementation.
4 Managed and Measurable	• The effectiveness of the cybersecurity controls are periodically assessed and improved when necessary. • This periodic measurement, evaluations and opportunities for improvement are documented.	• Effectiveness of cybersecurity controls are measured and periodically evaluated. • Key risk indicators are trend reporting are used to determine the effectiveness of the cybersecurity controls. • Results of measurement and evaluation are used to identify opportunities for improvement of cybersecurity controls.
5 Adaptive	• Cybersecurity controls are subject to continuous improvement plan.	• The enterprise wide cybersecurity program focuses on continuous compliance, effectiveness and improvement of the cybersecurity controls. • cybersecurity controls are integrated with enterprise management framework and practices. • Performance of cybersecurity controls are evaluated un peer and sector data

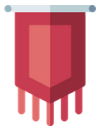
NETWORK INTELLIGENCE APPROACH OR METHODOLOGY TO ACHIEVE SAMA MATURITY LEVEL 3/4

Maturity Level 3

Network Intelligence will define & assist in implementing cybersecurity controls for the organization.

Network Intelligence will prepare cybersecurity documentation that incorporates cybersecurity policies, cybersecurity standards and cyber security procedures that will clearly indicate “why”, “what” and “how” cybersecurity controls should be implemented for their customers.

Network Intelligence will assist in preparing the cybersecurity policy and ensure that policy is endorsed and mandated by the board of the Member Organization. Network Intelligence will ensure that policy highlight which information assets must be protected and “what” cybersecurity principles and objectives should be established by the customer.



Network Intelligence will assist in preparing the cybersecurity standards. These standards define “what“ cybersecurity controls must be implemented, such as security and system parameters, segregation of duties, password rules, monitoring events and back-up and recovery rules. Network Intelligence will ensure that standards support & reinforce the cybersecurity policy and are to be considered as cyber security baselines.

Cybersecurity procedures will be further prepared by Network Intelligence that incorporates the step-by-step tasks and activities that should be performed by staff, third parties or the customers. These procedures will further prescribe “how” the cybersecurity controls, tasks and activities have to be executed in the operating environment and support the safeguarding of the information assets of the customer according to the cybersecurity policy and standards.

The process in the context of this framework will be defined by Network Intelligence as a structured set of activities designed to accomplish the specified objective.

Key performance indicators (KPIs) will be defined by the Network Intelligence to ensure actual progress of the implementation, performance and compliance of the cybersecurity controls is periodically monitored & evaluated.

NETWORK INTELLIGENCE APPROACH OR METHODOLOGY TO ACHIEVE SAMA MATURITY LEVEL 3/4

Maturity Level 4

To achieve maturity level 4, Network Intelligence will assist to periodically measure and evaluate the effectiveness of implemented cybersecurity controls.

In order to measure and evaluate whether the cybersecurity controls are effective, key risk indicators (KRIs) will be defined by the Network Intelligence for the customer. KRI indicates the norm for effectiveness measurement and should define thresholds to determine whether the actual result of the measurement is below, on, or above the targeted norm.

KRIs defined by the Network Intelligence are used for trend reporting and identification of potential improvements in near future.

DETAILED SAMA FRAMEWORK IMPLEMENTATION METHODOLOGY

Stage 1 : Planning of SAMA Framework

Purpose	**The purpose of this phase is to provide the initial planning and preparation for the assignment. The steps in this phase help re-emphasize the project objectives and goals and plan the various focus / target areas to be considered during the assignment.**
Tasks	**SAMA Project Kick Off** **Conduct a Project Kick-off Meeting: The team will meet with client management to confirm the proposed approach and draw up the project plan. In this phase, we will** • **Agree upon the scope and objectives of the SAMA framework assignment.** • **Identify individuals required to participate in project.** • **Establish project time frames.** **Understanding current Business Operations** • **Gain an insight into the business objectives of and business operations of the customer.** • **Gathering organisational details through extensive interactions with different levels of management and thorough analysis of operational documents.** • **Perform a comprehensive review of the various business processes and supporting information systems.** **Existing documentation review from SAMA framework perspective** • **Review of existing policy and procedures from SAMA framework perspective.** • **Review of Information Security Objectives.** • **Risk assessment and risk treatment methodology.** • **Review of IT procedures.** • **Review latest VA/PT test results.** **Perform SAMA framework Gap Analysis across following key domains** • **Cybersecurity Leadership and Governance.** • **Cybersecurity Risk Management and Compliance.** • **Cybersecurity Operations and Technology.** • **Third Party Cybersecurity**
Deliverables	• **Detailed Project Plan.** • **Finalization of SAMA framework Scope.** • **SAMA Objectives Plan for Aligning the Organisational Objectives with the Information Security.** • **Performing SAMA Gap Analysis.** • **Review report on the identified gaps in the existing document.** • **Gap Analysis Report**

