

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

# مؤسسة النقد العربي السعودي

المركز الرئيسي

الإدارة العامة للرقابة على البنوك



الرقم :

( ٣٣ )

المرفقات :

تعميم

المحترم

سعادة

بعد التحية:

الموضوع: استراتيجية أمن المعلومات للقطاع المصرفي.

أشير إلى التقدم التقني والثورة المعلوماتية التي يشهدها العالم حيث أصبحت الجهات المالية تتنافس في تقديم الخدمات الإلكترونية والاعتماد بشكل كبير على التقنية في ممارسة أعمالها. وبالرغم من تقديم التقنية للعديد من التسهيلات إلا أنه يصاحبها العديد من المخاطر التي يخشى أن تؤثر على سرية ودقة وتوافر المعلومات. كما لا يخفى عليكم تزايد الهجمات الإلكترونية عالمياً وإقليمياً والتي تستهدف العديد من البنى التحتية والتي من أهمها القطاع المصرفي الذي هو أحد ركائز الاقتصاد الوطني. لذا رأت مؤسسة النقد العربي السعودي من منطلق دورها الإشرافي والرقابي تطوير استراتيجية شاملة لأمن المعلومات للقطاع المصرفي ( Cyber Security Strategy of the Saudi Banking Sector) مستندة على أفضل الممارسات والتجارب العالمية. وعليه قامت المؤسسة خلال الفترة الماضية بالتعاون مع البنوك والمصارف العاملة بالمملكة من خلال لجنة مدراء أمن المعلومات البنكية وأحد المكاتب الاستشارية بتطوير هذه الاستراتيجية وعقد العديد من ورش العمل وزيارات للبنوك والمصارف ومقابلة مسؤولي أمن المعلومات والجهات ذات العلاقة. بالإضافة لأخذ مرثيات جميع البنوك والمصارف حيال مسودة الاستراتيجية المرسله لهم بالخطاب رقم ١٣٣٢٢.١٠٠٠.٣٨١ وتاريخ ٢٠٣/٠٢/١٤٣٨هـ حيث كانت مشاركة البنوك فعالة مما ساهم في صياغة الاستراتيجية بشكلها النهائي.

وعليه يسرني أن أرفق لكم النسخة النهائية للاستراتيجية الخاصة بأمن المعلومات للقطاع المصرفي حيث يتعين على البنك/ المصرف الالتزام بالآتي:

أولاً: عرض الاستراتيجية على مجلس الإدارة والتأكيد على الإدارة التنفيذية والإدارات ذات العلاقة في البنك/ المصرف بدعم هذا التوجه الاستراتيجي للمؤسسة نحو تأسيس سياسات وبيئة أمن معلومات ناضجة.

ثانياً: التأكد من أن استراتيجية أمن المعلومات الخاصة بالبنك/ المصرف متوافقة ومتناغمة مع استراتيجية القطاع المصرفي، وتزويد إدارة أمن المعلومات بالكفاءات البشرية والأدوات والتدريب المناسب.

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

## مؤسسة النقد العربي السعودي

المركز الرئيسي

الإدارة العامة للرقابة على البنوك

التاريخ : \_\_\_\_\_

الرقم : \_\_\_\_\_

الموافق : \_\_\_\_\_

المرفقات : \_\_\_\_\_

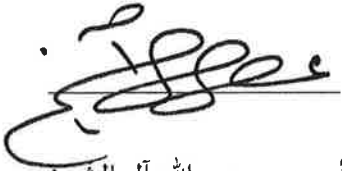
ثالثاً: تبني تطبيق استراتيجية أمن المعلومات للقطاع المصرفي وما ينبثق منها من مبادرات لتحقيق الأهداف الإستراتيجية شاملة المستهدفات التي ستكون مدرجة ضمن كل مبادرة.

رابعاً: دعم ممثلي البنك/ المصرف المشاركين مع فرق العمل في إعطاء تبني الاستراتيجية الأهمية العالية وعمل مراجعة دورية مع الإدارة التنفيذية ومجلس الإدارة للاطلاع على المستجدات والتأكد من تذليل جميع العقبات التي تواجه فرق العمل المشتركة في المهام الموكلة لهم.

ومما تجدر الإشارة إليه أن تطبيق الاستراتيجية يتطلب تكامل وتضافر الجهود المادية والبشرية بين المؤسسة والبنوك لإنجاز هذا العمل الوطني الهام، ونفيدكم أن المؤسسة ستقوم بترتيب اجتماع مع مدراء أمن المعلومات لشرح آلية التنفيذ وتكوين فرق العمل وذلك لتحقيق الأهداف المنشودة. وفي حال وجود أي استفسار يمكنكم التواصل مع مدير مخاطر تقنية المعلومات البنكية الأستاذ/ مروان بن حمد اللحيدان على الرقم ٤٦٣٣٠٠٠ تحويلة ٥٨١٨ أو بريد إلكتروني [maalohaidan@sama.gov.sa](mailto:maalohaidan@sama.gov.sa).

رئيس

وتقبلوا خالص تحياتي،،،  
العيسى



أحمد بن عبدالله آل الشيخ

وكيل المحافظ للرقابة

نطاق التوزيع:

\* البنوك/ المصارف العاملة في المملكة العربية السعودية

\* شركات المعلومات الانتمانية



مؤسسة النقد العربي السعودي  
Saudi Arabian Monetary Authority

# **Cyber Security Strategy of the Saudi banking sector**

**Saudi Arabian Monetary Authority**

**Version 1.0**

**March, 2017**



---

## Foreword

We live in a digital society with high expectations of flawless customer experience, continuous availability of services and effective protection of sensitive data. Information and online services are now strategically important to all public and private organizations, as well as to the broader society.

Recent cyber incidents globally and regionally have indicated that the number, impact and sophistication of cyber-attacks have increased steadily. It is worth noting that the malicious use of technology could have cross border implications, thereby disrupting both the national and international financial stability.

The Saudi Arabian Monetary Authority is proud to announce the Cyber Security Strategy to drive continuous improvement of cyber security and to ensure that the Saudi banking sector is well prepared in the five cyber security domains, namely: identification, protection, detection, response and recovery.

The strategy recognizes the rate at which the cyber threats are evolving, as well as the changing technology and business landscape. This places a premium on agility and flexibility in cyber security, underpinned by comprehensive intelligence on cyber threats and effective collaboration between SAMA and other member organization.

We strongly believe that the Cyber Security Strategy will set the sector on strong foundations to address present and future threats.

Ahmed Al Sheikh

Deputy Governor for Supervision



## Contents

Foreword .....	2
<b>1 The Importance of Cyber Security.....</b>	<b>5</b>
1.1 The Rationale for Cyber Security .....	5
1.2 Challenges and Threat Landscape.....	5
<b>2 The Cyber Security Strategy Highlights .....</b>	<b>5</b>
2.1 Mission, Vision, Objectives and Governing Rules .....	6
2.2 Scope.....	6
2.3 Governance .....	6
2.4 Principles for Implementation .....	7
2.4.1 Shared Responsibilities .....	8
2.4.2 Management Commitment and Funding .....	8
2.4.3 Integrated Planning.....	8
2.4.4 Monitor Progress and Improvements.....	9
2.5 Maintaining and Evaluating the Cyber Security Strategy .....	9
<b>3 The Cyber Security Strategic Objectives, Streams and Initiatives.....</b>	<b>10</b>
3.1 Objective 1: Proactively Protect Saudi banking sector Critical Information Assets.....	10
3.1.1 Critical Information Assets.....	11
3.1.2 Strategic Cyber Threat and Attack Scenarios.....	11
3.1.3 Strategic Cyber security risk assessment.....	11
3.2 Objective 2: Detect, Respond to and Recover from Cyber Security Incidents .....	12
3.2.1 Cyber Security Monitoring and Detection .....	13
3.2.2 Cyber Threat Intelligence Sharing.....	13
3.2.3 Cyber Security Incident Management .....	13
3.2.4 Cyber Security Crisis Management .....	13
3.3 Objective 3: Foster a Cyber Security Culture .....	14
3.3.1 Education and Awareness.....	15
3.3.2 National Training Capabilities and Talent Management .....	15
3.3.3 Contracting Cyber Security Services .....	15
3.4 Objective 4: Understand and Manage Interdependencies.....	16
3.4.1 National Interdependencies .....	17
3.4.2 International Interdependencies .....	17





