Central Bank of Kuwait

With reference to FSB CIRR Virtual Meetings on "***Effective Practices for Cyber Incident Response and Recovery***" Consultation Paper (Published on 20/04/2020), please find below Central bank of Kuwait (CBK) comments as follows:

(1) We suggest considering Financial/Banking Regulators' perspective on Cyber Incident Response and Recovery, namely, the role of the Financial/Banking Regulators in managing sector-wide cyber incidents and crises.

(2) Updating the definition and classification of Cyber Incidents and their severity impact levels; both on single organization-level and on sector-wide level.

(3) The Central Bank of Kuwait suggests developing a severity impact matrix for initiating response and recovery actions for cyber incidents. The impact matrix criteria dictate appropriate mitigating actions and timelines for reporting incident to stakeholders (including regulators – as a priority). Furthermore and on a sectoral level, this shall help regulators analyze the reported incident to evaluate the sector wide impact in accordance with sector wide severity impact matrix, and advise on necessary response/recovery actions.

(4) We are attaching Central Bank of Kuwait's "***Cybersecurity Framework for Kuwaiti Banking Sector***" (2020) for your reference.

بنك الكويت المركزي
CENTRAL BANK OF KUWAIT

CYBERSECURITY FRAMEWORK
FOR
KUWAITI BANKING SECTOR

Foreword

As the global financial ecosystem is reshaped by rapid developments in technology, the banking sector, in particular, is becoming more suspectable to a significantly rising number of cyber security attacks. Traditionally considered a custodian of information and financial assets, the banking sector, is no longer only responsible for their safe keeping, but also for proactively preventing or mitigating cyber threats. With the obvious material risks posed to individual institutions, extreme cyber events can spiral into systemic risk, or even threaten to paralyze the whole nation. Consequently, strengthening cybersecurity and cyber resilience measures are at the top of the agenda.

As the regulator of Kuwait's banking sector, the Central Bank of Kuwait (CBK), institutes this Cybersecurity Framework with the objective of improving its cyber resilience. It outlines the requirements regulated entities must fulfil to improve their capabilities, readiness, cooperation, information sharing and standardization. CBK commits to providing the necessary support, supervision and regulation to promote the realization of this objective.

We are confident that this Cybersecurity Framework will guide the banking sector to effectively manage imminent cyber risks, ensure continued services to society and uphold the reputation of the State of Kuwait.

Dr. Mohammad Y. Al-Hashel
Governor, Central Bank of Kuwait

CYBERSECURITY FRAMEWORK

FOR

KUWAITI BANKING SECTOR

TABLE OF CONTENTS

1. Introduction

While recent developments in technology and wide-scale adoption of online digital services have benefited the financial sector, they have also increased the cyber risks we face. The growing frequency and sophistication of cyber attacks have reinforced the need for organizations to have strong cybersecurity controls to mitigate cyber risks.

As per Article 15 of Law No. 32 of 1968, Central Bank of Kuwait is responsible to supervise the Kuwaiti banking sector. Accordingly, the Central Bank of Kuwait (CBK) recognizes the need for the banking sector to improve its resilience to cyber attacks. To support this objective, CBK is institutes this Cybersecurity Framework (CSF), which applies to all Regulated Entities within the banking sector to ensure consistent management of cybersecurity in the banking sector. The CSF defines the cybersecurity strategy and regulatory framework to enhance the cybersecurity of the sector's systems, operations, infrastructure, and data.

1.1 Definitions

CSF defines the following terms for consistent reference and interpretation:

'Cybersecurity' is the Preservation of *confidentiality*, *integrity* and *availability* of information and/or information systems through the cyber medium. In addition, other properties, such as *authenticity*, *accountability*, *non-repudiation* and *reliability* can also be involved. [1]

'Cyber Resilience' is the ability to continue to carry out mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.[2]

'Cyber Risk' is the combination of the probability of an event occurring within the realm of an organization's information assets, computer and communication resources and the consequences of that event.[3]

1 Cybersecurity Lexicon, Nov 2018, Financial Stability Board (FSB)
2 Cybersecurity Lexicon, Nov 2018, Financial Stability Board (FSB)
3 CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures

1.2 Drivers

The CSF exists in the context of several strategic drivers that fundamentally influence the Kuwaiti banking sector as identified below:

- C**ompliance with CBK Law 32 of Year 1968 and Law 20 of Year 2014**: CBK understands the need for managing an elevated and rapidly evolving cyber threats to financial markets as an integral part of CBK's core responsibility of managing the stability and integrity of the Kuwaiti Banking sector.
- **Expanding role of CBK in managing the stability of Payment Systems and FinTechs:** The introduction of instructions for electronic payments in the State of Kuwait increased CBK's responsibilities.
- **Increasing dependencies on third parties:** As Regulated Entities are increasingly dependent on third parties for facilities, infrastructure, technology management, and operational support, appropriate controls are vital to ensure the stability and resilience of Regulated Entities.
- **The need for greater visibility and regulatory supervision:** With the increasing number of high profile cyber attacks across the banking sector, CBK requires greater visibility of the effectiveness (i.e. maturity) of the cybersecurity controls in operation across the banking sector.
- **The need to maintain the resilience of the banking sector as it adapts to the rapid advancement of and increased reliance on technology:** With the continuous and rapid introduction of new technologies to the banking sector, there is a need to manage the evolving cyber threats.
- **Alignment with and execution of the National Cyber Security Strategy (NCSS) for the State of Kuwait:** The NCSS identifies and outlines its vision for cybersecurity for the State of Kuwait. Compliance with the CSF will assist Regulated Entities in managing their cyber risks in alignment with the NCSS.
- **The need for continuous improvement due to the increase in frequency and sophistication of cyber attacks:** The increased number of cyber attacks and their growing complexity continues to expose vulnerabilities, and highlights the need for continuous improvement in cybersecurity controls.

1.3 Scope

The scope of the CSF is limited to cybersecurity related to strategies, policies and procedure, and system controls within the Regulated Entities, including:

- Strategies such as outsourcing (third-party), digitalization, use of FinTechs;
- Policies and procedures, such as cyber crisis management, information technology security, access control management, communication, disaster recovery and compliance and audit;
- IT systems and networks, such as Core Banking, SWIFT, ATM network connectivity ; and
- IT Processes such as change management, asset management, secure disposal etc.

1.4 Applicability

This CSF is applicable to all Regulated Entities supervised by the CBK.

1.5 Target Audience

The CSF is issued for the Board of Directors, Senior Management, Information Security Professionals, Information Technology professionals and others who are responsible for establishing, implementing and ensuring their entity's compliance with the CSF.

2. Cybersecurity Framework Overview

The CSF defines and addresses the objectives by establishing multiple components that work together to improve the cybersecurity of Regulated Entities and the sector as a whole.

2.1 Objectives

The objectives of the CSF are:

- To improve cyber resilience within the Kuwaiti banking sector by defining requirements that seek to enhance capabilities, preparedness, cooperation, information sharing, and standardization of the Regulated Entities' cybersecurity approaches;
- To enhance the maturity of the cybersecurity controls in place within the sector as well as provide a mechanism to inform and mandate strategic security initiatives required to improve cybersecurity maturity; and
- To ensure that CBK executes its sectoral responsibility to provide appropriate levels of informed supervision and regulation for the improvement of cyber resilience in the sector.

2.2 Framework Core Principles

The CSF defines three core principles that enhances the banking sector's cybersecurity and resilience capabilities:

- Governance, Risk management and Compliance (section 2.2.1)
- Collaboration (section 2.2.2)
- Continual Improvement (section 2.2.3)

The core principles and their underlying components, tools and functions co-exist and operate as necessary to fulfill the objectives of the CSF, and are illustrated below (Figure 1):

Figure 1: Cybersecurity Framework

2.2.1 Governance, Risk Management and Compliance

CBK identifies Governance, Risk Management and Compliance (GRC) as one of the core principles of the CSF. The underlying GRC components identified in the following sections will enable Regulated Entities to integrate and coordinate Governance, Risk and Compliance initiatives within their business processes. A holistic view of the current GRC posture with respect to cybersecurity will enable the management teams of Regulated Entities to make informed decisions to effectively manage cyber risks.

Regulated Entities' Board of Directors are accountable for the cybersecurity of their organizations however, they may delegate responsibility for delivering effective cybersecurity to individuals or entities within their organization who have the appropriate qualifications and expertise.

2.2.1.1 Governance

CBK requires Regulated Entities to embed an effective governance model into their organizational structure, which will provide adequate support to build, implement, and manage an effective cybersecurity program, including the following responsibilities:

1. The Board of Directors (hereinafter referred as, the Board) and Senior Management of Regulated Entities shall be accountable and responsible for defining and overseeing the business strategy, risk appetite, and governance of cyber risk. The Board shall approve the cybersecurity policy and oversee its implementation.

2. The Board and Senior Management shall be accountable, responsible, and actively engaged in understanding and managing their entity's cyber risk, including related risk posture assessments, evolving cybersecurity trends and threats within the banking sector, and any other relevant initiatives.

3. The Board and Senior Management shall allocate adequate cybersecurity budget, assign roles and responsibilities with relevant expertise and promote cybersecurity culture at all levels within the Entity.

4. The Board and Senior Management shall ensure the implementation of appropriate security controls to mitigate cyber risks in both internal and outsourced functions executed through third party service providers.

5. The Regulated Entity shall have Information Security function independent from Information Technology operations. This Information Security function shall set the policies and standards, and monitor the implementation and operation of cybersecurity controls.

6. The information security function shall assess the adequacy of security controls to mitigate cyber risks, and would approve/ ensure approvals of any exceptions taking into consideration of applicable regulatory guidance and the entity's risk appetite.

7. The information security function shall update the board members periodically and on need basis about the overall status of their cybersecurity program (For example; briefing the Board about major cybersecurity crises, ongoing incidents response efforts, current cybersecurity risks, business impacts of such risks and plan to address them, review of exceptions, Briefing on applicable laws, regulations and industry best practices, Audit findings and corrective actions).

2.2.1.2 Risk Management

Risk management is an ongoing process to identify, assess, and address the risks. Accordingly, Regulated Entities shall conduct regular risk assessments to identify and manage cyber risks. Regulated Entities shall define criteria for risk acceptance and mitigation in their policies, and document all risks accordingly.

Regulated Entities shall align their risk management policies and procedures with the applicable areas of the CSF. Such alignment must prioritize the implementation of policies, procedures, and resources to improve cyber resilience.

While the CSF defines the cybersecurity baselines for Kuwaiti banking sector as a minimum security controls that must be complied with, Regulated Entities are encouraged to implement additional enhanced controls based on their risk appetite. Regulated Entities are also encouraged to collaborate across the sector on such enhanced controls to improve overall sector risk posture and may influence future updates to CSF baselines.

2.2.1.3 Compliance

Compliance is the process of conforming to stated requirements, applicable laws, regulations, internal and external standards, contracts, strategies, and policies. Regulated Entities' compliance with laws and regulations promotes the alignment of cybersecurity practices across the sector and enhances collaboration to increase the sector's overall maturity. As such, Regulated Entities shall comply with the CSF and applicable national and international laws, regulations and standards. Regulated Entities shall be able to demonstrate their:

- Identification and documentation of applicable national and international security compliance requirements;
- Compliance with Kuwaiti national laws, CBK regulations, and international standards, as applicable;

CBK shall continue to provide the necessary directives in the form of regulations, instructions and circulars as a part of its supervision initiatives.

2.2.2 Collaboration

As the technology, landscape evolves with fast changing innovations that disrupt the financial market leading to increasing cyber risks and threats. The need to foster collaboration is essential to improve skills, knowledge sharing, and leadership. CBK strongly encourages the Regulated Entities to closely collaborate to enable the Kuwaiti banking sector to combat the rapidly evolving cyber threat landscape.

2.2.2.1 Information Security Working Group

The CSF establishes the Information Security Working Group (ISWG) as a forum for collaborative discussions on cybersecurity controls, and the maturity of the Kuwaiti banking sector. The ISWG shall be a permanent forum where the Kuwaiti banking sector can collaborate and share insights into cybersecurity risks, trends and best practices. The ISWG may also engage and undertake activities of continual improvement.

The objectives of the ISWG include the following:

1. Provide a forum for the collaborative exchange of information, knowledge and intelligence to assist ISWG members to better manage cybersecurity risk.
2. Facilitate discussions on the latest cybersecurity trends and technologies that affect the Kuwaiti banking sector.
3. Provide support and guidance on cybersecurity initiatives and assist in complying with regulations.
4. Provide a robust platform to inform and undertake strategic initiatives that are relevant to cybersecurity risk.
5. Facilitate the analysis and monitoring of necessary safeguards and actions in response to cyber incidents.
6. Act as a forum to coordinate with external entities, such as the Government and other entities.
7. Facilitate cybersecurity awareness to engage and educate the Kuwaiti banks through events and initiatives.
8. Support Regulated Entities cyber resilience initiatives to protect against adverse cyber events.

2.2.2.2 Sectoral Initiatives, Awareness and Training

The CSF, recognizes the volatile nature of cyber risks and their impact on the banking sector, envisages a need for undertaking collaborative sectoral initiatives that will help to address awareness, training needs and specific cybersecurity concerns based on the current and evolving threat landscape and sectoral maturity. These initiatives aim to increase awareness and to train Regulated Entities (and the public, where appropriate) on specific issues, using a range of tools such as awareness campaigns, structured training programs and simulations.

2.2.2.3 Cyber Threat Intelligence Sharing

This component of the CSF defines the strategy and functions of a Cyber Threat Intelligence Sharing (CTIS) to facilitate collaboration between Regulated Entities in the discovery, analysis, understanding, and sharing of information about cyber threats arising out of global, regional, and local events. This collaboration, supported by various threat intelligence feeds, shall promote proactive measures for continuous improvement of cybersecurity controls by Regulated Entities.

The CTIS Strategy establishes the structure, considerations, policies and procedures for CTIS. The CTIS strategy elaborates the requirement of CTIS platform for collaboration along with a Sectoral Computer Security Incident Response Team (CSIRT) to provide valuable analysis to support incident response efforts of an entity, and to safeguard the other Regulated Entities by sharing cyber intelligence.

The cyber threat intelligence information shall be classified as strategic, operational, or tactical depending on whether the information is relevant against immediate threats, or to improve the protection of Regulated Entities against possible threat, or if it assists the Kuwaiti Banking Sector to visualize the risks related to strategic business trends.

The CTIS process for Kuwaiti Banking sector is illustrated as below, and is elaborated in the CTIS Strategy.