DETAILED SAMA FRAMEWORK IMPLEMENTATION METHODOLOGY

Stage 2: Cyber security risk management & compliance review

Purpose	**The purpose of this phase to perform a comprehensive Risk Assessment on the identified critical Information Assets that would enable the team to select appropriate risk mitigation controls in line with SAMA framework.**
Tasks	**Risk management sub-domains under review** **Following risk management domains will reviewed as part of this phase:** • **Cyber security risk management.** • **Regulatory compliance.** • **Compliance with international industry standards.** • **Cybersecurity review.** • **Cybersecurity audits.** **Risk Assessment** • **Identification of processes and sub-processes** • **Identification of existing controls** • **Identification of risks on the processes and sub- processes correlated with the critical assets** • **Calculating the risk based on the impact and likelihood of occurrence.** **Risk Treatment** • **Discussions with the department heads/team members to evaluate the applicable SAMA controls** • **Evaluating the risk treatment options based on the severity of risk** • **Documentation of a detailed treatment plan for treatment of the risk** • **Identify the residual risk after the implementation of controls.**
Deliverables	• **Risk Assessment Report.** • **Risk Mitigation and Treatment Plan**

DETAILED SAMA FRAMEWORK IMPLEMENTATION METHODOLOGY

Stage 3: Documentation of Policies & Procedures

Purpose	**The purpose of this stage is to develop detailed and functional information security policies and procedures for the client in compliance with SAMA framework.**
Tasks	**Assistance for SAMA Documentation** • **SAMA policies and procedures creation** • **Mandatory and non- Mandatory documents for compliance to SAMA framework** **Assistance for Technical Documentation** **Following policies will be created and reviewed as part of this phase:** • **Human resource security policy.** • **Physical security policy.** • **Asset management policy.** • **Identity and access management policy.** • **Application security policy.** • **Change management policy.** • **Cryptography policy.** • **BYOD policy.** • **Security disposal if information assets policy.** • **Cybersecurity event management policy.** • **Cybersecurity incident management policy.** • **Vulnerability management policy.** • **Contracts and vendor management policy.** • **Outsourcing policy.** • **Cloud computing policy.** **Defining Monitoring Plan** **Defining Information Security Metrics based on:** • **What will be monitored.** • **When it will be monitored.** • **Who will monitor?** • **How it will be monitored.** • **When the review will be done.** **Ensuring the implemented controls remain effective.** **Defining plan of action for ineffective controls.**
Deliverables	• **Information Security Policy document** • **SAMA cybersecurity Policies and Procedures** • **Security metrics**

DETAILED SAMA FRAMEWORK IMPLEMENTATION METHODOLOGY

Stage 4: Network Intelligence assistance in achieving maturity level 3 & 4

Purpose	**The main purpose of this stage is to provide the client assistance in achieving maturity level 3 & 4 in line with SAMA cybersecurity framework.**
Tasks	**Maturity Level 3** **Network Intelligence will assist in following tasks to the client to achieve Maturity level 3 :** **• Network Intelligence will define & assist in implementing cybersecurity controls for the organisation.** **• Network Intelligence will prepare cyber security documentation that incorporates cyber security policies, cyber security standards and cyber security procedures that will clearly indicate "why", "what" and "how" cybersecurity controls should be implemented for their customers.** **• Network Intelligence will assist in preparing the cybersecurity policy and ensure that policy is endorsed and mandated by the board of the Member Organisation. Network Intelligence will ensure that policy highlight which information assets must be protected and "what" cyber security principles and objectives should be established by the customer.** **• Network Intelligence will assist in preparing the Cybersecurity standards. These standards define "what" cyber security controls must be implemented, such as security and system parameters, segregation of duties, password rules, monitoring events and back-up and recovery rules. Network Intelligence will ensure that standards support & reinforce the cyber security policy and are to be considered as cyber security baselines.** **• Cybersecurity procedures will be further prepared by Network Intelligence that incorporates the step-by-step tasks and activities that should be performed by staff, third parties or the customers. These procedures will further prescribe "how" the cyber security controls, tasks and activities have to be executed in the operating environment and support the safeguarding of the information assets of the customer according to the cyber security policy and standards.** **• The process in the context of this framework will be defined by Network Intelligence as a structured set of activities designed to accomplish the specified objective.** **• Key performance indicators (KPIs) will be defined by the Network Intelligence to ensure actual progress of the implementation, performance and compliance of the cybersecurity controls is periodically monitored & evaluated.** **Maturity Level 4** **Network Intelligence will assist in following tasks to the client to achieve Maturity level 4:** **• To achieve maturity level 4, Network Intelligence will assist to periodically measure and evaluate the effectiveness of implemented cybersecurity controls.** **In order to measure and evaluate whether the cybersecurity controls are effective, key risk indicators (KRIs) will be defined by the Network Intelligence for the customer. KRI indicates the norm for effectiveness measurement and should define thresholds to determine whether the actual result of measurement is below, on, or above the targeted norm.** **KRIs defined by the Network Intelligence are used for trend reporting and identification of potential improvements in near future.**
Deliverables	• **Maturity level road map and assistance.** • **Maturity level 4 road map and assistance.**

ABOUT US

We are a global cybersecurity provider founded in 2001 with more than 600+ team members working out of our New York, Singapore, Dubai and Mumbai offices. We offer services across 6 broad spectrums - Assessment, BCMS, GRC, Professional Services, MSSP & Trainings. We serve customers across industry verticals such as Banks and Financial Services, Technology and Media, Oil & Power, Airlines, E-commerce, Retail, etc. We believe that cybersecurity is not a destination, it is a journey and we partner with our clients to address the dynamic cybersecurity threat landscape.

US | Singapore | India | UAE | KSA

info@niiconsulting.com

www.niiconsulting.com