---

3.5	Objective 5: Maintain an Adaptive Cyber Security Framework.....	18
3.5.1	Cyber Security Framework.....	19
3.5.2	Periodic Self-Assessments and Reviews .....	19
Appendices .....		20
Appendix A – Glossary .....		21
Appendix B – Detailed Initiatives Objectives and Expected Outcome.....		24

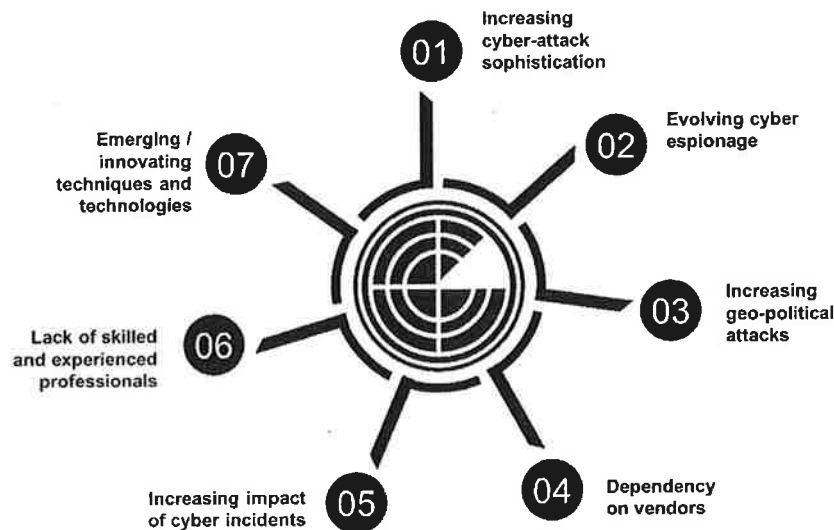
# 1 The Importance of Cyber Security

## 1.1 The Rationale for Cyber Security

Public cyber incident disclosures over the past few years have indicated that the number, impact and sophistication of cyber-attacks have increased steadily. This trend is especially true within the global banking sector and the Kingdom of Saudi Arabia. At the same time, as mentioned in the foreword, banking customers have ever increasing expectations for service availability, privacy, usability – expectations that can only be met via information technology and its continual innovation. This innovation often results in new business models that increase reliance on third parties and external resources, complicating governance and supply chains. As a result of these trends, the Saudi Arabian banking sector (“the Sector”) must improve cyber security throughout its ecosystem to counter malicious threats while also delivering on its promise to provide safe and efficient transaction services to its customers. The strategy contained in this document has been developed to achieve these objectives in a structured way, based on international best practices.

## 1.2 Challenges and Threat Landscape

Today’s threat landscape is diverse and advanced. Threat actors, ranging from individual hackers and insiders to organised groups, exploit sophisticated attacks. Their goals are diverse from espionage, financial gain to online (h)activism. The most significant cyber security threats and challenges to the Saudi banking sector which have been considered when developing the strategy (“the Strategy”) are summarised below:



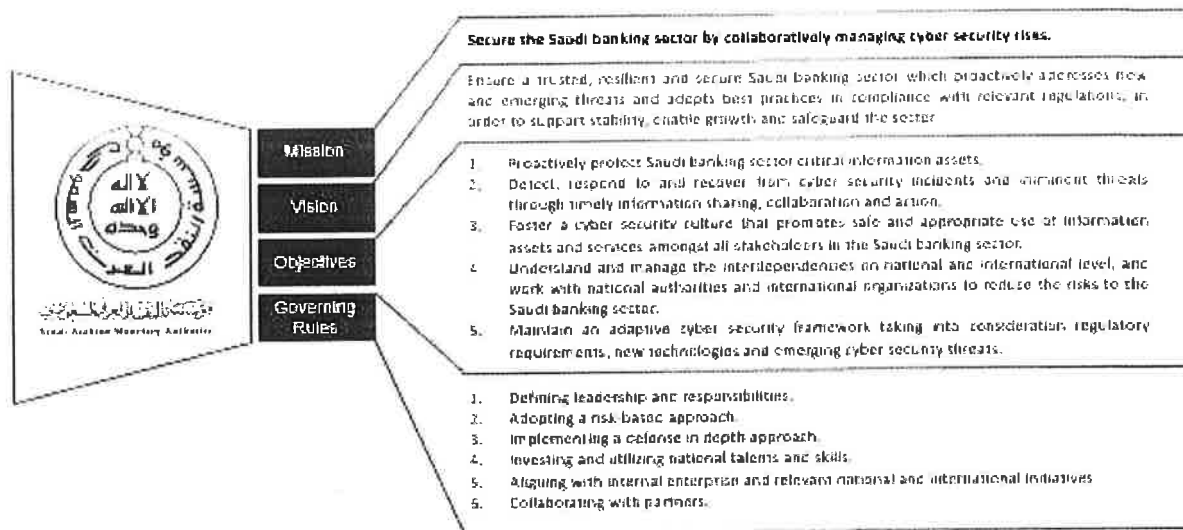
## 2 The Cyber Security Strategy Highlights

Cyber security is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats.



## 2.1 Mission, Vision, Objectives and Governing Rules

The table below illustrates the mission, vision, objectives and governing rules for cyber security within the Saudi banking sector.



## 2.2 Scope

In order to fulfil the mission, SAMA has collaborated with the Banking Committee for Information Security (BCIS) to develop this Strategy, which is applicable to the whole Saudi banking sector, including:

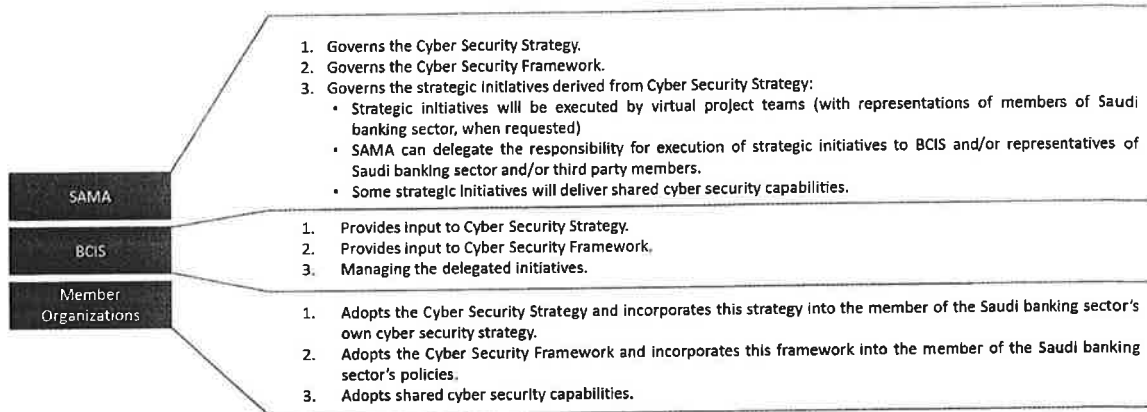
- the Saudi Arabian Monetary Authority;
- all organizations affiliated with SAMA (“the Member Organizations”);
- all banks operating in Saudi Arabia;
- all banking subsidiaries of Saudi banks situated within Saudi Arabia or abroad;
- subsidiaries of foreign banks situated in Saudi Arabia.

## 2.3 Governance

A robust governance structure will be put in place to direct, monitor and evaluate efforts related to the execution of Strategy. The governance structure will ensure that all parties involved are fully aware of their roles and responsibilities in the execution and the maintenance of the Strategy.



The parties involved and their role and responsibilities are summarized below:



## 2.4 Principles for Implementation

The implementation of the Strategy will be through a comprehensive set of strategic streams which together achieve the objectives of the Strategy.

A 5 year roadmap will set out how the strategic streams will be taken forward but will also recognize the need for the Strategy to be periodically evaluated under the governance of SAMA. Where necessary, the Strategy will be refined and new initiatives are to be defined if required.

The challenge of building a trustworthy, resilient and secure Saudi banking sector requires an integrated and collaborative approach in a number of domains:

- State of the art capabilities in identification, protection, detection, response and recovery.
- An organizational culture that promotes safe and appropriate use of information and online services among stakeholders.
- A deep understanding of dependencies on national critical infrastructure and online services, and seamless cooperation with national authorities to reduce the cyber security risks.