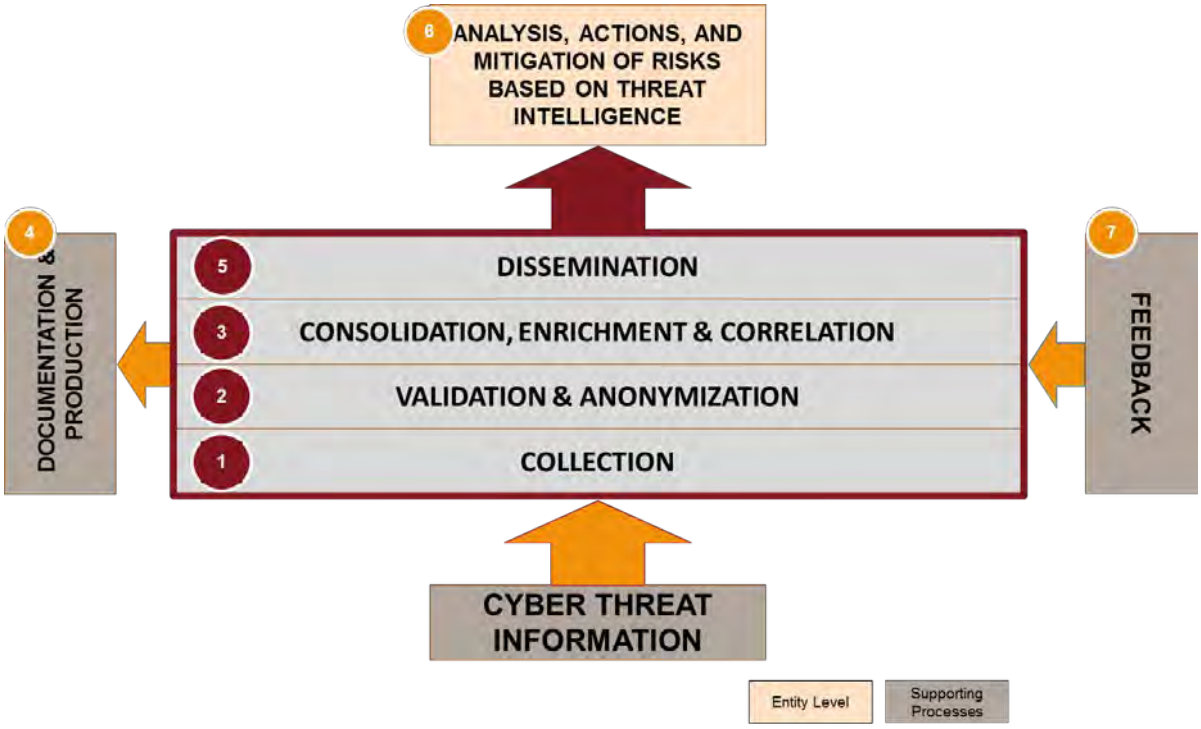


Figure 2: Cyber Threat Information Sharing Process

CBK and CTIS Management shall undertake necessary efforts to establish a culture of trust, sharing and caring. The CTIS Strategy is based on the principles that entities and individuals who share information:

- enable better protection of the Banking Sector and the State of Kuwait; and
- shall only be judged for how they responded and reacted to threats and incidents (i.e. being opened and sharing rather than hiding and letting others also be attacked).

The cyber threat intelligence labelling methodology identified in the CTIS strategy is based on the following principles to assist in protecting identity of reporting entity and promoting sectoral collaboration with established trust:

- all Regulated Entities shall abide by the usage and sharing method defined for each label category; and
- only the originator of the information can determine the final label of intelligence.

CBK will assess the sectoral criticality and requirement to promote establishment of a sectoral Security Operations Center (SOC) on long-term plan for centralizing the operations of essential sectoral monitoring and for invoking the timely identification, communication, stakeholder engagement, and management of cyber incidents within the sector.

2.2.3 Continual Improvement

The CSF identifies continual improvement as an essential category of the CSF that drives the cyclical and event based improvement of cybersecurity maturity across the banking sector. The continual improvement components require Regulated Entities to implement cybersecurity baselines, execute continual assessments of the effectiveness and maturity of their cybersecurity baselines, and prepare to respond to cyber-attacks.

The CSF defines the following components of continual improvement.

2.2.3.1 Cybersecurity Baselines

The CSF envisages the need to establish Cybersecurity Baselines (hereinafter referred to as Baselines) as minimum requirements that Regulated Entities shall implement to improve their overall cybersecurity posture. The Baselines have been designed with necessary and appropriate consideration of CBK's regulations, instructions and guidelines, prevalent international cybersecurity standards and frameworks such as National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Information Security Forum (ISF), Payment Card Industry (PCI), Center for Internet Security (CIS) and CPMI-IOSCO PFMI.

The baselines are grouped into a hierarchical structure of domains, subdomains and controls. The baselines will ensure consistent implementation and interpretation of controls across the banking sector. CBK will monitor the implementation of these baselines and undertake necessary initiatives to improve the sectoral maturity. The four domains of baselines are as below:

a) Governance, Risk management, and Compliance:

Governance, Risk management and Compliance processes are essential for effective management of cybersecurity risks. These processes shall assist Regulated Entities to define, implement, monitor, oversee and assess the effectiveness of framework, strategies, policies and controls.

b) Technology and Operations:

Regulated Entities depend on technology to operate and deliver services to end customers and internal users. To ensure the security and reliability of technology assets, Regulated Entities shall implement appropriate security controls within their technology assets.

c) Third Party Security:

Regulated Entities depend on multiple third-party vendors to operate or execute their business functions. Innovation and efficiency are key drivers for such continued and increasing reliance on third party vendors. Further, entities increasingly engage with third party vendors for expertise, ease of operations, and access to new technologies to improve the overall delivery of financial services to its customers. This domain specifies controls to identify, mitigate and effectively monitor risks emanating from third party service providers.

d) Protection of Electronic Payment Systems:

Global demand for faster and reliable electronic payments has resulted in rapid development of innovative electronic payment systems. Electronic payment systems are anticipated to evolve further with new technologies, innovative customer services and improved products and solutions. This domain specifies controls to identify, mitigate and effectively monitor risks related to payment systems.

The above domains are further classified into sub-domains pertaining to specific cybersecurity as listed in below table:

Governance, Risk Management, and Compliance	Technology and Operations	Third Party Security	Protection of Electronic Payment Systems
Governance	Security Architecture Design	Third Party Outsourcing	Common Security Controls For Electronic Payment Systems
Cybersecurity Strategy	Asset Management and Classification	Cloud Security	Electronic Payment Transaction Monitoring
Cybersecurity Policy	Infrastructure Security		Online Banking Security

Governance, Risk Management, and Compliance	Technology and Operations	Third Party Security	Protection of Electronic Payment Systems
Cybersecurity Risk Management	Secure Software Lifecycle Management		Mobile Banking Security
Compliance	Security Considerations for Emerging Technologies		Customer Self Service Machines (ATMs,POSs,KIOSKs,ITMs,XTMs, etc.)
Independent Audit	Access Control Management		Contactless Technology
	Cryptography		
	Change and Release Management		
	Capacity Management		
	Data Privacy And Security		
	Email Security		
	Portable Device Security		
	Reputation Protection		
	Logging, Monitoring and Security Incident Management		
	Vulnerability Management		
	Human Resource Security		
	Security Awareness and Training		

Governance, Risk Management, and Compliance	Technology and Operations	Third Party Security	Protection of Electronic Payment Systems
	Physical and Environmental Security		
	Business Continuity and Disaster Recovery (BC and DR)		
	Cyber Crisis Management		
	Cyber Threat Intelligence Management		

Table 1: Domains and Sub-domains of Cybersecurity Baselines for Kuwaiti Banking Sector.

The sub-domains contain the control considerations for effective management of cybersecurity controls within that area and detailed in Cybersecurity Baselines. All controls are uniquely numbered across the baselines for ease of reference.

Regulated Entities shall implement necessary mechanisms and processes to ensure compliance with the baselines and address the gaps identified by undertaking appropriate corrective actions.
This is essential to limit the impact of potential cyber-attacks that may disrupt business operations, damage customer trust and an entity's reputation, and/or result in regulatory action.

The Regulated Entities shall adhere to the baselines at all times. The implementation of the baselines shall assist in achieving an acceptable risk level for an entity and improve sectoral maturity. CBK encourages the Regulated Entities to exceed these baselines in accordance with their risk appetite. Regulated Entities may also refer on a case by case basis to CBK for clarifications, and may suggest improvements or initiatives for consideration by CBK and the ISWG.

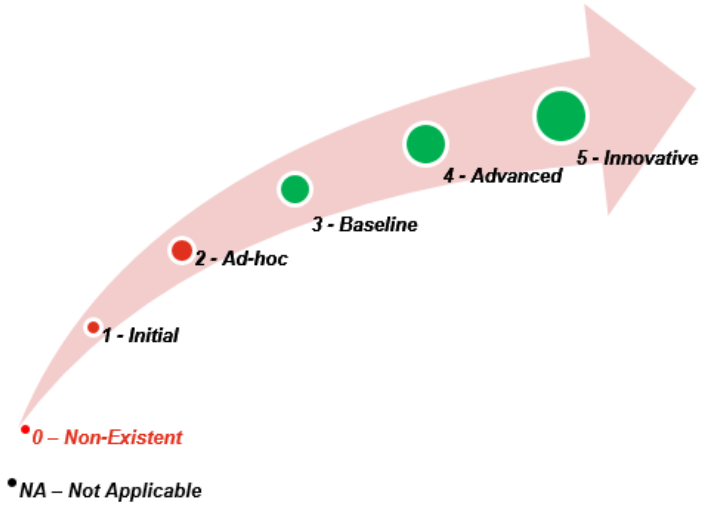
2.2.3.2 Assessment & Maturity

The Assessment and Maturity component helps CBK to identify the existing levels of cyber risk within the Regulated Entity and also across the sector and sets the required levels of maturity of cybersecurity controls within the Regulated Entities. This component is a repeatable and measurable process that leverages an assessment tool (template) that allows CBK to measure and report on the cyber risk that exists within the Regulated Entities, and the Regulated Entities' compliance with the baselines. This component promotes Regulated Entities' compliance to baselines and continual improvement of cybersecurity maturity.

This component incorporates international best practice, frameworks and standards and is aligned to the risk profile of the Regulated Entities. It contains three (3) key elements that the Regulated Entities are required to complete:

1. **Inherent Risk Profile:** This identifies the inherent risk to the Regulated Entity's business operations prior to implementing controls, which informs minimum control maturity requirements;
2. **Baselines Assessment:** Regulated Entities shall complete an assessment against the baselines to assist in identifying the maturity of its cybersecurity controls and hence residual risks within the Regulated Entities; and
3. **Assessment Reporting:** Regulated Entities shall provide CBK with their baseline assessment results along with the remediation activities and plans where required.

In addition, the assessment template provides a rating scale for assessment of controls. The rating scale is designed specifically for Kuwaiti Banking Sector and factors their varied businesses, technical needs, inherent risks, and progressive implementation plans. The rating scale for cybersecurity assessment and maturity is as below:



The Cybersecurity assessment template and the guidebook document are designed to assist consistent assessment and reporting.

Assessments, reports, and plans shall be subject to CBK's periodic review and supervision. CBK may suggest/ mandate necessary changes to inherent risk profiling, baseline assessment, plans, exceptions and exclusions and may conduct necessary inspection.

While this component enhances the visibility of the risks and controls within the individual Regulated Entities, when the assessment results are combined and aggregated appropriately, it also improves the visibility of the maturity of cybersecurity across the sector. This enables CBK to identify necessary initiatives or actions required to drive essential sectoral improvements.

2.2.3.3 Cyber Crisis Management & Plan

The volatile nature of cyber threats can create significant service interruptions and quickly spread across systems and virtual boundaries. This increases the risk for Regulated Entities as they potentially become vulnerable to secondary exposure. CBK recognizes the need for Regulated Entities to be alert and capable to appropriately identify and efficiently manage crisis responses. This requires Regulated Entities to engage in leading practices, including:

- Consistent preparation based on clear policy derived organizational structures and roles;
- Thorough response planning based on severity and impact;
- A continuous learning posture, including exercising of response plans; and
- Update plans and preparation based on lessons learned from real and simulated responses.

The Cyber Crisis Management component is identified as a critical component to ensure resilience of Kuwaiti Banking Sector by promoting effective, efficient, and consistent responses to cybersecurity incidents and related crises. This component fulfils the objectives of CSF by enhancing sector wide preparation, collaboration, compliance, and continuous improvement to manage cyber crises. While Cyber Crisis Management necessitates collaboration among Regulated Entities, it is classified under continual improvement due to the cyclical nature.

The Cyber Crisis Management Strategy and Plan (CMSP) defines requirements which is independent from business continuity management considerations, for the Regulated Entities' crisis management preparation and response processes to promote the sector's resilience and capability to emerge stronger from Cyber incidents. The CMSP's minimum requirements for effective crisis management within regulated entities are also included within the CSF's baselines. The Regulated Entities must align their internal incident management and crisis management programs accordingly.

3. Cyber Resilience Components, Tools and Functions

The below illustration (Figure 2) depicts the components and their underlying tools and functions. Although the tools and functions are represented as separate identifiable activities, the tools and functions may connect with each other on need basis. For example, a crisis management exercise may lead to a strategic initiative or awareness and training campaign, or a threat intelligence update might lead to updates in baselines.

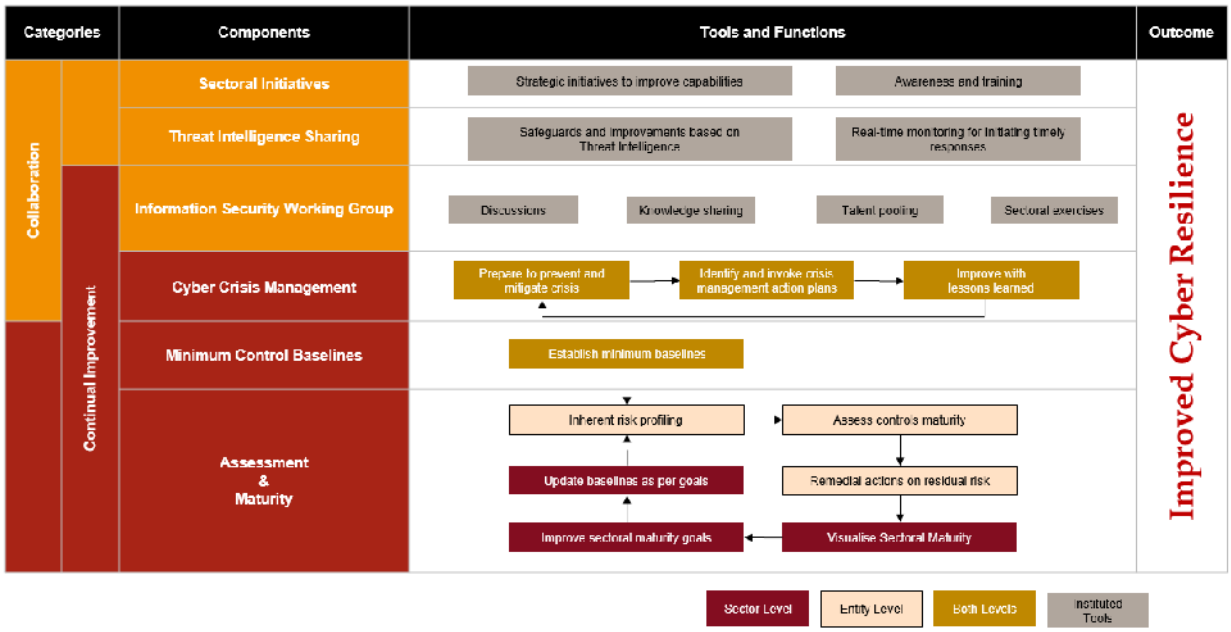


Figure 2: Cyber Resilience Roadmap – Operational View.

3.1 Collaboration Components, Tools and Functions

The tools, functions and supporting process of collaboration components shall be effective on need basis as listed below to promote the adoption of best practices through collaboration and knowledge sharing:

3.1.1 Sectoral Initiatives: The CSF provides this collaborative tool to discuss and undertake the necessary sectoral initiatives to improve cybersecurity of the banking sector.

3.1.2 Awareness and Training: This facilitates the necessary propagation of awareness and training to improve cybersecurity.

3.1.3 **Safeguards and improvements based on threat intelligence:** This facilitates the Kuwaiti Banking sector to proactively discuss, identify, and implement the necessary safeguards and improvements within the Regulated Entities to address specific current threats.

3.1.4 **Real-time monitoring for initiating timely responses:** This facilitates a structure for reporting incidents and updates for initiating timely responses.

3.1.5 **Information security working group:** ISWG facilitates collaborative discussions, knowledge sharing and talent pooling for enhancing cybersecurity. ISWG can also undertake collaborative sectoral exercises for improving sectoral preparedness on cybersecurity.

3.2 Continual Improvement Components, Tools and Functions

The tools and functions that underpin continual improvement components operate as constant and repeating cycles to enable the Regulated Entities to gradually improve the maturity of their cybersecurity controls, and hence the improve cyber resilience of the Kuwaiti Banking sector. The cycles of continual improvement leveraging the components of Cyber Crisis Management, Baselines, Assessment and Maturity are elaborated in the following sections.

3.2.1 Cyber Crisis Management Cycle

The Cyber Crisis Management cycle includes the following key functions as a continual flow:

1. **Prepare to prevent and mitigate crisis:** The CSF's baselines include minimum controls required for the Regulated Entities to mitigate crisis, focused on:
   - Cybersecurity strategy;
   - Cyber crisis organizational structure, including at a minimum of crisis management team, crisis response lead, and a Board approved severity impact matrix;
   - Board approved planning for crisis management, disaster recovery, and business continuity;
   - Regular exercising to improve familiarity and internalization;
   - Appropriate threat intelligence feeds that inform improvement opportunities; and
   - Continuous learning model for crisis management preparation.

2. **Identify and invoke crisis management action plans:** The CMSP specifies the process of continuous monitoring and facilitates the timely invocation of sectoral crisis based on a pre-defined severity impact matrix for such assessment. A crisis response plan would then be invoked to ensure response and recovery measures.

3. **Improve with lessons learned:** The CSF and the CMSP drive continual learning, which is based on lessons learnt during a crisis. The plans that were identified as effective during a crisis or during a simulation of a crisis can be utilized by the Regulated Entities and further improved.

3.2.2 Cybersecurity Baselines and Assessment-Maturity Cycle

The Baselines and Assessment & Maturity cycle includes the following key functions as a continual flow:

1. **Establish baselines:** The baselines are identified collaboratively and must be complied with by Regulated Entities. They ensure the existence of a minimum level of maturity of cybersecurity controls in operation across the banking sector.

2. **Inherent risk profiling:** Regulated Entity's level inherent risk profiling enables the identification of appropriate control measures and associated assessment procedure to be applied to the specific Regulated Entity. Entity level profiling results are shared with CBK. CBK will issue appropriate guidance on applicable assessment procedures based on the results, and aggregate the results to visualize sectoral risk posture.

3. **Assess control maturity:** Entity level assessment of control maturity of Regulated Entities enables the regulatory framework to verify the effectiveness of implemented controls and understand the control maturity and residual risks of each Regulated Entity.

4. **Remedial actions on residual risks:** Regulated Entities assess and commence necessary actions to remediate the identified residual risks and improve cybersecurity controls maturity. Such actions are time bound and the progress of remediation is reported to CBK.

5. **Visualize sectoral maturity:** CBK will aggregate the results of entity level Inherent risk profiling and cybersecurity controls assessments to analyze and understand sectoral maturity and underline necessary actions to improve sectoral maturity.

6. **Improve sectoral maturity goals:** Subsequent to visualization of sectoral cybersecurity controls maturity, CBK reviews the maturity levels and undertakes the necessary actions to improve them by utilizing the various components defined within this framework.

7. **Update the baselines:** CBK considers available observations from entity and sectoral maturity reviews and undertakes the necessary amendments to the baselines for adherence by the Regulated Entities in the subsequent iteration of this cycle.

Assessment results, supporting documents and remediation plans are subject to CBK review, supervision, and audit. CBK shall aggregate their observations based on such assessment results and may direct the periodicity and methodology for subsequent assessments and audits as a part of CBK's supervision procedures.

4. Review and Update

The CSF is a framework with cohesive set of strategies, policies and approaches that are aligned to the overall objectives. It is essential that the CSF remains relevant to evolving technologies, emerging trends, regulatory expectations and improved controls for continued adherence and performance. Accordingly, the CSF shall be reviewed on an annual basis and updated where necessary.

5. Appendix – Glossary

The effective management of cybersecurity requires consistent understanding and interpretation of Cybersecurity Framework, related documents, circulars, and notifications. The entities and stakeholders in scope of CSF documentations are as below:

Term	Definition
CBK	Refers to the Central Bank of Kuwait.
Regulated Entities	Refers the following: ● Kuwaiti Banks ● Foreign Banks ● Finance Companies ● Exchange Companies ● Investment Companies ● Companies/ Organizations that are subject to Payments Regulations (Law 20 of 2014 Chapter 6).
Regulated entity level or Entity level	Refers to aspects or expectations at each entity level.
Kuwaiti Banking Sector	Refers the entire banking sector including the Regulated Entities and CBK.
ISWG	Refers to the Information Security Working Group.
Third Party	Refers to any organization providing products or services to the Regulated Entities. The term also includes such third parties who have access to technology assets of the regulated entity.
Users	Refers to employees and third-party vendor staff having access to information assets.

The below terms shall assist in interpreting the roles and assignment of specific actions to the roles:

Term	Definition
Accountability	Refers to the identification of the role, team, unit or entity that is ultimately answerable for the referred activities or decisions.
Responsibility	Refers to the assignment of tasks, actions or implementation steps to team or personnel for ensuring the execution. Responsibility can be shared or delegated based on documented authorizations.
Relevant stakeholders	Refers to personnel at entity level who are accountable or responsible for performance, compliance, decisions, or approvals.
Asset Owner	Refers to an individual who is approved by the management to control, use and be responsible and accountable for security of the specific asset.
Crisis Response Lead	Refers to an employee of Regulated Entity who is authorized to make crisis response related decisions independently and on behalf of the Regulated Entity and to act as a single point of contact and lead representative of the Regulated Entity in CBK-led, sector-wide responses.

The below terms explain reference to the various components and their documentation as a part of the overall Cybersecurity Framework for Kuwaiti Banking Sector:

Term	Definition
CSF	Refers to the Cybersecurity Framework issued by Central Bank of Kuwait.
ISWG TOR	Refers to the Terms of Reference of Information Security Working Group.
Cybersecurity Baselines or Baselines	Refers to Cybersecurity baselines that are required to be implemented by Regulated Entities.
CMSP	Refers to the Cyber Crisis Management Strategy and Plan.
CTIS Strategy	Refers to Cyber Threat Intelligence Sharing Strategy.
CSIRT	Refers to Computer Security Incident Response team.

The below references are made within the CSF documentation:

Term	Definition
CIS	Refers to Center for Internet Security.
Cyber Lexicon	Refers to the Lexicon of terms related to cybersecurity and cyber resilience published by Financial Stability Board.
ISAC	Refers to Information Sharing and Analysis Center.
ISAO	Refers to Information Sharing and Analysis Organization.
ISF	Refers to Information Security Forum.
ISO/IEC	Refers to International Organization for Standardization/ International Electrotechnical Commission.
NIST	Refers to National Institute of Standards and Technology.
PCI	Refers to Payment Card Industry.

INFORMATION SECURITY WORKING GROUP
TERMS OF REFERENCE

INFORMATION SECURITY WORKING GROUP
TERMS OF REFERENCE

TABLE OF CONTENTS

1 Introduction

As per Article 15 of Law No. 32 of 1968, Central Bank of Kuwait (CBK) is responsible to supervise the Kuwaiti banking sector. As part of these supervision initiatives, a decision was made by H.E. the Governor, to have a forum to discuss cybersecurity risks and trends among the Kuwaiti banking sector under the CBK leadership. The purpose of the forum is to oversee the effectiveness of cybersecurity risk management and to foster effective cybersecurity practices among Kuwaiti banking sector to promote cyber resilience.

Based on this initiative, CBK identified the need for a permanent forum whereby the Kuwaiti banking sector can openly collaborate and share insights into cybersecurity risks and trends. The Information Security Working Group (ISWG) was then formed and cybersecurity professionals from the Kuwaiti banks were invited to join. The ISWG comprises of members from all Kuwaiti banks and CBK.

This Terms of Reference (hereinafter referred to as 'ISWG TOR' or 'TOR') document describes the objectives, roles and responsibilities, and the code of conduct of the ISWG. This document forms a part of CBK's initiative of Cybersecurity Framework for the Kuwaiti Banking Sector

2 Objectives

It is the responsibility of ISWG members to collaborate with the Kuwaiti banking sector and the relevant government and other external entities in order to protect critical assets, respond to the incidents effectively, and recover operations in a timely manner. The ISWG objectives includes the following:

a) Provide a forum for the collaborative exchange of information, knowledge and intelligence to assist ISWG members to better manage cybersecurity risk.

b) Facilitate discussions on the latest cybersecurity trends and technologies that affect the Kuwaiti banking sector.

c) Provide support and guidance on cybersecurity initiatives and assist in complying with applicable regulations.

d) Provide a robust platform to inform and undertake strategic initiatives that are relevant to cybersecurity risk.

e) Facilitate the analysis and monitoring of necessary safeguards and actions in response to cyber incidents.

f) Act as a forum to coordinate with external entities, such as, the Government and other entities.

g) Facilitate cybersecurity awareness to engage and educate the regulated entities through events and initiatives.

h) Support the cyber resilience initiatives of Regulated Entities to protect against adverse cyber events.

3 Roles and Responsibilities

3.1 ISWG Chairman

The ISWG Chairman is appointed by H.E. the Governor. The Chairman, will ensure that the ISWG functions properly, that there is full participation during meetings, facilitate discussion on all relevant subject, and that effective decisions are made and carried out. The Chairman is also responsible for initiating and executing necessary activities to achieve ISWG objectives, annual review of this ISWG TOR, and final approval of ISWG decisions. In the event of the Chairman being absent, a CBK representative will be assigned with temporary Chairman responsibilities as outlined above.

3.2 CBK Representatives

CBK representatives are appointed by the ISWG Chairman and are responsible for assisting the ISWG Chairman in achieving the objectives of ISWG, as well managing and coordinating ISWG meetings. In addition, CBK representatives will manage communication, which is comprised of meeting schedules, attendance, meeting minutes, invitations and third-party engagements.

3.3 Member Organizations

Member organizations are responsible for contributing resources, time, and expertise in order to serve the ISWG objectives and collaborate engagements by sharing timely cyber incident, escalations, early warnings, studies, raising issues, proposing solutions to protect critical assets, responding to the incidents in an effective manner and recover operations in a timely manner within the Kuwaiti banking sector.

Member organizations will commit to participating in ISWG meetings, agenda and plans for the whole duration. Member organizations shall nominate representatives to join the ISWG by submitting a written request to the ISWG Chairman. The Chairman, will formally review and approve the nominations of representatives from member organizations. The approval is subject to the nominated representative adequately complying with the following requirements:

a) The representative should have a senior role within the member organizations' information security / cybersecurity team.

b) The representative should have cybersecurity experience to ensure they are able to understand the content discussed within the ISWG, contribute to discussions and they are able to effectively communicate required information back to the member organizations.

c) The approved representatives are required to abide by the Code of Conduct.

4 Code of Conduct

The ISWG Code of Conduct is an important safeguard to the relationships between ISWG members. Failure to meet the requirements included in this section, would significantly undermine the effectiveness of ISWG. The enforcement of the Code of Conduct will be at the ISWG Chairman's discretion.

4.1 Conduct

All members of the ISWG are treated equally and are required to treat other members of this group with respect and courtesy. The members must focus on achieving the ISWG objectives, which are stated above in this document and must not use the information shared within ISWG for gaining competitive advantages. All member organizations must adhere to the decisions and directions of the ISWG Chairman.

4.2 Confidentiality

All discussions, information shared, issues raised, meeting minutes noted or meetings recordings are to be considered confidential. Confidential information should not to be shared outside of the member organizations by the representatives. Member organizations and their representatives of the ISWG agree not to use confidential information shared and discussed within the ISWG for competitive or commercial purposes. Members of the ISWG also agree not to share any personal information of other members of the group.

4.3 Conflicts of Interest

Any actual or potential conflicts of interest by ISWG members shall be noted by the CBK member concerned and raised to the ISWG Chairman. The Chairman, will assess any raised conflict of interest in conjunction with the impacted members' roles and responsibilities, and initiate possible actions.

4.4 Attendance

The representatives should attend all meetings and provide in advance notice (one business day) in case of absence; exceptions will be applied for emergency meetings. Members should be prepared for the meetings in accordance with the agenda and should contribute proactively in discussions, raising of issues, recommending solutions, and resolving conflicts. All

members are encouraged to fulfill the responsibilities assigned to them with the aim of achieving the objectives ISWG.

4.5 Invitees

Invitees could be other representatives from the CBK team, government entities, third parties or subject matter experts (SMEs) to provide an independent input based on experience and expertise on the subjects under discussion during the meeting. Invitees, are responsible to abide by ISWG's code of conduct and agree to keep meeting engagements and discussion private. Invitees are only allowed to join the ISWG sessions with approval from the ISWG Chairman and for the time slot that they have been allocated.

5 Frequency of Meetings

The ISWG meetings will be held at least once every quarter or whenever necessary. Member organizations that require additional ISWG meetings should submit a written request to the ISWG Chairman. Any additional ISWG meetings will be held at the discretion of the Chairman.

5.1 Meeting Agenda

The meeting agenda will be distributed to the members within two business days in advance of ISWG meeting, so that members can prepare accordingly for the ISWG meeting. Exceptions will be made for emergency meetings at the discretion of the ISWG Chairman. Member organizations can request to include certain discussions by contacting the Chairman/CBK representatives.

5.2 Meeting Minutes

Meeting minutes serve as an official record of the meetings of the ISWG. The meeting minutes will be recorded by a CBK representatives and distributed to members after the ISWG meeting for any feedback before finalization.

5.3 Reporting

The ISWG would primarily work on the basis of an agenda, discussions, presentations, and minutes. Some of the underlying action items may cascade into additional initiatives or action items that eventually executed separately and are included as updates in subsequent presentations to ISWG.

6 Review and Update

The ISWG Terms of Reference shall be reviewed on an annual basis and updated if necessary. Any reviews or updates should be discussed with the ISWG members and any changes made to the Terms of Reference must be approved by the ISWG Chairman.

7 Contact Information

All communication from member organization representatives should be addressed to CBK representatives via KB_ISWG@cbk.gov.kw.

CYBERSECURITY BASELINES
FOR
KUWAITI BANKING SECTOR

CYBERSECURITY BASELINES
FOR
KUWAITI BANKING SECTOR

TABLE OF CONTENTS

1 Introduction

The State of Kuwait recognizes the importance of promoting the security of 'Critical National Infrastructure' and has published the “National Cybersecurity Strategy for the State of Kuwait, highlighting Kuwait’s banking sector as critical national infrastructure. Accordingly, the Central Bank of Kuwait (CBK) identifies the need for the banking sector to improve its resilience to cyber-attacks and is undertaking multiple initiatives under the ambit of Cybersecurity Framework (CSF). The CSF aims to integrate cybersecurity and cyber resilience within the governance and operations of Regulated Entities.

This document specifies the ‘Cybersecurity Baselines' (hereinafter referred to as 'Baselines') that Regulated Entities shall implement to improve their overall cybersecurity posture. This document forms a part of CBK’s initiative of Cybersecurity Framework for the Kuwaiti Banking Sector.

The Baselines are developed to ensure existence of consistent cybersecurity controls within Regulated Entities and improve the banking sector’s preparedness for cyber-attacks. Regulated Entities are encouraged to implement enhanced controls beyond these baselines depending on the risks identified within their environment and the entity's risk appetite.

1.1 Scope

The Cybersecurity Baselines are designed to provide the requirements to Cybersecurity management system and cybersecurity standards including selection, implementation, management and continual improvement of the cybersecurity controls in line with the entity inherent risk profile and cyber risk exposure.

The scope of the Baselines includes cybersecurity related policies, procedures and controls applicable to people, process and technology and covers:

a) hardware, software, network, and IT components;
b) electronic information / records;
c) physical installations such as data centers, information processing facilities and disaster recovery sites;
d) people and associated processes; and
e) third party providers and customers.