A successful cyber security strategy is founded on collaboration. All parties involved must join forces by contributing to effective community intelligence sharing and collectively coordinating responses to emerging cyber threats and attacks across the Saudi banking sector.

The implementation of the Strategy will be governed by the following rules when scoping, approving and taking forward the strategic streams and initiatives:

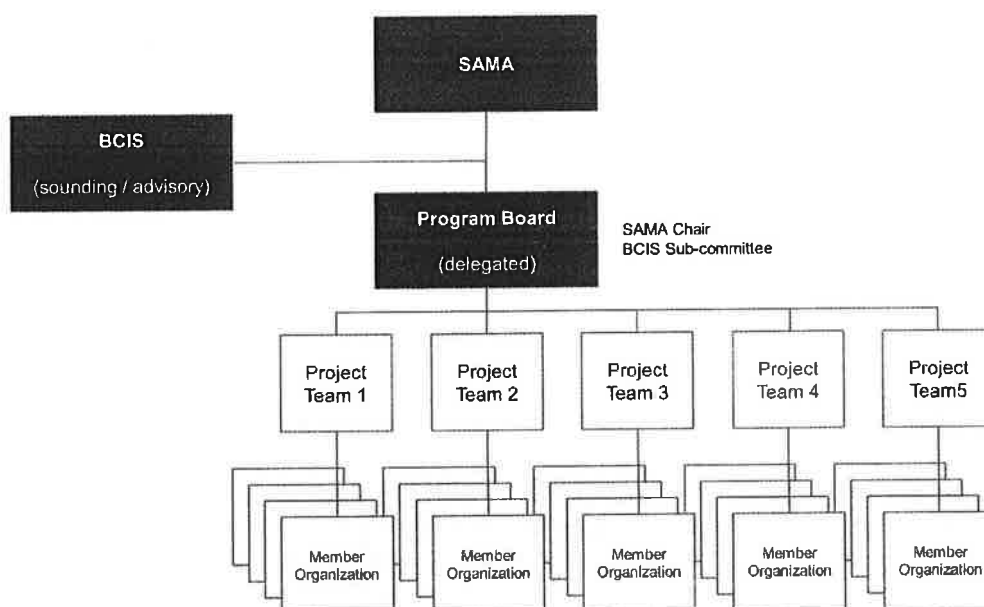
<b>GOVERNING RULES</b>	<ol style="list-style-type: none"> <li>1. Defining leadership and responsibilities.</li> <li>2. Adopting a risk-based approach.</li> <li>3. Implementing a defense in depth approach.</li> <li>4. Investing in and utilizing national talents and skills.</li> <li>5. Aligning with national and international initiatives.</li> <li>6. Collaborating with partners.</li> </ol>
------------------------	---

### 2.4.1 Shared Responsibilities

The execution of the Strategy is a shared effort between SAMA and Member Organizations. The implementation will be overseen by a Program Board comprising SAMA and representative members of BCIS when delegated. Individual Project Teams will be constituted by the Program Board to take forward execution of strategic streams assigned by the Program Board. Each Project Team will include representatives of the Saudi banking sector and other relevant stakeholders, with SAMA coordinating liaison with relevant government agencies.

The Member Organizations, through BCIS, will act as an Advisory Board for the Program Board, and through the Program Board individual Project Teams.

The figure below illustrates the proposed program structure for implementing the Strategy:



### 2.4.2 Management Commitment and Funding

Shared responsibility implies that the boards of Member Organizations must commit to the strategic directions and timelines within this Strategy, while also being prepared to commit the required resources and funding.

### 2.4.3 Integrated Planning

Effective initiation, definition, approval and implementation of strategic streams depends on careful prioritization and planning to ensure availability of the required resources and achievement of realistic timescales. This process will ensure engagement with relevant stakeholders within and outside the Saudi banking sector, while also avoiding duplication and overlap between strategic streams. The Program Board will ensure that integrated planning is aligned with, and agreed by, relevant stakeholders.



#### 2.4.4 Monitor Progress and Improvements

Effective monitoring of the execution of the Strategy, and associated strategic streams, is vital to successful achievement of the objectives and necessary improvements in cyber security. To achieve this, the Program Board will implement a performance management which will embrace:

1. The execution of the strategic streams and the underlying initiatives (i.e. during the initiation, definition, approval and implementation phases).
2. The adoption of the agreed directions or solutions by the Member Organizations.

Project initiation plans will be prepared for all strategic streams defining the scope, objectives, proposed approach, stakeholder engagement, dependency management, resourcing assumptions, risks and mitigation.

The progress of each strategic stream, and underlying initiatives, will be measured against key performance indicators (KPIs), such as:

- Progress against defined milestones and scope.
- Resources consumed (e.g. spend to date, level of effort).
- Quality of deliverables.
- Project management risks.
- Level of adoption by Member Organizations.

#### 2.5 Maintaining and Evaluating the Cyber Security Strategy

The Strategy will be maintained and periodically evaluated by SAMA to ensure continuous improvement, including its continued relevance to emerging cyber security threats and risks. If applicable, SAMA will update the Strategy based on the outcome of the evaluation, this may include adjustments to existing strategic streams and initiatives, or the creation of new strategic streams and initiatives.

### 3 The Cyber Security Strategic Objectives, Streams and Initiatives

#### 3.1 Objective 1: Proactively Protect Saudi banking sector Critical Information Assets

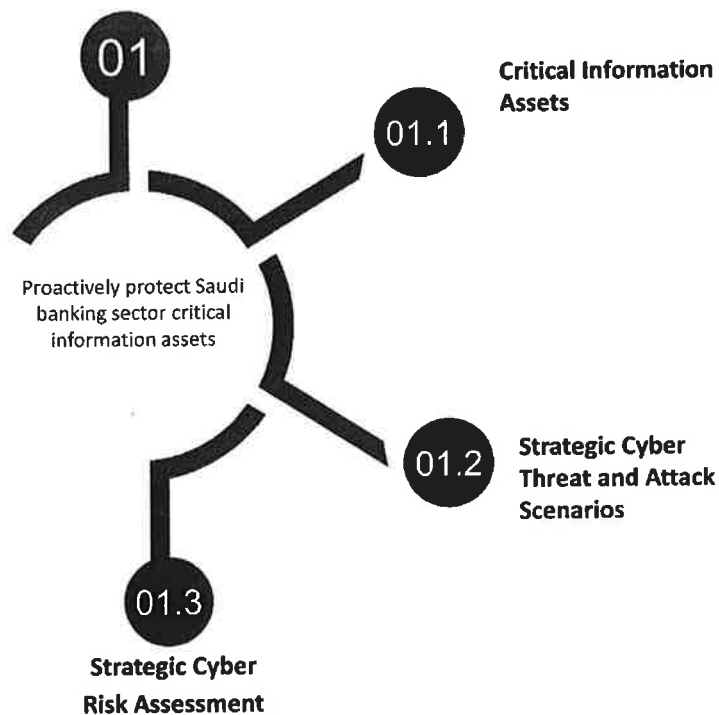
In order to achieve a stable and resilient Saudi banking sector, SAMA and the Member Organizations will identify and protect critical information assets. This should include but not be limited to:

- The identification of critical Saudi banking sector information assets supporting the delivery of essential services and capabilities.
- The analysis of key interdependencies with other sectors.
- The adoption of appropriate cyber security controls.

This will be supported by the creation of a strategic threat and capability analysis to collect and analyze the strategic and emerging cyber security threats and vulnerabilities, allowing the determination of potential attack scenarios and patterns, and forming the basis for identifying necessary enhancements in cyber security controls.

To build a sector-wide view of strategic cyber security risks to the Banking Sector, a periodic banking sector-wide strategic Cyber security risk assessment will be conducted. This will support the development of a banking sector-wide cyber action plans to address possible strategic and emerging cyber security risks.

The strategic streams for objective 1 are shown below:





### 3.1.1 Critical Information Assets

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Identify the Saudi Banking sector critical information assets.
2. Perform a cyber security risk assessment for the identified critical information assets to address the cyber security risks within the Saudi banking sector.
3. Select appropriate cyber security controls and develop cyber security standards.
4. Establish and implement a continuous monitoring capability to ensure compliance with the developed cyber security standards.
5. For the identified critical information assets under the authority of SAMA:
  - Perform a gap analysis to determine their compliance with cyber security standards;
  - Implement the required cyber security controls in order to comply with cyber security standards.
6. For identified systems at the Member Organizations which are connected to the identified critical information assets:
  - Perform a gap analysis to determine their compliance with cyber security standards;
  - Implement the required cyber security controls in order to comply with cyber security standards.
7. Determine the interdependencies of the identified Saudi banking sector critical information assets with other sectors (national and international), as an input into objective 4 'Understand and Manage the Interdependencies (section 3.4).

### 3.1.2 Strategic Cyber Threat and Attack Scenarios

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Establish an effective approach to periodically determine the Saudi banking sector-wide strategic threats, vulnerabilities and interdependencies.
2. Determine the Saudi banking sector-wide strategic threats, vulnerabilities and interdependencies and translate these into strategic threat and attack scenarios.
3. Incorporate the strategic threat and attack scenarios into the threat and vulnerability management processes of the Member Organizations. These scenarios will also be used as an input into strategic stream 3.1.3 'Strategic Risk Assessment'.

### 3.1.3 Strategic Cyber security risk assessment

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Establish an effective strategic cyber security risk assessment approach and framework to periodically determine the Saudi banking sector-wide strategic cyber security risks.
2. Perform a periodic strategic cyber security risk assessment to identify Saudi banking sector-wide strategic cyber security risks.
3. Develop and execute a Banking Sector-wide treatment plan to address the strategic cyber security risks.
4. Establish a cyber security risk and control repository capability.



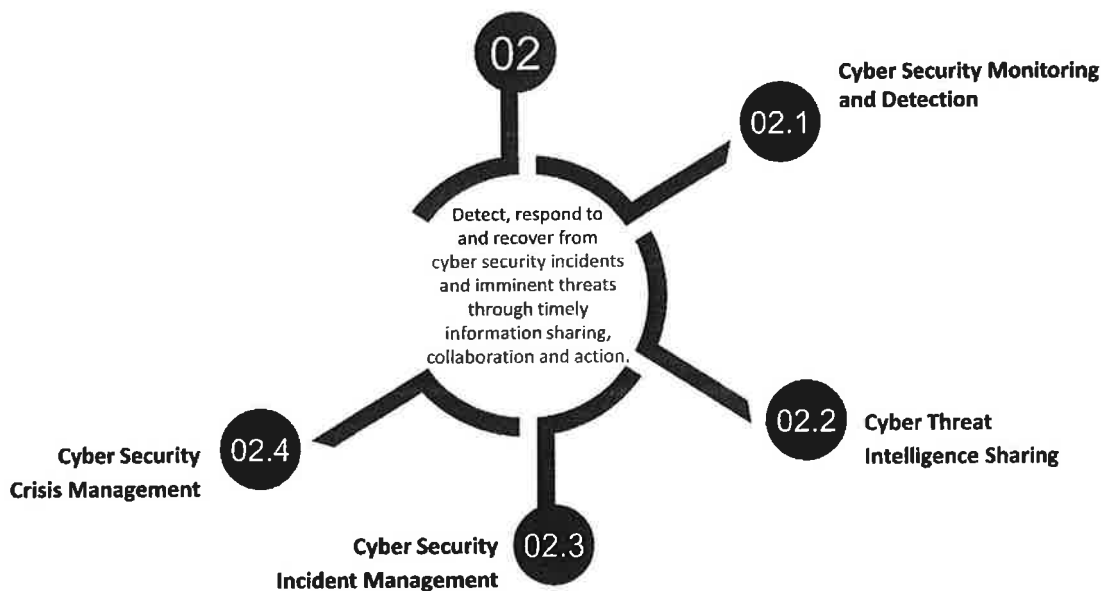
### 3.2 Objective 2: Detect, Respond to and Recover from Cyber Security Incidents

Situational awareness is necessary to effectively detect, respond to and recover from cyber security incidents. The creation of a Banking Cyber Security Centre (BCSC) will provide a focus for the necessary monitoring and detection capabilities. The BCSC will also support mutual and immediate sharing of detected suspicious events between the BCSC and Member Organizations.

A Saudi Banking sector threat intelligence capability will also be established, providing a platform for intelligence sharing between Member Organizations. This platform will also be used to aggregate and share common threat intelligence from preferred threat intelligence providers. Threat intelligence sharing is essential to maintain a proactive posture to counter emerging cyber security threats.

To ensure an effective response to a major cyber security incident, it is vital that all relevant parties know what to do and have a clear understanding of their roles and responsibilities. This will be achieved through the creation of a Saudi banking sector-wide cyber security incident management process. These processes will be rehearsed periodically to ensure that all relevant stakeholders are familiar with the agreed incident management procedures, as well as contributing to the training of relevant staff. The lessons from exercises and incidents will be used to continuously improve the incident management process. In addition, a Saudi banking sector-wide cyber security crisis management process will be established. The cyber security crisis management process will ensure that response and communication procedures within and beyond the Saudi banking sector-wide are in place to deal with a serious incident. These processes will also be periodically exercised.

The strategic streams for objective 2 are shown below:





### 3.2.1 Cyber Security Monitoring and Detection

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Establish an effective Saudi banking sector-wide cyber security monitoring and detection capability (i.e. BCSC), including people, processes and technology.
2. Establish an effective Saudi banking sector-wide capability for Member Organizations to connect to the BCSC, including people, processes and technology, for sharing analysis' of suspicious events, rule-sets and use cases.

### 3.2.2 Cyber Threat Intelligence Sharing

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Establish an effective Saudi banking sector-wide shared cyber threat intelligence capability, including people, processes and technology.
2. Establish an effective Saudi banking sector-wide capability for Member Organizations to connect to the shared cyber threat intelligence capability, including people, processes and technology, for sharing cyber threat intelligence.

### 3.2.3 Cyber Security Incident Management

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Establish an effective Saudi banking sector-wide cyber security incident management process, including supporting incident response procedures and forensic process.
2. Identify incident response capabilities that are required to support the defined cyber security incident management process.
3. Implement required capabilities, either by arranging this internally (within the Saudi banking sector) or by formalizing joint service agreements with third parties to ensure on-demand availability of the required capabilities.
4. Periodically rehearse the Saudi banking sector-wide incident response procedures.
5. Establish a cyber security incident repository capability.

### 3.2.4 Cyber Security Crisis Management

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Establish an effective cyber security crisis management process, including supporting procedures.
2. Conduct Saudi banking sector-wide cyber security crisis management exercises.



### 3.3 Objective 3: Foster a Cyber Security Culture

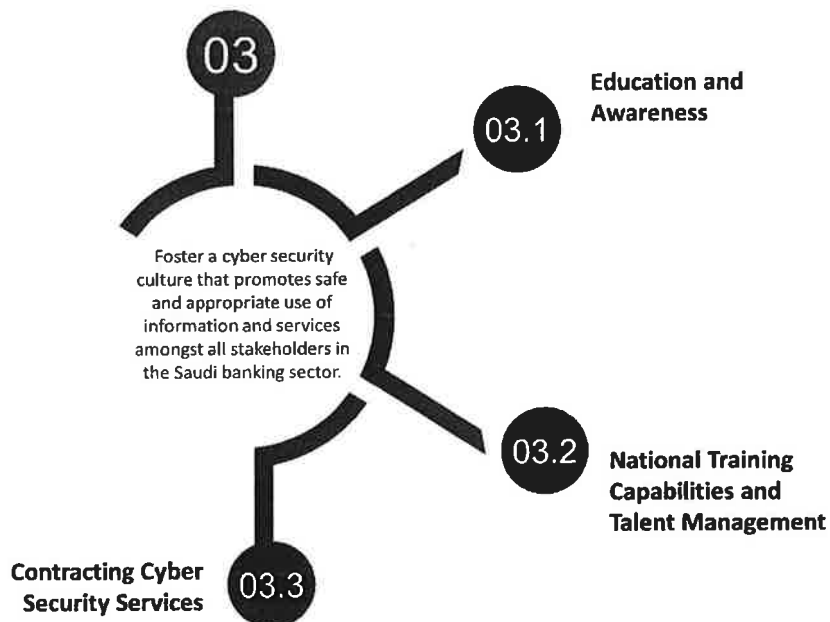
Cyber security is not only about technology. The effectiveness of technological measures largely depends on a security culture in which all stakeholders are sufficiently aware of cyber security risks. Awareness and the proper attitude in organizations are vital to foster a cyber security culture.