The Baselines have been designed with necessary and appropriate consideration of CBK’s regulations, instructions and guidelines, prevalent international cybersecurity standards and

frameworks such as National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Information Security Forum (ISF), Payment Card Industry (PCI), Center for Internet Security (CIS) and CPMI-IOSCO PFMI.

1.2 Applicability

The Baselines are applicable to all Regulated Entities supervised by the CBK and the compliance to Baselines is subject to CBK supervision/ assessment.

Further, the Baselines are applicable to Regulated Entities, their employees, third party vendors and third party vendor staff.

While complying with Baselines, the Regulated Entities may seek specific clarifications or approvals from CBK to ensure continued compliance.

1.3 Target Audience

The Baselines are issued for the Board of Directors, Senior Management, information security professionals and information technology professionals and any other personnel who are responsible for establishing, implementing and ensuring compliance with CBK directives.

1.4 Approach for Implementation

Regulated Entities shall follow a structured self-assessment approach, which assists in identifying and implementing the applicable controls as specified in the Baselines. The steps for implementing the Baselines are:

a) **Inherent Risk Profile**: Regulated Entities shall identify the inherent risk to business operations prior to implementing controls.

b) **Initial Baseline Assessment:** Regulated Entities shall complete an assessment against the baselines to assist in identifying the maturity of its cybersecurity controls and residual risks within the Regulated Entities. Appropriate business justifications for exclusion shall be documented as part of the assessment;

c) **Initial Reporting:** Regulated Entities shall provide CBK with their inherent risk profiling and initial baseline assessment results and the remediation activities and plans; and

d) **Periodic / adhoc assessment and reporting:** Regulated Entities shall conduct periodic / adhoc inherent risk profiling and baselines assessments as stipulated by CBK and report the assessment results.

Assessments, reports, and plans shall be subject to CBK's periodic review and supervision. CBK may suggest/ mandate necessary changes to inherent risk profiling, baseline assessment, plans, exceptions and exclusions and may conduct necessary inspection.

2 Principles of Cybersecurity Baselines

The Cybersecurity Baselines are established based on the below principles[1]:

a) **Confidentiality**: Ensuring that information is neither made available nor disclosed to unauthorized individuals, entities, processes or systems;

b) **Integrity**: Property of accuracy and completeness.;

c) **Availability**: Ensuring that information is accessible and usable by authorized users/ entities;

d) **Authenticity**: Establishing confidence that information is valid, verified, and can be trusted;

e) **Non-Repudiation**: Able to prove or establish the occurrence of a claimed event or action and its originating entities;

f) **Identification**: Initiating a process to identify an entity and to verify its professed identity;

g) **Authorization**: Approving an information system's operations based on a documented set of security controls and an authorization matrix; and

h) **Accountability**: Ensuring that the actions of a user/ an entity is traced uniquely to that user/entity.

[1] *The definition of the principles are adopted from the cyber lexicon published by Financial Stability Board.*

3 Structure for Baselines

The Cybersecurity Baselines (Baselines) are structured as domains, sub-domains, and controls as defined below:

- the domain specifies the intent for a given area;
- the sub-domain establishes the objective; and
- controls specify applicable baselines that shall be covered under each sub-domain.

Structure:

X. (Domain)

X.1 (Sub-Domain)

X.1.1 (Control)

Example:

4. Cybersecurity Governance, Risk management and Compliance

4.1 Governance

4.1.1 The Board of Directors…..

3.1 Domains

The Cybersecurity Baselines have been logically grouped into 4 broad domains and 36 sub-domains on the basis of the nature of controls. The controls specified within each domain and sub-domain collectively assist in establishing consistent cybersecurity controls within Regulated Entities and achieving the objectives of Cybersecurity Framework (CSF). The identified domains of the Baselines are:

a) Governance, Risk Management, and Compliance: This domain shall assist Regulated Entities in defining a governance framework. The framework shall enable effective management and mitigation of cybersecurity risks. This domain shall assist entities in adherence to and tracking of applicable global and local compliance requirements.

b) Technology and Operations: This domain defines the baselines that shall be implemented for securing the technology assets of the Regulated Entities. This shall help Regulated Entities to identify, mitigate and monitor technology risks.

c) Third Party Security: This domain specifies controls that shall be implemented to protect against risks emanating from third party service providers. This shall help Regulated Entities to identify, mitigate and effectively monitor third party risks.

d) Protection of electronic payment systems: This domain defines the baselines that shall be implemented by the Regulated Entities to identify, mitigate and monitor cybersecurity risks related to payment systems.

3.2 Sub-domains

The sub-domains of the above domains are represented below in tabular form:

Governance, Risk Management, and Compliance	Technology and Operations	Third Party Security	Protection of electronic payment systems
Governance	Security Architecture Design	Third Party Outsourcing	Common Security Controls For Electronic Payment Systems
Cybersecurity Strategy	Asset Management and Classification	Cloud Security	Electronic Payment Transaction Monitoring
Cybersecurity Policy	Infrastructure Security		Online Banking Security
Cybersecurity Risk Management	Secure Software Lifecycle Management		Mobile Banking Security
Compliance	Security Considerations for Emerging Technologies		Payment Card Information
Independent Audit	Access Control Management		Customer Self Service Machines (ATMs, POSs, KIOSKs, ITMs, XTM,…etc)
	Cryptography		Contactless Technology
	Change and Release Management		
	Capacity Management		
	Data Privacy And Security		
	Email Security		
	Portable Device Security		
	Reputation Protection		
	Logging, Monitoring and Security Incident Management		
	Vulnerability Management		
	Human Resource Security		
	Security Awareness and Training		
	Physical and Environmental Security		
	Business Continuity and Disaster Recovery (BC and DR)		
	Cyber Crisis Management		
	Cyber Threat Intelligence Management		

4 Governance, Risk management, and Compliance

Overview: Governance, Risk management and Compliance processes are essential for effective management of cybersecurity risks. These processes shall assist Regulated Entities to define, implement, monitor, oversee and assess the effectiveness of framework, strategies, policies and controls.

4.1 Governance

Objective: To ensure the required governance and operationalization of Cybersecurity initiatives within Regulated Entities, the Regulated Entities shall clearly define and identify the personnel and their roles and responsibilities with respect to cybersecurity.

4.1.1 The Board of Directors (hereinafter referred as, the Board) and Senior Management of Regulated Entities shall be the approving authority for the strategy, policy and other entity-wide cybersecurity initiatives. However, this right of approval may be delegated and shall be appropriately documented.

4.1.2 The Board and Senior Management shall be accountable, responsible, and actively engaged in understanding and managing their entity's cyber risk, including approving risk tolerance levels and managing evolving cybersecurity trends and threats within the banking sector and promote continual improvement.

4.1.3 The Board and Senior Management shall allocate adequate cybersecurity budget, assign roles and responsibilities with relevant expertise and promote cybersecurity culture at all levels within the organization.

Information security function

4.1.4 Regulated Entities shall establish an Information Security function independent from Information Technology operations, and empowered by the Board. This independent function shall be headed by a designated Information Security professional and shall have necessary skills, knowledge and competency.

4.1.5 The size of the information security function shall be based on the complexity, nature of business, technology assets and complexity of operations.

4.1.6 The information security function shall set the policies and standards for the implementation, operation and monitoring of cybersecurity controls in alignment with regulated entity's strategy and risk appetite.

4.1.7 The information security function shall assess the adequacy of security controls to mitigate cyber risks, and would approve/ ensure approvals of any exceptions taking into consideration of the applicable regulatory guidance and the entity's risk appetite.

4.1.8 The information security function shall ensure that cybersecurity awareness and training programs are effectively provided/ delivered to all employees and third party vendors, where applicable.

4.1.9 The information security function shall update their Board periodically and on need basis about the overall status of their cybersecurity program.

4.2 Cybersecurity Strategy

Objective: To ensure effective execution of cybersecurity initiatives, Regulated Entities shall define and implement a cybersecurity strategy in alignment with their overall business strategy and sectoral cybersecurity framework.

4.2.1 The cybersecurity strategy shall be defined, approved, implemented and reviewed annually.

4.2.2 Regulated entity's cybersecurity strategy shall:

a) include clear cybersecurity objectives aligned with organizational goals and business objectives;

b) align with the current deployed technology environment and future technology-related initiatives;

c) mandate compliance with applicable regulatory, legal and business requirements; and

d) define the thresholds and hierarchy for reporting.

4.2.3 Regulated Entities shall identify the responsibility and accountability for strategy implementation and monitoring.

4.3 Cybersecurity Policy

Objective: To set the management intent towards cybersecurity and plan the approach to manage cyber risks, the Regulated Entities shall adopt a cybersecurity policy that addresses the principles outlined in the Baselines.

4.3.1 The cybersecurity policy shall be defined, approved, implemented and communicated to all employees and third party vendors, where applicable.

4.3.2 The cybersecurity policy shall be reviewed at least annually or when warranted by changes to current business, technology assets and operating environment.

4.3.3 The cybersecurity policy shall:

a) define Senior Management's commitment, cybersecurity roles and responsibilities, enforcement mechanisms and deterrents for non-compliance;
b) include domains in alignment with the Regulated Entity's business objectives and technology assets;
c) incorporate relevant international best practices, frameworks and standards; and
d) consider applicable legal, regulatory and business requirements.

4.3.4 Regulated Entities shall ensure that supporting procedures, processes and guidelines are established to enable the implementation of the policy.

4.4 Cybersecurity Risk Management

Objective: To ensure that cyber risks are identified, analyzed, evaluated, tracked, reported and mitigated appropriately, Regulated Entities shall implement a cybersecurity risk management process.

Cybersecurity Risk Assessment Methodology:

4.4.1 The cybersecurity risk assessment methodology shall be defined, approved, implemented and reviewed annually.

4.4.2 The Regulated Entities shall ensure that:

a) risk assessment methodology is based on international best practices, frameworks and standards such as ISO 31000, ISO 27001, NIST 800-39 and ISF Standard of Good Practice;
b) scope, periodicity and execution responsibility for risk assessments are defined;
c) risk tolerance levels are specified and determined based on the organizational priorities and objectives; and
d) processes and templates for risk identification, assessment, response, and overall monitoring and reporting are specified.

Cybersecurity Risk Identification and Assessment:

4.4.3 The risk identification exercise shall consider both internal and external threats and vulnerabilities, as well as the risks impacting the basic principles set out in the Baselines.

4.4.4 The regulated entity shall take into account of the following during risk assessment:

a) regulatory and legal requirements as applicable;
b) technology assets;
c) connections with external networks;
d) customer delivery channels; and
e) application interfaces.

4.4.5 The identified cybersecurity risks shall be documented in a risk register.

4.4.6 Risks shall be evaluated on the basis of severity, impact to business and operations, and likelihood of their occurrence.

4.4.7 The risk assessment outcomes shall be discussed and agreed with the respective Business and Technology risk owners.

4.4.8 The risk assessment shall be conducted annually, or whenever:

a) new products and technologies are introduced;
b) there is a significant change in technology, business or operations-related processes;
c) new material risks are detected by the Regulated Entity; and
d) new third party agreements are signed.

Cybersecurity Risk Response:

4.4.9 Regulated Entities shall ensure that risks documented in the risk register translate into risk response plans.

4.4.10 Risk response shall be categorized (e.g., risk acceptance, risk avoidance, risk mitigation, transfer, etc.), tracked and managed. In case of risk acceptance, avoidance, or transfer, appropriate basis for categorization shall be documented and approved.

4.4.11 A risk monitoring process shall be implemented to track compliance and ensure effectiveness of risk mitigation controls. Further, the Board shall be updated regularly about current status of identified risks and response plans.

4.5 Compliance

Objective: To ensure compliance to national and international laws, regulatory requirements and policies provided by leading service providers (collectively referred hereinafter as compliance requirements), Regulated Entities shall implement necessary cybersecurity measures.

4.5.1 Regulated Entities shall identify, document and demonstrate compliance to applicable legal, regulatory and compliance requirements, such as:

a) CBK Law 32;
b) Law 20/2014, E-Transaction Law;
c) CCTV Law No 61/2015;
d) E-Crime Law No 60/2015;
e) Instructions for Regulation of the Electronic payment of funds;
f) Cybersecurity Baselines for Kuwaiti Banking Sector; and
g) Other requirements, instructions, regulations issued by CBK.

4.5.2 Regulated Entities shall comply with latest version of the applicable best practices and standards such as:

a) Payment Cards Industry Data Security Standard (PCI-DSS);
b) Payment Application Data Security Standard (PA-DSS);
c) EMV (Europay, MasterCard, and VISA) technical standard;
d) SWIFT Customer Security Controls Framework; and
e) International Organization of Standardization (ISO 27001, ISO 22301, ISO 31000).

4.5.3 Regulated Entities shall ensure that any changes to applicable compliance requirements are identified, assessed, implemented and appropriately incorporated in a compliance register.

4.6 Independent Audit

Objective: To ensure the adequacy and effectiveness of implemented cybersecurity controls, Regulated Entities shall conduct independent audit.

Audit Function of Regulated Entity:

4.6.1 The audit function shall ensure that independent audits are conducted to evaluate implementation of the Information Security Management System.

Audit Planning and Execution:

4.6.2 An audit charter based on generally accepted auditing standards and the cybersecurity framework shall be defined, approved, implemented and reviewed annually. The audit charter shall specify the purpose, mandate, responsibility, and accountability of management with respect to the audit.

4.6.3 An audit plan shall be defined and approved by the Board or Senior Management.

4.6.4 Regulated Entities shall ensure that:

a) high risk areas are audited at least annually; and
b) medium and low risk areas may be audited once in two years.

Independent Third party Audits:

4.6.5 The cybersecurity audits shall be performed by independent competent third party approved by CBK.

4.6.6 The third-parties entrusted to perform independent audits shall be changed at least once every two years.

Independent Audit Reporting:

4.6.7 The Board shall be provided with periodic feedback regarding the comprehensiveness and effectiveness of the cybersecurity policy and its implementation.

4.6.8 Regulated Entities shall track and monitor independent audit findings and publish an assessment and compliance dashboard to the Board on a quarterly basis.

5 Technology and Operations

Overview: Regulated Entities depend on technology to operate and deliver services to end customers and internal users. To ensure the security and reliability of technology assets, Regulated Entities shall implement appropriate security controls within their technology assets. The following Sub-Domains specify the necessary controls to address the risks related to technology and operations.

5.1 Security Architecture Design

Objective: To ensure consistent implementation of cybersecurity principles, Regulated Entities shall establish a security architecture in line with the overall strategic objectives of the organization.

5.1.1 A security architecture shall be defined, approved, implemented, monitored, periodically reviewed and updated. The reviews and updates shall be based on business–requirements, inputs from IT and information security functions and shall be approved by relevant stakeholders.

5.1.2 The security architecture shall protect the confidentiality, integrity and availability of Regulated Entities information and be designed to avoid disruption to service, minimize attack surface, reduce the impact on entity and detect the adversaries easily.

5.1.3 The security architecture shall be based on 'secure-by-design' principles and consider:

a) segregation of networks (e.g., trusted, untrusted, wired, wireless, production, test, payment systems, general IT systems, web, app, DB, administration etc.,) based on criticality, access and integration requirements;
b) protection of sensitive data at rest, in use and in transit from unauthorized disclosure, alteration, malicious attacks;
c) principles of multi-layer security, least privilege and segregation of duties;
d) logging, monitoring, reporting requirements;
e) preventing internet access from users, systems and devices unless there is valid need to allow;
f) business continuity and disaster recovery arrangements; and
g) specific security considerations which are relevant and important to meet business objectives.

5.2 Asset Management and Classification

Objective: To ensure information assets of the organization are classified and securely managed, Regulated Entities shall implement an asset management and classification process.