Raising awareness and investing in education are effective ways to improve the cyber security culture. Therefore, a Saudi banking sector-wide education program and awareness campaign will be developed and delivered.

SAMA has the ambition to be at the forefront of building and maintaining a skilled cyber security workforce. It is recognized that it will be difficult to create and maintain a sufficient national cadre of skilled cyber security professionals. Therefore, a Saudi banking sector-wide cyber security training and talent management program will be developed and implemented to ensure the development of such a national cadre.

In addition, a code of practice will be developed which ensures that contracting processes preserve and build cyber security knowledge within the Saudi banking sector by ensuring appropriate knowledge transfer from contractors or consultants.

The strategic streams for objective 3 are shown below:







### 3.3.1 Education and Awareness

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Establish an effective Saudi banking sector-wide education program and awareness campaign on cyber security.
2. Contribute to broader cyber security awareness through education institutions and community action.
3. Formalize joint service agreements with third parties to provide education programs and awareness campaign services.

### 3.3.2 National Training Capabilities and Talent Management

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Establish an effective Saudi banking sector-wide training program on cyber security skills for relevant cyber security professionals.
2. Formalize joint service agreements with third parties to provide such training courses.
3. Develop a Saudi banking sector-wide code of practice on the retention and talent development of cyber security professionals.
4. Engage with colleges and universities to develop and implement cyber security curricula and educational programs at the graduate and post-graduate levels.
5. Establish a periodic award for the best cyber security research or thesis relevant for the Saudi banking sector.
6. Establish a periodic award for best cyber security professional within the Saudi banking sector.

### 3.3.3 Contracting Cyber Security Services

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Develop a Saudi banking sector-wide code of practice specifying requirements for knowledge transfer in cyber security service contracts.

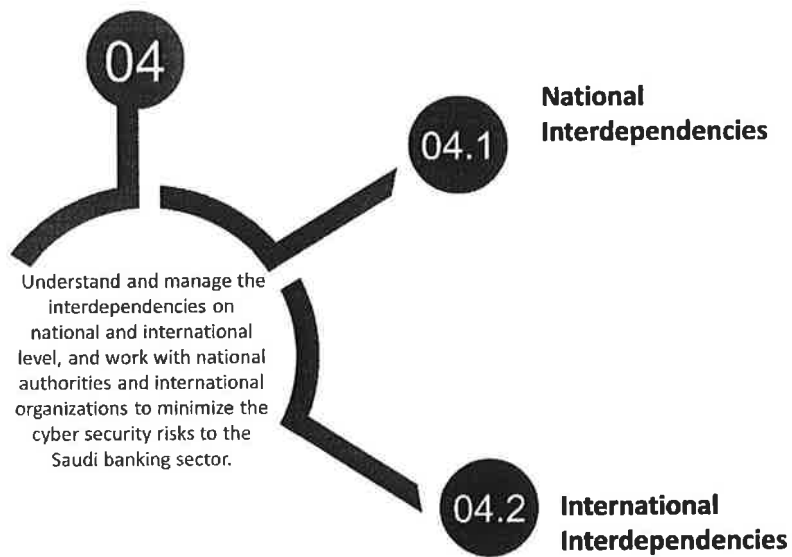


### 3.4 Objective 4: Understand and Manage Interdependencies

The interconnected and distributed nature of the internet allows malicious actors to cross national and international boundaries. To counter cyber security threats, the Saudi banking sector must have an effective approach to national and international collaboration.

Engagement strategies and relationships will be developed and maintained with key national authorities and international organizations to promote cyber security information (e.g., threat intelligence) sharing, enable cyber security investigations and support cyber security operations.

The strategic streams for objective 4 are shown below:





---

#### 3.4.1 National Interdependencies

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Develop and establish a national relationship management process to promote cyber security information sharing, enable cyber security investigations, and support cyber security operations.
2. Engage periodically with national authorities to identify and address cyber security threats and coordinate actions to improve cyber security on a national level.

#### 3.4.2 International Interdependencies

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Develop and establish an international relationship management process to promote cyber security information sharing, enable cyber security investigations, and support cyber security operations.
2. Engage periodically with international organizations to identify and address cyber security threats and coordinate actions to improve cyber security on a national and international level.

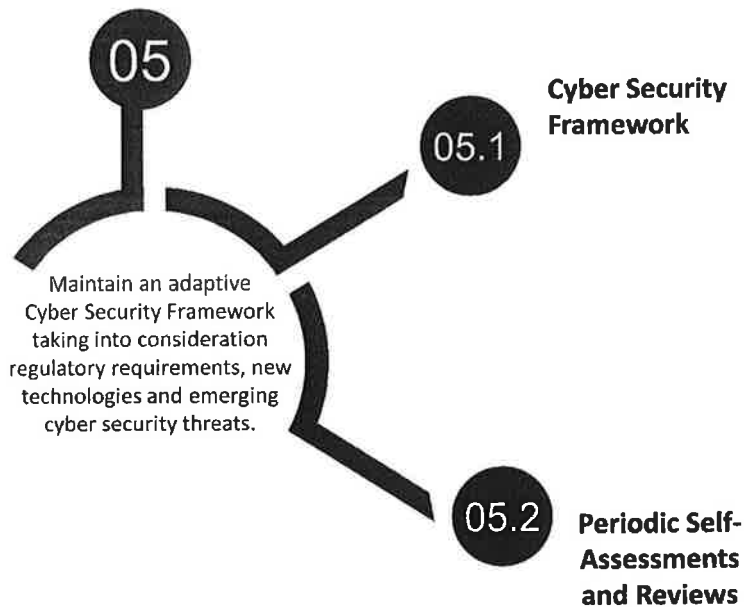
### 3.5 Objective 5: Maintain an Adaptive Cyber Security Framework

Objectives 1 – 4 will be underpinned by the creation of a cyber security framework which will provide the basis for effectively protecting information assets throughout the Saudi banking sector.

The framework will be mandated by SAMA and will be applicable to all Member Organizations, it will be based on national and international good practice. It will be kept under continuous review in the light of emerging cyber threats and developments.

An implementation approach and process for periodic self-assessments will be established to direct, monitor progress and evaluate the adoption of the cyber security framework by the Member Organizations.

The strategic streams for objective 5 are shown below:





### 3.5.1 Cyber Security Framework

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Establish an effective Saudi banking sector-wide cyber security framework, detailing cyber security objectives, controls and compliance measures based on national and international good practices.
2. Establish an effective and adaptive governance framework and implementation approach to direct, monitor and evaluate the adoption of, and compliance with the cyber security framework.
3. Adopt the cyber security framework, governance structure and implementation approach, including performing periodic self-assessments and demonstrating the level of compliance.
4. Maintain and continuously improve the cyber security framework based on changes in regulations, technologies, emerging cyber security threats and newly released national and international good practices.

### 3.5.2 Periodic Self-Assessments and Reviews

This strategic stream should include the following initiatives but should not be limited to these initiatives if required:

1. Mandate the governance framework and implementation approach to direct, monitor the progress and evaluate the adoption of, and compliance with, the cyber security framework across the Saudi banking sector (including ambition and anticipated implementation timelines).
2. SAMA, or (appointed) third party, undertakes periodic reviews at Member Organizations and challenges the self-assessments and level of compliance with the cyber security framework.
3. SAMA, or (appointed) third party, undertakes thematic reviews and assessments periodically on cyber security controls at Member Organizations.





---

## Appendices





## Appendix A – Glossary

<b>Term</b>	<b>Description</b>
<i>Availability</i>	Ensuring timely and reliable access to and use of information. (NIST IR 7298 Glossary of Key Information Security Terms)
<i>Code of practice</i>	Document that recommends practices or procedures for the design, implementation, maintenance or utilization of documents, structures or products. (NIST IR 89-4194)
<i>Confidentiality</i>	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (NIST IR 7298 Glossary of Key Information Security Terms)
<i>Cyber security</i>	Cyber security is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats.
<i>Cyber security awareness</i>	Activities which seek to focus an individual's attention on a cyber security issues. (NIST IR 7298 Glossary of Key Information Security Terms)
<i>Cyber security awareness program</i>	A program that explains proper rules of behavior for the safe and secure use of IT systems and information. The program communicates cyber security policies and procedures that need to be followed.
<i>Cyber security control</i>	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. (NIST IR 7298 Glossary of Key Information Security Terms)
<i>Cyber security framework</i>	Document detailing cyber security objectives, controls and compliance measures based on national and international good practices.
<i>Cyber security governance</i>	A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction for cyber security, ensuring that cyber security objectives are achieved, ascertaining that information risks are managed appropriately and verifying that the enterprise's resources are used responsibly.
<i>Cyber security incident</i>	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
<i>Cyber security incident management</i>	The monitoring and detection of security events on an information systems and the execution of proper responses to those events.
<i>Cyber security program</i>	Top-down management structure and mechanism for coordinating security activities throughout the organization.
<i>Cyber security review</i>	Independent review and examination of security-related records and activities to provide limited assurance that system controls are adequate and that established policies and operational procedures are compliant. (NIST IR 7298 Glossary of Key Information Security Terms)





<b>Term</b>	<b>Description</b>
<i>Cyber security risk assessments</i>	The process of identifying risks to organizational operations, organizational assets, individuals, other organizations, and the nation, arising through the operation of an information system. A part of risk management, it incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. (NIST IR 7298 Glossary of Key Information Security Terms)
<i>Cyber security strategy</i>	A high-level plan, consisting of projects and initiatives, to mitigate cyber security risks while complying with legal, statutory, contractual, and internally prescribed requirements.
<i>Cyber security threat</i>	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NIST IR 7298 Glossary of Key Information Security Terms)
<i>Incident management</i>	Refer to 'Cyber security incident management'.
<i>Incident management plan</i>	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack against an organization's information system(s). Also Refer to 'Cyber security incident management'. (NIST IR 7298 Glossary of Key Information Security Terms)
<i>Integrity</i>	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (NIST IR 7298 Glossary of Key Information Security Terms)
<i>Key performance indicator</i>	A type of performance measurement that evaluate the success of an organization or of a particular activity in which it engages. Numerical threshold(s) are typically used to categorize performance.
<i>Member organization</i>	Organizations affiliated with SAMA.
<i>Resilience</i>	The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.
<i>Risk</i>	A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (NIST IR 7298 Glossary of Key Information Security Terms)
<i>Threat</i>	Refer to 'Cyber security threat'
<i>Threat intelligence</i>	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. (Gartner)
<i>Threat landscape</i>	<ol style="list-style-type: none"><li>1. An overview of threats, together with current and emerging trends.</li><li>2. A collection of threats in a particular domain or context, with information on identified vulnerable assets, threats, risks, threat actors and observed trends. (ENISA)</li></ol>







---

<i>Term</i>	<b>Description</b>
<i>TOM</i>	A target operating model (TOM) is a desired operating model that visualizes (i.e. using a model or collection of models, maps, tables and charts) how the organization operates so as to deliver value to its customers or beneficiaries.
<i>Vulnerability</i>	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NIST IR 7298 Glossary of Key Information Security Terms)
<i>Vulnerability management</i>	Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. Also refer to 'Vulnerability'.



## Appendix B – Detailed Initiatives Objectives and Expected Outcome

### Objective 1 – Proactively Protect Saudi banking sector Critical Information Assets

#### Strategic Stream 1 - Critical Information Assets

#	Initiative	Objective	Expected Outcome
1	Identify the Saudi Banking sector critical information assets.	The essential information assets which support key banking sector or banking services and assets which are key to SAMA and the Member Organizations need to be identified first, to be able to protect these information assets.	<ul style="list-style-type: none"> <li>• A defined process to identify all critical information assets within the banking sector which are key for SAMA and all Member Organizations, including owners and custodians.</li> <li>• An up-to-date overview of critical assets.</li> <li>• SAMA senior management endorsement and approval of the list.</li> </ul>
2	Perform a cyber security risk assessment for the identified critical information assets to address the cyber security risks within the Saudi banking sector.	To identify the relevant cyber security risks regarding the identified critical information assets within the Saudi banking sector.	<ul style="list-style-type: none"> <li>• A defined and agreed cyber security risk assessment methodology and approach.</li> <li>• A cyber risk assessment and resulting report that includes the relevant risk for the identified critical information assets within the Saudi banking sector and classification of the identified risks as an input into objective 4, 'Understand and Manage Interdependencies' (section 3.4).</li> </ul>
3	Select appropriate cyber security controls and develop cyber security standards.	To document the mandatory controls in cyber security standards that properly protect the identified critical information assets and mitigate the identified cyber security risks.	<ul style="list-style-type: none"> <li>• A defined and approved Saudi banking sector cyber security standards (for the owners, users and custodians), including mandatory controls, for all identified critical information assets.</li> <li>• Standards updates.</li> <li>• Communication and adoption of the standards.</li> </ul>
4	Establish and implement a continuous monitoring capability to ensure compliance with the developed cyber security standards.	To be able to monitor the Member Organizations' compliance with cyber security standards for the identified critical information assets.	<ul style="list-style-type: none"> <li>• A compliance monitoring approach and process.</li> <li>• A monitoring and compliance tool.</li> <li>• A communication and adoption plan.</li> </ul>



#	Initiative	Objective	Expected Outcome
5	<p>For the identified critical information assets under the authority of SAMA:</p> <ul style="list-style-type: none"> <li>Perform a gap analysis to determine their compliance with cyber security standards;</li> <li>Implement the required cyber security controls in order to comply with cyber security standards.</li> </ul>	<p>To ensure that SAMA, as the owner or custodian of those identified critical information assets under their authority, identifies the gaps with regard to the mandatory cyber security standards and implements the required cyber security controls lacking according to the cyber security standards.</p>	<ul style="list-style-type: none"> <li>A gap analysis report for those critical information assets under authority of SAMA.</li> <li>A project plan or roadmap to execute the identified improvements.</li> <li>A project completion report per critical information asset.</li> </ul>
6	<p>For identified systems at Member Organizations that are connected to the identified critical information assets:</p> <ul style="list-style-type: none"> <li>Perform a gap analysis to determine their compliance with cyber security standards;</li> <li>Implement the required cyber security controls in order to comply with cyber security standards.</li> </ul>	<p>To ensure that each Member Organization, as the custodian or user of those identified critical information assets, identify the gaps with regard to the mandatory cyber security standards and implements the required cyber security controls lacking according to the cyber security standards.</p>	<ul style="list-style-type: none"> <li>A gap analysis report for those critical information assets relevant for those Member Organizations that make use of, or are responsible for the custody of these assets.</li> <li>A project plan or roadmap to execute the identified improvements.</li> <li>A project completion report per critical information asset.</li> </ul>
7	<p>Determine the inter-dependencies of the identified Saudi banking sector critical information assets with other sectors (national and international) as an input into objective 4, 'Understand and Manage Interdependencies' (section 3.4).</p>	<p>To identify and gain insight into the interdependencies of the identified critical information assets for the Saudi banking sector with other national or international sectors or parties.</p>	<ul style="list-style-type: none"> <li>An overview of those national and international sectors or parties that are relevant and important for the Saudi banking sector critical information assets.</li> </ul>

#### Strategic Stream 2 – Strategic Cyber Threat and Attack Scenarios

#	Initiative	Objective	Expected Outcome
1	<p>Establish an effective approach to periodically determine the Saudi banking sector-wide strategic threats, vulnerabilities and interdependencies.</p>	<p>To develop an approach and methodology that helps identify new and emerging strategic threats, vulnerabilities and interdependencies throughout the banking sector.</p>	<ul style="list-style-type: none"> <li>A strategic threats, vulnerabilities and interdependencies approach and methodology.</li> </ul>
2	<p>Determine the Saudi banking sector-wide strategic threats, vulnerabilities and interdependencies and translate these into strategic threat and attack scenarios.</p>	<p>To identify new and emerging strategic threats, vulnerabilities and interdependencies throughout the banking sector.</p>	<ul style="list-style-type: none"> <li>A strategic threats, vulnerabilities and interdependencies analysis.</li> <li>A strategic threats and attack scenarios report.</li> </ul>





#	Initiative	Objective	Expected Outcome
3	Incorporate the strategic threat and attack scenarios into the threat and vulnerability management processes of the Members Organizations. These scenarios will also be used as an input into strategic stream 1.3 'Strategic Cyber Risk Assessment'.	To enrich the members organization's threat and vulnerability management processes with the strategic threats and attack scenarios	<ul style="list-style-type: none"> <li>A vulnerability assessment and confirmation of protection against emerging threats.</li> </ul>