5.2.1 Asset management and classification process shall be defined, approved, implemented, monitored, periodically reviewed and updated to secure assets throughout their lifecycle.

5.2.2 The process shall define the roles of Asset Owner, Custodian and intended users. It shall include controls for identification, protection and monitoring of information assets.

5.2.3 A policy for acceptable use of information assets shall be defined, approved, implemented and periodically reviewed.

5.2.4 All information assets shall be identified and an inventory shall be maintained in an asset register. At a minimum, the asset register shall contain asset name, description, owner, custodian, and classification. End-of-life/end-of-support information shall be considered where applicable.

5.2.5 Regulated Entities shall identify business functions, supporting information assets, and processes and conduct risk assessment to understand their value and importance to organization.

5.2.6 Information Assets shall be classified using a risk-based approach in accordance with their value, importance, criticality, and legal requirements. Information asset labeling and handling guidelines shall be defined accordingly.

5.2.7 All critical information assets shall be labelled as per the labeling guidelines.

5.2.8 The acquisition of information assets shall be consistent with the regulated entity's procurement process, licensing agreements and shall comply with the security architecture.

5.2.9 Information assets shall be disposed when no longer required, in accordance with relevant regulations, industry requirements, contractual agreements and policies of the Regulated Entities.

5.2.10 The procedures for the sanitization and destruction of information assets shall be defined, approved, implemented and regularly reviewed. This shall be in line with information classification requirements.

5.2.11 Disposal of sensitive information residing on information assets shall be executed by appropriate techniques that render the information to be non-retrievable (e.g. secure erase, secure wiping, double crosscut, shredding, etc.).

5.2.12 Process shall be defined and implemented to detect and prevent the use of unauthorized or rogue assets.

5.3 Infrastructure Security

Objective: To ensure that technology components are securely installed and configured, Regulated Entities shall implement appropriate infrastructure security controls.

Security configuration standards:

5.3.1 Security configuration standards shall be defined, approved, implemented, monitored and periodically reviewed and updated to cover technology assets used within the enterprise .

5.3.2 Security configuration standards shall be based on global best practices (such as NIST, Center for Internet Security (CIS) benchmarks), Guidelines issued by Original Equipment Manufacturers (OEMs), and internal policies and best practices of the Regulated Entity.

5.3.3 Security configuration standards shall, at a minimum, include the following:

a) installing only approved and supported version of software;
b) installing minimum components or services necessary to meet the requirements;
c) applying up-to-date security updates;
d) protecting data in line with asset management and information classification requirements;
e) disabling or restricting access to weak or unnecessary services and ports;
f) changing default passwords, removing or disabling unneeded accounts;
g) configuring access control based on need-to-know and need-to-have principles;
h) removing local administrator privileges from end-users devices;

i) disabling weak or insecure protocols and algorithms and ensuring that only latest and industry supported algorithms are used;

j) setting security measures to lock or terminate (logout or logoff or close the application page) sessions after meeting a predefined period of inactivity and conditions ;

k) measures to protect against malicious software, malware, ransomware, data loss, denial of services, advanced threats etc.;

l) synchronizing system clocks with central-clock; and

m) enabling logging and monitoring.

5.3.4 Compliance against security configuration standards shall be monitored periodically.

5.3.5 New technology deployments shall be configured as per configuration standards and testing shall be performed prior to go live to confirm the compliance.

Network security:

5.3.6 The network architecture shall be documented, approved, implemented, periodically reviewed and updated whenever there are changes to the architecture.

5.3.7 Networks shall be protected through appropriate configuration and implementation of security solutions (e.g. router, firewall, intrusion prevention system, intrusion detection systems, proxy, advanced persistent threat protections, email/internet filtering, virtual private network etc.) to protect against and detect cyber threats.

5.3.8 The network shall be segregated into production, testing and development zones with established network security policy for each zone based on its criticality and purpose.

5.3.9 All external connections to enterprise internal network shall be authenticated and encrypted.

5.3.10 Logging of network devices shall be enabled to capture changes made to network configurations.

5.3.11 All wireless access points / base stations that are connected to the enterprise network shall be registered, approved and securely configured.

5.3.12 Network shall be monitored to detect unauthorized /rogue devices connected to the network. All such unauthorized devices identified shall be deactivated.

Security Patch management:

5.3.13 Security patch management process shall be defined, approved, implemented and periodically reviewed. Effectiveness of the process shall be measured.

5.3.14 Regulated Entities shall define schedule (e.g. monthly, quarterly, etc.,) for deployment of patches based on the criticality and importance of the asset and the threats posed by the vulnerability.

Network Connections and Application Interfaces:

5.3.15 Security standards for network connections and application interfaces shall be defined, approved, implemented, periodically reviewed and updated.

5.3.16 Network connections, application interfaces and data flows shall be documented and maintained for internal and external connections to the enterprise network whether on premises or on cloud.

5.3.17 The security configuration standards shall include requirements related to network encryption, authentication, session management, session time-outs, access governance, data security, etc.

5.3.18 The network connections and application interfaces shall be tested in accordance with security configuration standards periodically.

5.4 Secure Software Lifecycle Management

Objective: To ensure that cybersecurity controls are designed, implemented and managed throughout application development lifecycle or while acquiring new applications, Regulated Entities shall establish secure software lifecycle management process.

5.4.1 Secure Software Lifecycle management process shall be defined, approved, implemented, monitored, periodically reviewed and updated.

5.4.2 Security and privacy design principles and classification requirements shall be taken into consideration while designing new application or outlined in the agreement with the entity supplying commercial off the shelf application. All enhancements to the in-house applications or commercial off the shelf applications shall follow the same process.

5.4.3 The information security team shall be involved to ensure that security requirements are addressed during all phases of software lifecycle management (design, development, testing, implementation, maintenance, disposal etc.).

5.4.4 Secure coding practices shall be adopted as per organizational requirements and global best practices (e.g. Open Web Application Security Project (OWASP) Secure Coding Practices) to ensure common coding vulnerabilities are addressed during development and appropriate protective, detective, corrective and recovery control measures are implemented.

5.4.5 Segregation of duties shall be implemented by restricting access to production, test and development environments.

5.4.6 Access to the program source code shall be restricted and logged.

5.4.7 For critical applications, access to source code shall be managed by:

a) storing the code on premises; or
b) through an escrow arrangement; or
c) strict contractual terms with application/service provider.

5.4.8 Security assessment certificate or equivalent evidence shall be obtained for commercial off the shelf products to ensure that the applications are tested and identified vulnerabilities are remediated.

5.4.9 Application and/or systems shall display generic error messages by considering at a minimum below principles:

a) use custom error pages;
b) authentication failure responses do not indicate which part of the authentication data was Incorrect; and
c) do not disclose or display sensitive information in error responses, including system details, session identifiers or account information, etc.

5.5 Security Considerations for Emerging Technologies

Objective: To ensure secure and reliable incorporation and use of emerging technologies, Regulated Entities shall implement relevant security policy and controls during emerging technology adoption.

5.5.1 A policy for adopting new emerging technologies shall be defined, approved, implemented and reviewed periodically.

5.5.2 Regulated Entities shall seek approval from CBK when adopting new and emerging technologies.

5.5.3 Regulated Entities shall conduct risk assessment for adopting new technologies, identify controls required to secure the new and emerging technologies and mitigate the identified risks as per the entity's risk management process.

5.5.4 Regulated Entities shall ensure that sufficient tests are carried to ensure that new technology meets the requirements and address the identified risks.

5.5.5 Regulated Entities shall inform their customers about the risks involved in using the emerging technologies and provide customers the choice to use such technology.

5.6 Access Control Management

Objective: To facilitate required and sufficient access to systems, services, physical premises, information and information processing facilities, Regulated Entities shall implement appropriate security measures within their access management program.

Identity and access management:

5.6.1 Access management policy shall be defined, approved, implemented and reviewed periodically. The policy shall be based on business and information security requirements and shall leverage the basic cybersecurity principles defined in this Cybersecurity Baseline document.

5.6.2 Access management policy shall, at a minimum, include the following:

a) user registration, modification and revocation for regular and privileged access;
b) logging and monitoring of access management activities;

c) access review; and
d) safe and secure use of credentials.

5.6.3 An authorization process shall be established and a record of all privileges allocated shall be maintained.

5.6.4 Privileges shall be granted to users on need-to-know and need–to-do basis in line with the access management policy, and after the authorization process is complete.

5.6.5 Segregation of duty controls shall be integrated into the user registration, modification and revocation process.

5.6.6 Unique IDs shall be assigned to each user and system.

5.6.7 Generic or Group IDs shall be permitted based on a review and validation of business / operational reasons and prior approval shall be necessary for creation and usage of such IDs.

5.6.8 Authentication information of users shall be stored and transmitted in a secure manner.

5.6.9 Concurrent logins shall be monitored and prevented for critical systems and applications.

5.6.10 Appropriate audit records of all access management activities and user access shall be logged and monitored.

5.6.11 Regulated Entities shall conduct access control review at least annually. All redundant access rights shall be identified and disabled/deleted.

5.6.12 Users must activate a password protected screensaver or logoff the application when leaving workstation unattended.

Remote access management:

5.6.13 All remote access granted to users shall be subject to validation of business / operational reasons and shall be approved by relevant stakeholders after due risk assessment.

5.6.14 Multi-factor authentication shall be implemented for all remote access users.

5.6.15 Remote access shall be permitted only from a list of approved devices or IPs and shall be associated with specified user.

5.6.16 All access and activities performed using remote access shall be logged and monitored.

5.6.17 Direct remote access to internal production systems shall not be permitted.

Password management:

5.6.18 A comprehensive password management policy shall be documented, approved, implemented and reviewed periodically.

5.6.19 The password policy shall include complexity requirements such as password history, account lockout, maximum password age, minimum password length and include secure log-on procedures.

5.6.20 Passwords shall:

a) be at least eight or more characters in length; and
b) include letters, numbers and special characters.

5.6.21 All systems default, vendor supplied and publicly documented accounts passwords (including service accounts) shall be changed.

5.6.22 Passwords shall be communicated in a secure manner to ensure access by the intended user.

5.6.23 The use of multi-factor authentication (such as one-time password or token-assisted authentication) shall be required for users having privileged or administrative or elevated access to system resources.

5.7 Cryptography

Objective: To protect from unintentional information disclosures, Regulated Entities shall implement appropriate information protection measures using cryptographic techniques.

5.7.1 A cryptographic policy shall be documented, approved, implemented, periodically reviewed and updated. The policy shall include organization specific principles and acceptable use of cryptographic controls and consider industry best practices.

5.7.2 Procedures shall be established to protect the cryptography technology setup. The procedures shall consider:

a) selection of cryptographic control (e.g. strength, length, method) requirements in accordance with data privacy and protection policy requirements and industry best practices;
b) cryptographic key management such as generation, distribution, storage, archival, retrieval, usage, backup, recovery, disposal etc.; and
c) usage of combination keys / split knowledge / dual control requirement for login into the key store.

5.7.3 The key length used for encryption shall be as per the latest globally acceptable industry best practices.

5.7.4 Regulated Entities shall use appropriate encryption techniques to secure sensitive data within system logs, databases, networks, applications and other information assets as applicable. These techniques shall be applied consistently across on-premise and cloud installations.

5.8 Change and Release Management

Objective: To ensure existence and effectiveness of necessary security requirements within changes, Regulated Entities shall incorporate security considerations within change and release management process.

5.8.1 A change and release management process shall be defined, approved, implemented, monitored, periodically reviewed and updated.

5.8.2 The change and release management process shall ensure appropriate consideration of defined security controls in complete cycle of change, configuration and release management.

5.8.3 Regulated Entities shall classify the changes based on priority, complexity and nature of change and ensure that risks are identified, assessed and addressed.

5.8.4 Appropriate documentation, testing and approvals shall be in place before change is implemented in production.

5.8.5 All changes shall be reviewed and approved to ensure consistent adherence to applicable policies and procedures.

5.8.6 Testing shall be planned, executed and documented to validate expected outcome. Testing shall consider the following:

a) user acceptance testing (to validate functionality);
b) stress testing, exception handling, and integrity of application interfaces;
c) security testing for user management, application and infrastructure security, source code reviews, penetration testing and vulnerability assessment; and
d) audit trails.

5.8.7 Appropriate fallback procedures shall be in place in case of recovering from unsuccessful changes and unforeseen events.

5.8.8 Regulated Entities shall seek approval from CBK for changes which have a major impact on the Regulated Entity core business services and/or affecting customers.

5.9 Capacity Management

Objective: To ensure availability and adequate performance of technology components, Regulated Entities shall implement system monitoring and capacity management process.

5.9.1 A capacity management process shall be documented, approved, implemented and reviewed at periodic intervals.

5.9.2 Regulated Entities shall define appropriate thresholds for capacity monitoring and consider current utilization, future requirements, current system performance, service unavailability etc. and implement measures to address them.

5.10 Data Privacy and Security

Objective: To ensure protection from information breaches and to create trust by responsible use of data, Regulated Entities shall establish appropriate data protection and privacy measures.

Data Security:

5.10.1 A Data Protection policy and supporting procedure/s for, identification and protection of important records shall be documented, approved, implemented and reviewed periodically.

5.10.2 The policy and procedure/s shall include specifications for processing, storage, retention and disposal of important records in accordance with:

a) regulatory and legal requirements; and
b) local and cross-border business requirements.

5.10.3 Security controls shall be implemented to protect confidentiality, integrity and availability of sensitive data and important records while at rest and in transit.

5.10.4 Encryption techniques used to protect important records shall be in accordance with the cryptography policy of the Regulated Entity.

5.10.5 Data security and privacy considerations/ measures shall be considered and implemented for protecting data shared with supply-chain vendors.

5.10.6 Data privacy and protection requirements shall be communicated to and adhered by third party vendors, and specified within the outsourcing agreement.

Data Privacy:

5.10.7 A data privacy policy shall be documented, approved, implemented and reviewed periodically as per compliance requirements.

5.10.8 The following privacy principles shall be included in the policy:

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes shall not be considered to be incompatible with the initial purposes (purpose limitation);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization);

d) accurate and, where necessary, kept up to date; steps shall be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy);

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes to safeguard the rights and freedoms of the data subject (storage limitation);

f) collected by obtaining consent from the data subject for the purpose specified. Such consent shall be clear, explicit, unambiguous and involve a clear affirmative action and should be separate from other terms and conditions and should not generally be a precondition of signing up to a service (consent); and

g) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

5.10.9 Data subject should have the right to have personal data erased when no longer processed, no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn consent, personal data does not comply with legal and regulatory requirements (right to be forgotten).

5.10.10 Entity shall communicate to the data subject in case of a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk in order for data subject to take necessary precautions.

5.10.11 A privacy impact assessment shall be conducted on periodic basis or whenever significant changes occurs the environment to identify potential sensitive information at risk and ascertain that appropriate technical measures are in place to protect such information.

5.10.12 Data protection requirements shall be communicated to and adhered by third party vendors, and specified within the outsourcing agreement.

5.11 Email Security

Objective: To ensure a secured and trusted electronic communication channel, Regulated Entities shall adopt appropriate security measures to protect emails.

5.11.1 Email usage guidelines shall be documented, approved, implemented and periodically reviewed. The guidelines shall include:

a) granting email access in accordance with access management policy and procedure;
b) safe practices for sending/receiving emails;
c) acceptable use of emails and email system;
d) handling attachments, links within email, spam email etc.;
e) protection, detection and monitoring of content circulated in emails; and
f) email data retention in accordance with data protection and privacy policy and procedures.

5.11.2 Controls to protect and secure email and messaging systems from security risks (such as spam, malicious links / attachments, email phishing) shall be implemented.

5.11.3 Employee and third-party vendor staff shall use email communication in adherence to data privacy and data security requirements of the regulated entity.

5.11.4 Appropriate security measures (such as digital signatures and encryption) shall be implemented to protect the confidentiality of information being communicated through emails.

5.12 Portable Device Security

Objective: To ensure that risks arising from usage of unauthorized or unprotected portable computing devices are mitigated, Regulated Entities shall adopt necessary Portable Device security measures.

5.12.1 A policy for portable device security shall be defined, approved, implemented, monitored and reviewed periodically and updated.

5.12.2 Portable devices shall be permitted to connect to the enterprise network after necessary authorization.

5.12.3 Regulated Entities portable device policy shall include acceptable use policy.

5.12.4 Security configuration standards shall be implemented on the portable device prior to allotting them to users and / or allowing them to connect to the network.

5.12.5 The portable device shall be tagged to a unique employee or third-party vendor staff.

5.12.6 All portable devices that are connected to the enterprise network shall be monitored.

5.12.7 For devices owned by the regulated entity, the portable computing devices of terminated employees or end of service of the third-party vendor staff shall be returned, and the data residing on these devices shall be securely erased or backed up as necessary.

5.12.8 For devices owned by the employee, the data of the regulated entity residing on the portable computing device shall be securely backed up and stored as necessary when no more required (e.g. no requirement to store data on employee device or termination of employment).

5.12.9 When devices are provisioned or re-provisioned to new users, the security configuration standards shall be re-installed before handover to the users.

5.12.10 Regulated Entities shall secure important records stored on portable devices by ensuring that:

a) installed applications are pre-approved by the regulated entity;
b) only authorized software are installed; and
c) end-point encryption or containerization.

5.12.11 Regulated Entities shall set a maximum number of devices to be connected to entities network by employees.

5.13 Reputation Protection

Objective: To ensure that the Regulated Entities are protected against misuse of reputation in cyberspace, Regulated Entities shall adopt reputation protection initiatives.

5.13.1 A policy for protecting the online presence of the enterprise shall be defined, approved, implemented and reviewed periodically.

5.13.2 The policy shall include at a minimum, controls to monitor misuse of the brand, related products and identity of key influential personnel of the regulated entity. The policy shall also contain appropriate measures to escalate and remediate identified brand abuse.

5.13.3 Regulated Entities shall establish measures to identify and address incidents of brand abuse and misrepresentation in the cyberspace to protect its online presence.

5.13.4 Content for public facing systems shall be reviewed by internal team before being published.

5.13.5 Training shall be provided to relevant employees to assist them in understanding reputation-related cyber risks and safe usage of social media.

5.14 Logging, Monitoring and Security Incident Management

Objective: To ensure that events generated from various technology assets are continuously collected, monitored, analyzed, and tracked for early detection, and remediation, Regulated Entities shall implement appropriate security information and event management program.

Logging:

5.14.1 A policy for logging and monitoring shall be defined, approved, implemented and reviewed periodically. The policy shall include requirements of log content, protection, retention, archival and destruction.

5.14.2 Logs shall be enabled on all critical technology assets on premises and / or in cloud.

5.14.3 The level of logging should be based on the classification of the information and risk assessment. At a minimum, the logs should contain the following information:

a) user ID (who);
b) date, time (when);
c) source of activity such as location, IP address, service etc. (from where);
d) details of event such as log-on, log-off (what);
e) details of successful and unsuccessful system access attempts;
f) details of successful and unsuccessful resource access attempts; and
g) details of successful and unsuccessful configuration / settings change access attempts.

5.14.4 Relevant log sources and logs received shall be monitored.

Incident detection and analysis:

5.14.5 A security information and event management process to identify, track, and monitor events, issues, and incidents shall be documented, approved, implemented and reviewed periodically. The process shall include criteria for:

a) classification of an event or series of events as incident;
b) assigning ownership;
c) assessing whether they constitute security breach;
d) assessing the criticality of the incident; and
e) sharing of incident information and associated threat intelligence.

5.14.6 Indicators of compromise shall be identified using detection techniques and rapidly reported for investigation.

5.14.7 Incidents shall be validated by correlating evidence obtained through different sources and logs (e.g., firewall logs and source IP addresses, application logs and usernames).

Incident response:

5.14.8 An Incident Response Team (IRT) or equivalent group shall be formed by Regulated Entities to respond to security incidents. The IRT shall be available to respond to information security incidents or events.

5.14.9 A security incident containment method shall be prepared and made readily accessible to limit/ mitigate security risks.

5.14.10 A summary of incidents shall be reported to Board and Senior Management on a periodic basis.

5.14.11 Reported security incidents shall be tracked, recorded and remediated. Remediation strategy shall be implemented in a manner that is consistent with the nature and character of the incident.

Forensics:

5.14.12 Procedures for performing forensic tasks shall be established and maintained. The procedures shall mandate the appropriate use of forensic tools to collect, retain and archive evidences.

5.15 Vulnerability Management

Objective: To ensure identification, prioritization and treatment of technical vulnerabilities, Regulated Entities shall implement vulnerability management process.

5.15.1 A vulnerability management process shall be defined, approved, implemented, monitored, measured, periodically reviewed and updated. The process shall include vulnerability discovery, prioritization and treatment.

5.15.2 Vulnerability assessments (e.g. missing security updates, missing baseline configuration, application security testing, penetration testing and code reviews) of network, systems and applications shall be conducted on periodic basis or whenever significant changes occur to the environment, to identify the existence of vulnerabilities and classify them based on their impact.

5.15.3 Regulated Entities shall receive notifications from trusted information sources about latest vulnerabilities and follow risk-based approach for prioritizing and treating the vulnerabilities identified and notifications received from information sources in line with risk management process.

5.15.4 Regulated Entities shall conduct validation after remediating the vulnerabilities to assess whether gaps addressed are in line with risk decisions.

5.15.5 The findings of vulnerability assessments shall be reported, logged for initiating remediation activities and tracked till closure.

5.15.6 The information security function shall update the Board and Senior Management on periodic basis about the effectiveness of vulnerability management process.

5.16 Human Resource Security

Objective: To protect against inappropriate acts of employees or third-party vendor staff, Regulated Entities shall integrate security considerations within their human resource policies and procedures.

Regulated Entities shall:

5.16.1 Perform sufficient background screenings in line with relevant laws, regulations and organizational requirements prior to onboarding/hiring employees.

5.16.2 Ensure that appropriate confidentiality or non-disclosure agreements are signed by the employees and third party vendors where applicable.

5.16.3 Ensure that all employees and third-party vendors formally acknowledge their commitment to adhere to information security policies, procedures and guidelines.

5.16.4 Ensure a formal disciplinary process is defined, documented, and implemented to cover violations of code of conduct and/or internal policies and standards.

5.16.5 Ensure that upon termination, all technology assets allocated to employees and third-party vendors are returned and access privileges are revoked.

5.17 Security Awareness and Training

Objective: To ensure that a cyber-aware culture is embedded in the organization and adequate skillset is available, Regulated Entities shall undertake appropriate security awareness and training program.

5.17.1 A security awareness and training program shall be established for all employees and relevant third-party vendor staff.

5.17.2 The security awareness and training program shall be conducted on a regular basis and shall ensure role based dissemination of awareness and training.

5.17.3 The security awareness program shall include information security policies, information security roles and responsibilities, relevant procedures, latest cybersecurity trends etc.

5.17.4 Regulated Entities shall conduct customer security awareness with respect to cybersecurity threats, risks and practices for safe and secure use of financial service through effective communication channels.

5.17.5 Customers shall be encouraged to report phishing mails or phishing sites or unusual behavior observed through appropriate channels identified by the regulated entity.

5.17.6 Regulated Entities shall monitor the effectiveness of the security awareness and training program.

5.17.7 Regulated Entities shall retain relevant documented information as evidence of conducting security awareness and training programs.

5.18 Physical and Environmental Security

Objective: To secure the locations and premises from unauthorized physical access, security breaches and natural / environmental hazards, Regulated Entities shall adopt appropriate physical and environmental security measures.

5.18.1 Physical and environmental security policy shall be documented, approved, implemented reviewed periodically and updated.

5.18.2 Physical security perimeters or zones shall be identified, protected by appropriate physical and logical security controls and monitored in line with the Physical and environmental security policy.

5.18.3 An approved list of individuals with authorized physical access to a restricted areas shall be maintained and periodically reviewed.

5.18.4 All access points shall be controlled to prevent unauthorized entry to restricted/ secure areas (such as core data center where servers and network equipment

are located). Additionally, Regulated Entities shall consider isolating loading, storage or delivery areas from secure areas.

5.18.5 Regulated Entities shall comply with health and safety guidelines for facilities.

5.18.6 Security measures and policies shall be consistently applied to on-site and off-site equipment.

5.18.7 Access to restricted/secured areas shall be monitored using Closed Circuit television (CCTV) in accordance to CCTV Law No 61-2015.

5.18.8 Environmental considerations shall be incorporated into the design and construction of facilities. All IT enabled environmental solutions (e.g. HVAC Systems, Building Management Solutions etc.) need to adhere to applicable controls to the Cybersecurity baselines.

5.18.9 Restricted/secure areas shall have measures (e.g. temperature and humidity controls, fire extinguishers, smoke detectors, sprinklers, water leakage detection mechanisms, etc.) to detect and protect against environmental hazards.

5.18.10 Restricted/secure areas shall have functional power backup systems to address partial or complete electrical failure.

5.18.11 The implemented physical and environmental controls shall be appropriately and periodically tested. Preventive maintenance shall be conducted to ensure performance as per intended purpose and specifications.

5.18.12 Evacuation plans shall be established and communicated to all employees and third party vendors, and periodic evacuation drills shall be conducted. The logs of evacuation drills shall be maintained and necessary corrective and improvements initiatives shall be undertaken.

5.19 Business Continuity and Disaster Recovery (BC and DR)

Objective: To ensure system and data availability during disaster scenarios, Regulated Entities shall adopt appropriate Business continuity and Disaster Recovery program.

5.19.1 Business continuity and disaster recovery (BCP/DR) processes and plans shall be documented, approved, implemented and reviewed periodically. The plans shall be established for individual business units and integrated for the overall entity.

5.19.2 Regulated Entities shall define the Recovery Time Objectives (RTO) and Recovery Point objectives (RPO) for critical systems and functions.

5.19.3 An alternate recovery site shall be identified for restoration of critical systems and business operations. The site shall be located in a separate location other than the primary site. Required work recovery procedures, manuals and list of names and phone numbers of the external service providers and its relevant staff shall be placed at the recovery site.

5.19.4 Recovery strategies shall be defined to include:

a) activities to be performed during various crisis scenarios;
b) roles and responsibilities; and
c) communication channels for updating concerned stakeholders on an ongoing basis.

5.19.5 A backup strategy shall be defined, approved, implemented and reviewed periodically. The strategy shall include:

a) backup periodicity;
b) storage and disposal mechanisms; and
c) security measures to protect information and media.

5.19.6 Information shall be backed up, retained, and stored in accordance with the backup strategy. Periodic restoration tests shall be conducted on the backed-up information.

5.19.7 Regulated Entities shall conduct annual business continuity and disaster recovery exercises /tests. All major systems, core activities and system support and business users shall be part of these tests. Test results and deviations, if any, shall be documented and signed off by Senior Management.

5.19.8 Tabletop exercises shall be conducted at regular intervals to test scenario readiness and action plans.

5.19.9 Regulated Entities shall ensure that issues identified during business continuity and disaster recovery tests are addressed.

5.19.10 The alternate recovery site shall have physical security and access controls in accordance with Regulated Entity Risk Management process.

5.20 Cyber Crisis Management

Objective: To ensure consistent interpretation, preparation, responses, and recovery from crisis lifecycle, Regulated Entities shall adopt appropriate crisis management program.

5.20.1 Regulated Entities shall maintain updated crisis management plans that support their enterprise resilience beyond cyber crisis management planning. These plans shall be:

a) approved by the Board or senior management;
b) implemented enterprise-wide to ensure coverage of key organizational functions, authorities, and responsibilities;
c) aligned with legal, regulatory, and organizational requirements;
d) aligned with operational risk management considerations (e.g., disaster recovery, business continuity, and communications [internal/external] policies, plans, procedures, and templates).

5.20.2 Regulated Entities shall define a Crisis Management Team that integrates the technical, business, and management functions of regulated entity.

5.20.3 Crisis Management Team shall be led by the Crisis Response Lead and comprise of empowered representatives specifically from Operations, Information Technology / Information Security, Legal, and Communications. The team shall:

a) develop, maintain, promote, and exercise crisis management planning;
b) assist the Crisis Response Lead to assess whether an incident with crisis level impact exists and whether a formal response is required;
c) mobilize and deploy necessary internal and external resources to deliver the response;
d) oversee execution of response activities; and
e) manage the communication with internal and external stakeholders throughout a crisis management life-cycle.

5.20.4 Regulated Entities shall ensure that the Crisis Response Lead shall have:

a) skills and experience to understand the Regulated Entity's operations and to make decisions;
b) completed relevant training (e.g., has relevant qualifications, etc.) on emerging cyber crisis related trends; and
c) authority and responsibility to take decisions independently during crisis response.

5.20.5 A cyber crisis management process shall be documented, approved, tested and periodically updated. The process shall:

a) address operational risk management considerations (e.g., disaster recovery, business continuity, and communications (internal/external) policies, plans, procedures, and templates); and
b) cover the entire enterprise to ensure coverage of key organizational functions, authorities, and responsibilities

5.20.6 Regulated Entities shall define a severity impact matrix that is approved by their Board or Senior Management. The severity impact matrix shall:

a) consider the outcomes of entity specific business impact analyses, internal assessments, and risk analyses;
b) tier the impact to the Regulated Entities (e.g., low, medium, high; minor, moderate, severe; etc.) across their categories of significant consideration in alignment with the sectoral severity impact matrix defined in the CMSP, and entity specific risk appetite; and
c) specify the appropriate mitigating actions for each impact tiers.

5.20.7 Regulated Entities shall implement and maintain appropriate tools and threat intelligence feeds from internal systems and third party providers to assist the Regulated Entities to initiate enterprise-wide risk response efforts whenever necessary.

5.20.8 Regulated Entities shall implement emergency notification mechanisms to support timely contact with responders and employees in the event of an incident with crisis level impact.

5.20.9 Regulated Entities shall implement crisis management response tools (e.g., a decision and action logging capability) to create an auditable trail of response considerations and assist in improvements based on lessons learned.

5.20.10 Regulated Entities shall adopt a continuous learning model to promote improved future readiness for cyber incidents.

5.20.11 Regulated Entities shall provide:

a) regular training appropriate to crisis responders' roles in crisis response; and
b) ad-hoc training if there is any change to the Regulated Entity's response process.

5.20.12 Regulated Entities shall conduct cyber crisis exercises on an annual basis to ensure relevance and effectiveness of cyber crisis management plans, procedures, and response infrastructure.

5.20.13 Regulated Entities shall participate in CBK-organized sector-wide crisis exercises focused on cyber and other relevant scenarios.

5.20.14 Regulated Entities shall report incidents in accordance to the below timelines:

a) Low severity incidents shall be reported on monthly basis;
b) Medium severity incidents shall be reported within 8 business hours of discovery; and
c) High severity incidents shall be reported within 4 hours of discovery.

5.20.15 Regulated Entities shall update the situation/progress on reported incidents in accordance to the below timelines:

a) Medium severity incidents shall be updated in every 2 business days from prior notification; and
b) High severity incidents shall be updated on daily basis.

5.20.16 Regulated Entities shall report incidents in accordance to the predefined templates and communication channels.

5.20.17 Regulated Entities shall participate and collaborate for sectoral crisis responses based on assessed severity and action/s initiated by CBK.

5.21 Cyber Threat Intelligence Management

Objective: To ensure that necessary safeguards are proactively implemented to protect against emerging cyber-threats that are planning to target an organization or industry in general, Regulated Entities shall adopt a cyber-threat intelligence management program.