### Strategic Stream 3 – Strategic Cyber Risk Assessment

#	Initiative	Objective	Expected Outcome
1	Establish an effective strategic cyber risk assessment approach and framework to periodically determine the Saudi banking sector-wide strategic cyber security risks using, in part, outcomes from stream 2.2 (2 <sup>nd</sup> bullet) of objective 1 and stream 4.1 (2 <sup>nd</sup> bullet) of objective 2.	To create an approach and methodology to identify the Saudi banking sector-wide strategic cyber security risks.	<ul style="list-style-type: none"> <li>A Saudi banking sector-wide strategic cyber security risks approach and methodology.</li> </ul>
2	Perform a periodic strategic cyber risk assessment to identify Saudi banking sector-wide strategic cyber security risks.	To periodically identify the Saudi banking sector-wide strategic cyber security risks.	<ul style="list-style-type: none"> <li>A sector-wide strategic cyber security risks report.</li> </ul>
3	Develop and execute a Banking Sector-wide treatment plan to address the strategic cyber security risks.	To eliminate, mitigate and acknowledge strategic cyber security risks.	<ul style="list-style-type: none"> <li>A cyber security risk treatment plan.</li> <li>Cyber security risk treatment plan updates.</li> </ul>
4	Establish a cyber security risk and control repository capability.	To establish a single information source that gives the banking sector a significant edge.	<ul style="list-style-type: none"> <li>A centralized cyber security risk and control repository and management system.</li> <li>Repository updates.</li> </ul>

### Objective 2 – Detect, Respond to and Recover from Cyber Security Incidents

#### Strategic Stream 1 – Cyber Security Monitoring and Detection

#	Initiative	Objective	Expected Outcome
1	Establish an effective Saudi banking sector-wide cyber security monitoring and detection capability (i.e. BCSC), including people, processes and technology.	To develop a centralized cyber security monitoring and detection capability.	<ul style="list-style-type: none"> <li>A sector-wide cyber security monitoring and detection capability target operating model (TOM).</li> <li>A sector-wide cyber security monitoring and detection capability.</li> </ul>





#	Initiative	Objective	Expected Outcome
2	Establish an effective Saudi banking sector-wide capability for Members Organizations to connect to the BCSC, including people, processes and technology, for sharing analyses of suspicious events, rule-sets and use cases.	To develop a centralized cyber security monitoring and detection capability.	<ul style="list-style-type: none"> <li>• A sector-wide cyber security monitoring and detection connecting capability TOM.</li> <li>• A sector-wide cyber security monitoring and detection connecting capability.</li> </ul>

#### Strategic Stream 2 – Cyber Threat Intelligence Sharing

#	Initiative	Objective	Expected Outcome
1	Establish an effective Saudi banking sector-wide shared cyber threat intelligence capability, including people, processes and technology.	To develop a centralized cyber threat intelligence capability.	<ul style="list-style-type: none"> <li>• A sector-wide shared threat intelligence capability TOM.</li> <li>• A sector-wide shared threat intelligence capability.</li> </ul>
2	Establish an effective Saudi banking sector-wide capability for Members Organizations to connect to the shared cyber threat intelligence capability, including people, processes and technology, for sharing cyber threat intelligence.	To develop a centralized cyber threat intelligence capability.	<ul style="list-style-type: none"> <li>• A sector-wide shared threat intelligence connecting capability TOM.</li> <li>• A sector-wide shared threat intelligence connecting capability.</li> </ul>

#### Strategic Stream 3 – Cyber Security Incident Management

#	Initiative	Objective	Expected Outcome
1	Establish an effective Saudi banking sector-wide cyber security incident management process, including supporting incident response procedures and forensic process.	To develop a centralized Incident management across the banking sector. That will help in identifying patterns and anomalies.	<ul style="list-style-type: none"> <li>• A cyber security incident management process.</li> <li>• A cyber security incident management system.</li> </ul>
2	Identify specific incident response capabilities that are required to support the defined cyber security incident management process.	To help understand the current maturity of the incident response capabilities.	<ul style="list-style-type: none"> <li>• A specific incident response capabilities report.</li> <li>• A gap analysis.</li> <li>• Mitigation and implementation plans.</li> </ul>
3	Implement required capabilities, either by arranging this internally (within the Saudi banking sector) or by formalizing joint service agreements with third parties to ensure on-demand availability of the required capabilities.	To execute the implementation plan in order to develop the needed capabilities.	<ul style="list-style-type: none"> <li>• An implementation of expected capability measures.</li> </ul>





#	Initiative	Objective	Expected Outcome
4	Periodically rehearse the Saudi banking sector-wide incident response procedures.	To guarantee that the response procedures are efficient and effective.	<ul style="list-style-type: none"> <li>An sector-wide incident response procedure rehearsal plan.</li> </ul>
5	Establish a cyber security incident repository capability.	To establish a single information source that gives the banking sector a significant edge.	<ul style="list-style-type: none"> <li>A centralized cyber security incident data repository and management system.</li> </ul>

#### Strategic Stream 4 – Cyber Security Crisis Management

#	Initiative	Objective	Expected Outcome
1	Establish an effective cyber security crisis management process, including supporting procedures.	To increase the resilience of the banking sector	<ul style="list-style-type: none"> <li>A centralized cyber security crisis management system and supporting documents (policies, procedures and guidelines).</li> </ul>
2	Conduct Saudi banking sector-wide cyber security crisis management exercises.	To insure the resilience of the banking sector.	<ul style="list-style-type: none"> <li>Crisis management scenarios.</li> <li>A crisis management exercise plan.</li> <li>Crisis management scenarios and exercise plan updates.</li> </ul>

#### Objective 3 – Foster a Cyber Security Culture

##### Strategic Stream 1 - Education and Awareness

#	Initiative	Objective	Expected Outcome
1	Establish an effective Saudi banking sector-wide education program and awareness campaign on cyber security.	To improve the overall level of knowledge and awareness regarding cyber security across the sector and nation for banking staff and customers.	<ul style="list-style-type: none"> <li>Sector-wide education programs on cyber security.</li> <li>Sector-wide awareness campaigns on cyber security.</li> <li>Education programs and awareness campaigns updates.</li> <li>Improved cyber security knowledge and awareness of banking staff and customers.</li> </ul>
2	Contribute to broader cyber security awareness through education institutions and community action.	To improve the collaboration regarding cyber security awareness between Member Organizations within the Saudi banking sector.	<ul style="list-style-type: none"> <li>Improved collaboration between the Member Organizations within the Saudi banking sector towards joint cyber security awareness activities.</li> </ul>
3	Formalize joint service agreements with third parties to provide		<ul style="list-style-type: none"> <li>Formalized agreements with specialized parties or companies.</li> </ul>



#	Initiative	Objective	Expected Outcome
	education programs and awareness campaign services.	To utilize specialized parties to provide education programs and awareness campaign services.	<ul style="list-style-type: none"> <li>Professional and centrally organized and coordinated education programs.</li> <li>Professional and centrally organized and coordinated awareness campaign services.</li> <li>Updates on agreements, coordinated education programs and coordinated awareness campaign.</li> </ul>

### Strategic Stream 2 - National Training Capabilities and Talent Management

#	Initiative	Objective	Expected Outcome
1	Establish an effective Saudi banking sector-wide training program on cyber security skills for relevant cyber security professionals.	To provide the necessary training and improvement of skills for cyber security professionals across the Saudi banking sector.	<ul style="list-style-type: none"> <li>A sector-wide training program containing affordable and collective training possibilities.</li> <li>Program updates.</li> </ul>
2	Formalize joint service agreements with third parties to provide such training courses.	To utilize specialized parties to provide sector-wide cyber security training courses.	<ul style="list-style-type: none"> <li>Formalized agreements with specialized parties or companies.</li> <li>Professional and centrally organized and coordinated sector-wide training courses.</li> </ul>
3	Develop a Saudi banking sector-wide code of practice on the retention and talent development of cyber security professionals.	To retain and develop cyber security professionals and talents within the Saudi banking sector.	<ul style="list-style-type: none"> <li>An agreed upon sector-wide code of practice on talent development and retention.</li> <li>More experienced, motivated and loyal cyber security professionals.</li> <li>A talent development program for cyber security professionals.</li> <li>Code of practice and talent development program updates.</li> </ul>
4	Engage with colleges and universities to develop and implement cyber security curricula and educational programs at the graduate and post-graduate levels.	To support the development of various cyber security curricula and educational programs and increase the number of future cyber security professionals.	<ul style="list-style-type: none"> <li>An improved variety of cyber security curricula and educational programs.</li> <li>An attractive assortment of studies to meet the diverse demands of existing and future cyber security professionals.</li> <li>An improved collaboration between colleges, universities and the Saudi banking sector.</li> </ul>