5.21.1 A process for identification and management of cyber threats shall be documented, approved, implemented and reviewed periodically. This shall be in line with Cyber Threat Information Sharing Strategy.

5.21.2 Intelligence published by identified internal and external sources shall be collected and processed consistently.

5.21.3 Cyber threats and insights shall be communicated to management on as-needed basis.

5.21.4 Regulated Entities shall identify applicable threats and undertake necessary actions to protect their technology assets as per the incident management process. All such actions shall be tracked.

5.21.5 Regulated Entities shall review and improve their threat intelligence management capabilities on an ongoing basis.

5.21.6 Regulated Entities shall engage continually with CBK to:

a) consume threat intelligence provided by CBK;
b) share the identified threat intelligence (internal and external) to the banking sector community and management; and
c) proactively participate in sectoral collaboration for remediation of threats.

6 Third Party Security

Overview: Regulated Entities depend on multiple third party vendors to operate or execute their business functions. Innovation and efficiency are key drivers for such continued and increasing reliance on third party vendors. Further, entities increasingly engage with third party vendors for expertise, ease of operations, and access to new technologies to improve the overall delivery of financial services to their customers. The following section specifies the necessary controls to secure third party arrangements.

6.1 Third Party Outsourcing

Objective: To ensure risks arising from outsourcing to third party vendors are adequately assessed, governed, regulated and tracked, Regulated Entities shall establish robust risk management process and mandate inclusion of relevant security controls as part of outsourcing agreements.

6.1.1 An Outsourcing policy shall be defined, approved, communicated and implemented. The policy shall be reviewed by Risk Management, Information Security, and Audit functions of Regulated Entities.

6.1.2 Regulated Entities shall seek approval from CBK before engaging in any significant Information Technology (IT) related outsourcing agreements.

6.1.3 Regulated Entities shall identify and include the minimum cybersecurity requirements within all significant IT related outsourcing agreements.

6.1.4 Proper due diligence shall be conducted during the third party vendor selection process and shall cover the following:

a) experience and capability of the third party vendor;
b) financial strength of the third party vendor;
c) internal control environment of the third party vendor;
d) cybersecurity practices of third party vendor;
e) BCP and DR arrangements of the third party vendor; and
f) ability to comply with applicable laws and regulations.

6.1.5 Risk assessment shall be conducted for outsourcing services as per the risk management process.

6.1.6 Regulated Entities shall have written outsourcing agreements that shall include:

a) scope of services and service levels requirements;
b) roles and responsibilities with respect to implementation of security requirements;
c) confidentiality and security of information shared and non-disclosure requirement;
d) operations and risk management requirements;
e) business continuity and crisis management requirements;
f) right to audit and inspect;

g) termination clause; and
h) requirements with respect to notifications and disclosures of data breach events.

6.1.7 Regulated Entities shall maintain up-to-date inventory of all outsourcing agreements.

6.1.8 Regulated Entities shall perform assessment of third party vendor to ensure the adequacy of implemented/ to be implemented controls to address necessary security requirements as per the outsourcing agreement. Such assessments shall be conducted annually for significant outsourcing arrangements.

6.1.9 Regulated Entities shall implement processes to monitor activities of third party vendors. The following areas shall be reviewed as part of the monitoring process:

a) ongoing compliance with security requirements;
b) confidentiality and security of information shared; and
c) business continuity and disaster recovery arrangements.

6.1.10 Regulated Entities shall record risks and issues identified during the monitoring process and track the same to mitigation and closure.

6.1.11 Security requirements of the agreement shall be reviewed and updated periodically or upon significant changes in services provided by third party vendors.

6.1.12 Regulated Entities shall ensure secure disposal of information assets that were exchanged during the execution of outsourcing agreement.

6.2 Cloud Security

Objective: To ensure that the cybersecurity risks are assessed and adequately addressed for cloud services (For cloud computing models, refer to Appendix- Terms and Definitions), Regulated Entities shall establish cloud security measures.

The controls within the Sub-domain shall apply to public, community and hybrid cloud.

The controls in the Sub-Domain are in addition to other applicable controls specified in Baselines.

6.2.1 A policy covering security considerations for cloud services shall be defined, approved, implemented, communicated, periodically reviewed and updated.

6.2.2 The cloud security policy shall include:

a) controls from technology and operations domain (as applicable) for each type of cloud service;
b) management oversight and day-to-day operational responsibility and separation of roles;
c) data security requirements considering characteristics such as multi-tenancy, data commingling and processing of data in multiple locations; and
d) compliance with data residency requirements.

6.2.3 Regulated Entities shall seek approval from CBK before signing any cloud based outsourcing agreements. At a minimum, Regulated Entities shall submit the below information while seeking approval:

a) scope of services to be outsourced;
b) details of the risk assessment performed and the associated results;
c) proposed date to start the engagement and overall engagement period;
d) cloud service provider organization name and full address along with key contact details;
e) location of data storage;
f) operational support being provided by the cloud service provider;
g) baseline security controls established by the cloud service provider;
h) cloud service provider third party audit reports; and
i) proposed service level and operational level agreements.

6.2.4 Prior to engaging with cloud service providers, Regulated Entities shall determine whether the use of cloud services is consistent with their risk appetite and business strategy and shall conduct information classification for the function or service to be outsourced to identify sensitive data at risk.

6.2.5 Regulated Entities shall perform risk assessment that considers the benefits and risks associated with using cloud services and establish mitigation measures, as necessary. The assessment shall consider at a minimum:

a) potential impact of any disruption of the cloud service including impact on data availability;
b) access management and segregation of responsibilities with respect to cloud services;
c) location and data residency;

d) business viability, dispute management and arbitration, reputation, experience, exit strategies and conflict of interest;
e) sub-contractors (chain of contractors) engaged by cloud service providers;
f) limitations to right to audit, right to conduct security assessments and right to inspect (onsite and offsite);and
g) sole service providers risks (multiple agreements with same service provider).

6.2.6 Regulated Entities shall review the certifications and independent audits reports (e.g. ISO 27001 / 22301, SSAE16 Reports, Telecommunications Industry Association ANSI/TIA-942 Tier 3/ 4 DC certification, SOC1, SOC2, etc.) of security practices implemented by the cloud service provider.

6.2.7 Regulated Entities shall ensure adequate oversight of cloud service providers in order to effectively manage cloud security risks, as part of the overall governance and risk management process.

6.2.8 Regulated Entities shall ensure that cloud service providers use industry best practice (ISO 27001, 27018:2014, NIST Guidelines for Media Sanitization – NIST 800-88) for permanent erasure of data that has been transferred or is no longer needed. For storage that cannot be wiped, Regulated Entities shall ensure that cloud service providers uses a destruction process that destroys and renders the recovery of information impossible.

6.2.9 Regulated Entities shall ensure that a written agreement exist with cloud service providers that include the following requirements:

a) scope of services, operational level agreements and clearly defined roles and responsibilities;
b) cybersecurity regulatory and legal compliance;
c) locations of data storage, business continuity and disaster recovery, data privacy, confidentiality and information sharing, access to data, encryption, data portability, and data retention;
d) right to audit and inspect including rights to audit for CBK;
e) code of conduct and dispute management;
f) incident management, crisis management and breach notification strategies; and
g) secure termination of agreement.

7 Protection of Electronic Payment Systems

Overview: Global demand for faster and reliable electronic payments has resulted in rapid development of innovative electronic payment systems. The electronic payment systems are anticipated to evolve further with new technology solutions, innovative customer service and growing need for transparency and due-diligence.

The following section specifies the baselines essential to protect electronic payment systems from cyber risks. The section specifies the cybersecurity controls for online banking, mobile banking, digital wallets, ATM and card security and contactless payments. The controls in this domain are additional controls and need to be implemented along with the other applicable controls specified in Baselines.

7.1 Common Security Controls for Electronic Payment Systems

Objective: To secure electronic payment systems from cyber risks, Regulated Entities shall implement necessary security controls.

7.1.1 A policy for securing electronic payment systems shall be defined, approved, implemented, periodically reviewed and updated.

7.1.2 The electronic payment systems policy shall include:

a) mechanisms to protect important records against unauthorized disclosure, misuse, damage, destruction, loss, theft and manipulation; and
b) controls to monitor external parties involved in the payment and settlement systems;

7.1.3 Regulated Entities shall set the maximum three failed log-in or authentication attempts after which access to electronic payments systems is (temporarily or permanently) blocked. Regulated Entities shall set procedure in place to re-activate blocked accesses. Reactivation shall be performed with enhanced due diligence and after verifying the identity of the user.

7.1.4 Regulated Entities shall ensure secure delivery of customer credentials (user ID, password, PIN), perform authentication of customer devices and ensure security of credentials and payment software (web and mobile applications, plugins etc.).

7.1.5 Regulated Entities shall ensure the implementation of effective safeguards to minimize the risk of unauthorized fund transfer based on the channel or technology risks profile or customer profile.

7.1.6 Regulated Entities shall conduct independent security audits of the electronic payment systems annually in accordance with:

a) the assessment procedures outlined in the vulnerability management Sub-Domain; and
b) Requirements of industry regulations (such as PCI-DSS, EMV) and best practices.

7.1.7 All electronic payments shall have unique transaction reference numbers to enable traceability.

7.1.8 Transaction validation messages shall not reveal sensitive details/information of the payment systems (infrastructure or application/s).

7.1.9 Regulated Entities shall implement effective measures to notify customers on significant changes to payment profile. Such changes include:

a) changes to pre-set values such as password and limits;
b) creation of new account linkages;
c) registration of new payees; and
d) electronic remittances to beneficiaries.

7.1.10 Regulated Entities shall adopt secure and internationally recognized strong encryption algorithms for protection of sensitive information (such as login credentials, card information) at rest and in transit.

7.1.11 Regulated Entities shall ensure that personal identity verification measures such as the personal questions used by the customer service centers for verification of the customer's identity are neither generic nor easy to obtain or repeated (such as banking relations, current balance, information not available on the card, personalized questions and last transactions).

7.1.12 Changes to customer sensitive information (such as mobile number and email address) through ATM, Mobile Applications, IVR, online Banking shall be performed only after establishing authenticity of the customer using multi factor

authentication. In case of change of mobile number, second factor for authentication shall be sent to old number.

7.1.13 Effective controls shall be implemented to verify the integrity of information processed by electronic payment systems (e.g. account balances after transaction updates shall be reconciled between different systems).

7.1.14 Effective controls shall be implemented to ensure mitigation of network interconnectivity-related risks (e.g. of risk include man-in-the-middle attack, authentication bypass, network sniffing, etc.).

7.1.15 Regulated Entities shall provide appropriate facility for customers to block their Payments Cards by them self or through customer service center.

7.2 Electronic Payment Transaction Monitoring

Objective: To detect and prevent fraudulent electronic payment transactions, Regulated Entities shall implement transaction monitoring and authorization mechanisms.

7.2.1 An electronic payment transaction monitoring process shall be defined, approved, implemented and reviewed periodically and be in line with Instructions for regulation of the electronic payment of funds.

7.2.2 The electronic payment transaction monitoring process shall consider the following risk factors:

a) transaction limits;
b) known fraud scenarios;
c) abnormal payment patterns in relation to payment transaction history;
d) customer transaction preference;
e) risks based on the location of the payer and the payee at the time of the payment transaction;
f) failed authorization attempts;
g) velocity checks; and
h) Changes to sensitive information of customers.

7.2.3 Unusual transactions shall be investigated and reported to customers (if necessary).

7.2.4 Regulated Entities shall notify customers through effective communication channels for all transactions performed on their accounts including rejected transaction.

7.3 Online Banking Security

Objective: To ensure confidentiality, integrity and availability of online banking system, Regulated Entities shall implement online banking security controls.

7.3.1 Online banking systems and applications shall be configured to ensure that:

a) user sessions terminate after five minutes of inactivity;
b) concurrent sessions are disallowed; and
c) Validity of one-time passwords is restricted to a maximum of five minutes.

7.3.2 Online banking applications (other than mobile applications) shall include additional controls such as secure access image and/ or secure message at login to assist identification of phishing sites.

7.3.3 Regulated Entities shall establish reliable and effective authentication measures by implementing strong multi factor authentication controls:

a) Implement anti-phishing controls to identify the user (e.g. user name), identify the application (pre logon challenge questions, site key, multi-screen authentication, etc.) and authenticate the user with a password as part of the authentication process.
b) Use additional factor for account activation, financial transactions such as fund transfer, bill payments and beneficiary addition using out of band verification method stated below;
    i. OTP generated by device; or
    ii. OTP sent to customer via SMS; or
    iii. digital certificates stored in smart cards; or
    iv. Other devices in the customer's possession shall be used for transaction authorization as additional factor (something the customer has).

7.3.4 The Regulated Entities shall ensure that appropriate procedures and security measures are in place to validate the identity of all users enrolled through remote channels.

7.4 Mobile Banking Security

Objective: To ensure confidentiality and integrity of transactions initiated by mobile banking, Regulated Entities shall implement mobile banking security controls.

7.4.1 Regulated Entities shall implement controls to restrict installation and usage of mobile applications on jail-broken devices.

7.4.2 Regulated Entities shall ensure that the mobile application encrypts the data stored if any, locally by the application on the customer devices.

7.4.3 Regulated Entities shall conduct security assessment to identify and remediate vulnerabilities associated with their mobile applications.

7.4.4 Regulated Entities shall ensure that the mobile application verifies the mobile number and device IMEI of the customer for first time use of applications.

7.4.5 Customers may be allowed to access mobile banking application from up to three validated devices.

7.5 Payment Card Information

Objective: To ensure payment card information is adequately protected, Regulated Entities shall implement card data security controls.

7.5.1 Regulated Entities shall ensure compliance to applicable regulations and industry best practices (e.g. PCI-DSS, PA-DSS, EMV) for protecting payment card information.

7.5.2 Complete card number shall not be part of any communication to the customers.

7.5.3 Card PIN generation shall be secured so as to restrict access to PIN only to the intended recipient.

7.6 Customer Self Service Machines (ATMs, POSs, KIOSKs, ITMs, XTMs,…etc)

Objective: To prevent compromise or leakage of customer information through Customer Self Service Machines, Regulated Entities shall implement security measures.

7.6.1 Regulated Entities shall implement physical security measures to protect Customer Self Service Self Machines from theft, damage, etc

7.6.2 Customer Self Service Self Machines shall authenticate customer transactions using combination of card (e.g. debit card, credit card, tokenized card, civil ID) and PIN (static or one time) numbers as applicable.

7.6.3 Segregation of duty controls shall be implemented for card processing, PIN generation and delivery of the card and PIN to the customer. Regulated Entities shall ensure that the card is issued in inactive state and the process is established for activation.

7.6.4 The Regulated Entities shall block the card upon three unsuccessful attempts of usage of PIN and effectively notify the customer for prevention of potential misuse. Requests for activation of such cards shall be undertaken with enhanced diligence through secured channels.

7.6.5 Regulated Entities shall implement anti skimming and other latest security measures on Customer Self Service Self Machines

7.6.6 Regulated Entities shall undertake physical inspection of Customer Self Service Self Machines locations periodically to verify the effectiveness of implemented security measures.

7.7 Contactless Technology

Objective: To protect sensitive information from electronic pickpocketing or eavesdropping of contactless/ wireless traffic between customer mobile device and the payee, Regulated Entities shall implement controls to secure contactless technology.

7.7.1 Regulated Entities shall conduct risk assessment to identify risks due to use of NFC and QR code technology, and implement the controls to mitigate identified risks.

7.7.2 Regulated Entities shall implement appropriate limits on number and value of NFC transactions. Subsequent transactions shall enforce additional authentication.

7.7.3 Regulated Entities shall notify customers through effective communication channels for transactions performed using contactless technologies.