#	Initiative	Objective	Expected Outcome
5	Establish a periodic award for the best cyber security research or thesis relevant for the Saudi banking sector.	To promote the importance of cyber security and reward the most value adding research for the Saudi banking sector.	<ul style="list-style-type: none"> <li>An increased incentive for researchers and students to research or provide new insights on cyber security for the Saudi banking sector.</li> </ul>
6	Establish a periodic award for best cyber security professional within the Saudi banking sector.	To promote the importance of cyber security and reward the best cyber security professional the Saudi banking sector.	<ul style="list-style-type: none"> <li>An increased acknowledgment of continuously improving cyber security professionals.</li> </ul>

### Strategic Stream 3 - Contracting Cyber Security Services

#	Initiative	Objective	Expected Outcome
1	Develop a Saudi banking sector-wide code of practice specifying requirements for knowledge transfer in cyber security service contracts.	To ensure specific cyber security knowledge is being transferred and maintained within the Member Organizations.	<ul style="list-style-type: none"> <li>A Saudi banking sector-wide code of practice on knowledge transfer.</li> <li>Code of practice updates.</li> <li>Retention of specific cyber security knowledge within the Member Organizations after hiring specialized third parties or consultants.</li> </ul>

### Objective 4 – Understand and Manage the Interdependencies

#### Strategic Stream 1 - National Interdependencies

#	Initiative	Objective	Expected Outcome
1	Develop and establish a national relationship management process to promote cyber security information sharing, enable cyber security investigations, and support cyber security operations.	To formalize a process that supports the pro-active collaboration between relevant national authorities and sectors on cyber security.	<ul style="list-style-type: none"> <li>A relationship management process to maintain and support cyber activities across the nation.</li> </ul>
2	Engage periodically with national authorities to identify and address cyber security threats and coordinate actions to improve cyber security on a national level.	To build and maintain national community to improve the cyber security awareness and maturity at national level.	<ul style="list-style-type: none"> <li>A meeting schedule with mandated representatives from identified national authorities and sectors.</li> <li>Sharing cyber security related information or details.</li> <li>Improvement action plans at sector or national level.</li> </ul>





Strategic Stream 2 - International Interdependencies

#	Initiative	Objective	Expected Outcome
1	Develop and establish an international relationship management process to promote cyber security information sharing, enable cyber security investigations, and support cyber security operations.	To formalize a process that supports the pro-active collaboration between relevant international organizations on cyber security.	<ul style="list-style-type: none"> <li>• A relationship management process to maintain and support cyber activities across the globe.</li> </ul>
2	Engage periodically with international organizations to identify and address cyber security threats and coordinate actions to improve cyber security on a national and international level.	To build and maintain international community to improve the cyber security awareness and maturity at international level.	<ul style="list-style-type: none"> <li>• A meeting schedule with mandated representatives from identified international organizations.</li> <li>• Sharing cyber security related information or details.</li> <li>• Identification of improvement actions at sector or national level.</li> </ul>

Objective 5 – Maintain an Adaptive Cyber Security framework

Strategic Stream 1 – Cyber Security Framework

#	Initiative	Objective	Expected Outcome
1	Establish an effective Saudi banking sector-wide cyber security framework, detailing cyber security objectives, controls and compliance measures based on national and international good practices.	To support the banking sector: <ol style="list-style-type: none"> <li>a. with a comprehensive cyber security framework</li> <li>b. with focusing on the required cyber security objectives and principles,</li> <li>c. in achieving the required level of maturity,</li> <li>d. with the ability to periodically measure and evaluate the effectiveness of the required cyber security controls</li> <li>e. with the ability to measure the overall compliance.</li> </ol>	<ul style="list-style-type: none"> <li>• A single cyber security framework, owned by SAMA and adopted by all Member Organizations within the Saudi banking sector, which includes all good practices and SAMA requirements.</li> </ul>
2	Establish an effective and adaptive governance framework and implementation approach to direct, monitor and evaluate the adoption of, and compliance with the cyber security framework.	To structurally steer, monitor and evaluate the progress of implementation, the level of adoption, the compliance and the effectiveness of the cyber security framework within the Saudi banking sector a governance framework is required.	<ul style="list-style-type: none"> <li>• A governance framework for the Saudi banking sector cyber security framework which includes roles and responsibilities, clear directions for implementation and adoption.</li> </ul>



#	Initiative	Objective	Expected Outcome
3	Adopt the cyber security framework, governance structure and implementation approach, including performing periodic self-assessments and demonstrating the level of compliance.	To ensure the cyber security framework, the implementation approach, the framework governance, the periodic self-assessments and compliance measuring is actually adopted and can be demonstrated by Member Organizations.	<ul style="list-style-type: none"> <li>An overview of the number of Member Organizations which formally adopted the cyber security framework.</li> <li>The ability to periodic perform self-assessment and compliance with regard to the cyber security framework</li> <li>The ability to report the outcome of the self-assessments and compliance measurements to the executive board, cyber security committee and SAMA.</li> <li>The ability to benchmark the Member Organizations on their maturity levels and level of compliance.</li> </ul>
4	Maintain and continuously improve the cyber security framework based on changes in regulations, technologies, emerging cyber security threats and newly released national and international good practices.	To ensure that a process is established to continuously update and align the Saudi banking sector cyber security framework with new regulatory requirements, new and emerging cyber security threats, and both national and international frameworks and good practices.	<ul style="list-style-type: none"> <li>A change management process as part of the framework governance to ensure the cyber security framework is periodically reviewed and kept up-to-date.</li> </ul>

#### Strategic Stream 2 – Periodic Self-assessments and Reviews

#	Initiative	Objective	Expected Outcome
1	Mandate the governance framework and implementation approach to direct, monitor the progress and evaluate the adoption of, and compliance with, the cyber security framework across the Saudi banking sector (including ambition and anticipated implementation timelines).	To formally endorse the governance framework and the implementation approach by SAMA for all Member Organizations within the Saudi banking sector.	<ul style="list-style-type: none"> <li>A formalized mandate issued by SAMA, including the ambition and anticipated implemented timelines, to all Member Organizations within the Saudi banking sector.</li> <li>A formal adoption by all Member Organizations within the Saudi banking sector of the cyber security framework including the ambition and anticipated timelines.</li> </ul>



#	Initiative	Objective	Expected Outcome
2	SAMA, or (appointed) third party, undertakes periodic reviews at Members Organizations and challenges the self-assessments and level of compliance with the cyber security framework.	To periodically visit each Member Organization within the Saudi banking organization to supervise and challenge the executed periodic self-assessments and level of compliance with the cyber security framework.	<ul style="list-style-type: none"> <li>• Action plans of the required improvements with regard to the cyber security framework and required ambition, approved by the Member Organization Cyber Security Committee, in line with the anticipated timelines.</li> <li>• A schedule issued by SAMA for visiting the Member Organizations to review and challenge the executed self-assessments and level of compliance.</li> <li>• A benchmark of the Saudi banking sector and insight of the status of all Member Organizations regarding:               <ul style="list-style-type: none"> <li>○ the quality of the executed self-assessments;</li> <li>○ the level of maturity and compliance;</li> <li>○ the areas for improvement;</li> <li>○ the areas of special attention.</li> </ul> </li> </ul>
3	SAMA, or (appointed) third party, undertakes thematic reviews and assessments periodically on cyber security controls at Members Organizations.	To obtain a more detailed level of insight across the Saudi banking sector on specific cyber security themes or (a set of) implemented cyber security.	<ul style="list-style-type: none"> <li>• An overview of the thematic reviews on which SAMA will particularly focus.</li> <li>• Insights across the Saudi banking sector regarding:               <ul style="list-style-type: none"> <li>○ the level of maturity and compliance concerning specific themes;</li> <li>○ the areas for improvement;</li> <li>○ the areas of special attention.</li> </ul> </li> </ul>

مؤاد