8 Appendix – Terms and Definitions

Term	Definitions
Asset Owner	individual who is approved by the management to control, use and be responsible and accountable for security of the asset.
Cloud Service	Cloud Service is new operational model and set of technologies enables on-demand access to a shared pool of resources such as applications, servers, storage and network. **Cloud service delivery models**: • **Infrastructure as a Service:** The cloud service provider (CSP) delivers IT infrastructure, such as space, computing power, processing, networks, and other fundamental computing resources. • **Platform as a Service:** The CSP provides a computing platform for customers to develop and run their own applications. • **Software as a Service:** The CSP makes software applications available to customers. **Cloud service deployment models:** • **Private Cloud:** The cloud infrastructure is provisioned solely for a single organization. A CSP typically owns and manages the infrastructure of the private cloud, although the customer may also own and manage the infrastructure. The infrastructure is located either on customer premises or on the CSP's premises. • **Public Cloud:** The cloud infrastructure is provisioned for open use by the general public. A CSP owns and manages the infrastructure for the public cloud, which is not located on the premises of the customer. Although the data and services are protected from unauthorized access, a variety of customers use and share the infrastructure. • **Community Cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has–similar computing needs or requirements, such as security, reliability, and resiliency. The CSP or members of a community may own and manage the infrastructure. The infrastructure is located either on customer premises or the CSP's premises. **Hybrid Cloud:** The hybrid cloud is a combination of two or more of the private cloud, public cloud, and community cloud (and can involve use of non-cloud environments, as well). The CSP or the customer may own and manage the hybrid cloud infrastructure, and in either case the infrastructure may be located on- or off-premise, or both. The data and services can be managed based on the design of the solution, corresponding to whether the architecture has public, private, or community characteristics
Compliance requirements	Global regulations, national and international laws, regulatory requirements, applicable technology standards, and guidelines provided by leading service providers.
Contactless technology	Devices which enable payments without the need of swiping a card on point of sale machines (e.g. (e.g. QR (Short) code payments, Near Field Communication (NFC) payments, wearables)

Criticality	Magnitude of impact in case of failure of information assets on operations, compliance, service to customers, financial stability and confidentiality, integrity and availability of important records residing on the information asset.
Data Subject	A data subject is any person (customer, vendor, third party, and employee) whose personal identifiable information is being collected, held or processed.
Electronic records / Information	Records maintained by the entity in electronic form.
Emerging technologies	Emerging technologies include Block chain, technology enabled financial products / services, cloud services, robotic process automation, chat bots, internet of things, mobile and internet based value added service enablement, wearables, QR Code and NFC Payments, etc.
External Connections	Network connections other than internet connectivity used by internal users to browse the internet or used by customers/ third parties to access the web facing applications hosted in the demilitarized zone of the regulated entity.
External Parties	Third parties which may be part of the payment systems due to principal - agent relationship, transaction acquisition, payment aggregation, etc.
Important Records	Electronic records of the nature of transactional data, sensitive and personally identifiable information processed by the regulated entity.
Information Processing Facilities	A physical location which hosts information processing systems, services or technology assets.
Mobile Banking	Electronic banking channel enabled through a mobile application which needs to be installed on customers mobile.
Multifactor authentication	The use of two or more of the following factors to verify a user's identity: -- knowledge factor, "something an individual knows"; -- possession factor, "something an individual has"; -- biometric factor, "something that is a biological and behavioural characteristic of an individual". Example for first factor authentication can be User ID and passwords or PIN (i.e., something a user knows). Example for multifactor authentication include (i) OTP generated by a token/device that is in the customer's possession and associated with the customer's bank account; (ii) OTPs generated by Regulated Entities security systems and delivered to customers via SMS; and (iii) digital certificates stored in a smart card or other devices in the customer's possession (i.e., something a customer has)
Online Banking Channel	Internet based payment mechanism setup for convenience of the customers including mechanism such as internet / online banking, mobile banking, payment wallets.
Outsourcing Agreement	A written agreement setting out the contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations between the Regulated entity and third party vendor.

Portable devices	Portable devices include desktops, laptops, mobiles, and tabs owned by the regulated entity or employees and are allowed to connect to the Regulated Entities network.
Premises	Owned/leased offices, data center, disaster recovery sites, branches, extension counters and other operating facilities used by the Regulated Entities.
Relevant stakeholders	Internal employees who are empowered by the Board or Senior Management to independently make decision.
Sensitive information	Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the privacy to which individuals are entitled. Personally identifiable information (set of information which help identify an individual [name, address, date of birth, email address, card number, login credentials, etc.]), payment card information, Civil ID, passport number, other master records of customers / employees / third party vendor staff.
Significant Outsourcing Agreements	An outsourcing arrangement which; in the event of a service failure has impact on operations, compliance, service to customers, and important records of the regulated entity.
Third Party Vendors	All third parties who have access to technology assets of the regulated entity
Technology assets	Hardware, software, network, electronic records or IT components which are connected to the IT network of the regulated entity. This includes assets provided by the third party vendor as part of the third party vendor agreements.
Users	Employees and third party vendor staff having access to information assets.

9 Appendix - Glossary

Term	Definition
CBK	Refers to the "Central Bank of Kuwait".
CSF	Refers to the "Cybersecurity Framework".
CMSP	Refers to the "Cyber Crisis Management Strategy and Plan"
Cyber Lexicon	Lexicon of terms related to cybersecurity and cyber resilience published by Financial Stability Board.
Banking sector	Refers to CBK and all entities that are regulated by CBK including Local Banks, Foreign Banks, Exchange Companies, Investment companies, payment service providers, and other regulated Finance Companies.
Local banks	Refers to all Banks including the Kuwaiti Banks and the Foreign Banks authorized by CBK.
Regulated Entities	Refers the following: ● Kuwaiti Banks ● Foreign Banks ● Finance Companies ● Exchange Companies ● Investment Companies ● Companies/ Organizations that are subject to Payments Regulations (Law 20 of 2014 Chapter 6)
Regulated entity or Entity level	Refers to aspects or expectations at each entity level
Responsibility/ Responsible person	The responsible person is the individual(s) who actually complete the task. The responsible person is responsible for action/implementation. Responsibility can be shared.
Accountability/ Accountable person	The accountable person is the individual who is ultimately answerable for the activity or decision.
ISWG	Refers to the "Information Security Working Group"
Cybersecurity maturity	Refers to the assessment of cybersecurity against levels defined as a part of Cybersecurity assessment process.
NIST	National Institute of Standards and Technology
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
ISF	Information Security Forum
PCI	Payment Card Industry
CIS	Center for Internet Security

CYBER CRISIS MANAGEMENT STRATEGY & PLAN

CYBER CRISIS MANAGEMENT STRATEGY & PLAN

TABLE OF CONTENTS

1. Introduction

The National Cyber Security Strategy for the State of Kuwait identified Kuwait's banking sector as part of the Critical National Infrastructure. In line with the National Cyber Security Strategy, the Central Bank of Kuwait (CBK) recognizes the need for the banking sector to improve its resilience to cyberattacks and actions. Accordingly, the Cybersecurity Framework (CSF) has been developed, and it is applicable to all Regulated Entities within the banking sector. To meet the objectives of the CSF (illustrated in Figure 1), the Cyber Crisis Management Strategy and Plan (the Strategy) is developed to standardize and improve the cyber crisis management capabilities and response approaches for Regulated Entities across the Kuwaiti banking sector, regardless of their size, nature, type and complexity. Accordingly, Regulated Entities shall align their business continuity and disaster recovery arrangements with the Strategy.

Figure 1: Cybersecurity Framework

1.1 Definition of Cyber Crisis

CBK defines "Cyber Crisis" for the Kuwaiti banking sector as:

"An adverse, unstable, and complex incident triggered by a cyber-attack / action both that limits protection or restoration of systems' availability, integrity, authentication, confidentiality, or nonrepudiation and that creates sufficient impact as to represent a threat to the strategic objectives, reputation, or economic viability of Kuwait's banking sector."

1.2 Strategic Vision and Objectives for Cyber Crisis Management

CBK's strategic vision for the Strategy is to ensure a resilient banking sector by promoting effective, efficient, and consistent responses to cybersecurity incidents and related crises by enhancing sector wide preparation, collaboration, compliance, and continuous improvement initiatives.

1.3 Strategic Drivers

The Strategy exists to promote the:

a. protection of the Kuwaiti economy by maintaining the financial stability of the Regulated Entities;
b. protection of customer interests within the Kuwaiti banking sector; and
c. protection of the reputation of and trust in the Kuwaiti banking sector.

1.4 Scope

The Strategy's scope is limited to cyber crisis management, including:

a. defining requirements for cyber crisis management preparedness and response capability;
b. being alert and capable to identify and efficiently respond to cyber incidents that create crisis level impact;
c. mitigating the risks introduced by third parties to Regulated Entities;
d. conducting regular exercises to validate strategy and plan effectiveness; and
e. updating the Strategy to act on feedback and results from tests conducted and real incidents managed.

1.5 Applicability

The Strategy is applicable to all Regulated Entities supervised by CBK.

1.6 Target Audience

The Strategy is issued for the Board of Directors, Senior Management, Information Security Professionals, Crisis Management Professionals, Business Continuity and Disaster Recovery Professionals, Information Technology Professionals, and others who are responsible for establishing and implementing cyber crisis management strategies, plans, and responses.

1.7 Applicable Laws and Regulations

Article 15 of Law No. 32 of 1968 authorized CBK to supervise the Regulated Entities, and the Strategy is included within this scope. In addition to the Strategy, all Regulated Entities shall remain compliant with existing, national laws and regulations in their jurisdictions of operation (i.e., in Kuwait or elsewhere), including the following:

- Kuwait National Cyber Security Strategy;
- Instructions No. 2/BSA/152/2004 to all Islamic banks;
- Message from the Central Bank of Kuwait's Governor's Office, 26 September 2006 regarding business continuity plans;
- Article (198) of the Kuwait Civil Code dealing with emergencies; and
- Law No. 32/1968 regarding the unauthorized disclosure of customer information.

CBK will provide necessary clarifications, guidance, and directives to the Regulated Entities based on reviews, observations or submitted clarification requests.

2. Cyber Crisis Management Requirements

Regulated Entities are required to implement the following governance and organizational structures to maintain a compliant, cyber crisis management preparedness and response capabilities, which will assist them to respond to cyber incidents with crisis level impact throughout the crisis lifecycle: react; respond; and emerge stronger (i.e. recover). CBK will supervise Regulated Entities for compliance with these requirements during its inspection cycle (e.g. crisis management and response plans existence and use, results of exercises conducted, accountability of lessons learned, etc.).

2.1 Cybersecurity Strategy

Regulated Entities are required to establish cybersecurity strategies that are approved by Board or Senior Management and that are tailored to their organizational structure, risk profile, business objectives, and the strategic drivers (specified in Section 1.3). Regulated Entities' cybersecurity strategies shall align with the Cybersecurity Baselines for the Kuwait Banking Sector, organizational policies, and applicable national and international legal and regulatory requirements.

2.2 Cyber Crisis Organization Structure

Regulated Entities are required to establish a cyber crisis organizational structure[1] that defines and integrates technical, business and management functions. The structure shall include a Crisis Response Lead and Crisis Management Team proportional to the size, nature, type and complexity of the Regulated Entity.

2.2.1 Crisis Management Team

Regulated Entities are required to establish Crisis Management Team led by the Crisis Response Lead (specified in Section 2.2.2) and comprised of empowered, multi-functional representatives, specifically including Operations, Information Technology, Information Security, Legal, Communications, and other, relevant stakeholders. The team is responsible for:

a. developing, maintaining, promoting, and exercising crisis management planning;

[1] For some Regulated Entities, a singular team structure could deliver crisis as well as broader business continuity and other risk management support. For other, larger Regulated Entities with more diverse operations, dividing the remit between a more strategic / executive crisis management team and a more tactical / business continuity management team would promote having the appropriate participants with the needed authorities at different levels of focus and action. Final designs shall be tailored to each Regulated Entity.

b. assisting the Crisis Response Lead to assess whether an incident with crisis level impact exists and whether a formal response is required;
c. mobilizing and deploying necessary internal and external resources to deliver the response;
d. overseeing execution of response activities; and,
e. managing the communication with internal and external stakeholders throughout a crisis management lifecycle.

2.2.2 Crisis Response Lead

Regulated Entities are required to identify Crisis Response Lead, who is authorized to make crisis response related decisions independently and on behalf of the Regulated Entities. A Crisis Response Lead has the sole authority within a Regulated Entity to declare that a crisis exists and that a formal response is required. The Crisis Response Lead acts as a single point of contact and as the lead representative of the Regulated Entity in CBK-led, sector-wide responses (specified in Section 3.3.1). Regulated Entities are required to ensure Crisis Response Lead:

a. have sufficient skills and experience to comprehensively understand the Regulated Entity's operations and to make reasonable decisions guided by his/her own integrity, competence, and professional capability;
b. have successfully completed relevant training (e.g. has relevant qualifications) and continue to learn emerging cyber crisis related trends; and
c. have a documented set of authorities and responsibilities, including approval to make decisions independently in support of the crisis response on behalf of the Regulated Entity.

2.3 Severity Impact Matrix

Regulated Entities are required to develop a severity impact matrix that is approved by their Board or Executive Management and that tiers impacts to the Regulated Entities (e.g. low, medium, high) across their categories of significant consideration. The impact tiers dictate appropriate mitigating actions in response to cyber incidents. Impact categories shall include the categories captured within the Sector Severity Impact Matrix (specified in Section 3.2) as well as Regulated Entity-specific impact categories and measurements (e.g. impacts from

critical economic functions'[2] operational risk tolerances being exceeded because of a cybersecurity incident, etc.)[3] The tiers of the severity impact matrix will consider the outcomes of formal business impact analyses (BIA), internal assessments, and risk analyses.

2.4 Crisis Management Plans

Regulated Entities are required to maintain updated crisis management plans that support their enterprise resilience beyond cyber crisis management planning. These Board- or Executive Management-approved plans should address operational risk management considerations (e.g. disaster recovery, business continuity, and internal/external communications policies, plans, procedures, and templates). The crisis management plans shall be implemented enterprise-wide and shall structure key organizational functions, authorities, and responsibilities and shall be aligned with legal, regulatory, and organizational requirements.

2.5 Threat Intelligence, Notification, and Response Tracking

Regulated Entities are required to maintain and to use appropriate tools and threat intelligence feeds from internal systems and third party providers. This approach will help Regulated Entities to initiate enterprise-wide risk assessments and response efforts including:

2.5.1 Threat Intelligence Feeds

Threat intelligence and situational awareness feeds will support identification of relevant cyber threats and actors that will assist in protecting information and information assets, as further described in Cyber Threat Information Sharing Strategy[4].

2.5.2 Emergency Notification

Appropriate incident detection measures (e.g., IT system monitoring, logs analysis technologies) will support timely awareness of threats, and emergency notification mechanisms will support timely contact with responders and employees in the event of an incident with crisis level impact.

[2] A critical economic function delivers the output from a Regulated Entity, without which there would be a material impact on the Regulated Entity or its operations and by extension could represent a material impact on the Kuwaiti banking sector.

[3] CBK recognizes that the tiered, impact details within Regulated Entities' severity impact matrices will differ, based on their service offerings, geographic spread of operations, volume and type of customer, etc. As such, CBK cannot mandate a common set of categories and tier thresholds therein for every Regulated Entity in the sector. To promote some consistency across Regulated Entities, CBK encourages Regulated Entities to interpret the Strategy's Sector Severity Impact Matrix categories (specified in Section 3.2) on the scale of their own operations.

4 Cyber Threat Information Sharing Strategy is part of Cybersecurity Framework

2.5.3 Response Tracking Tools

Crisis management response tools (e.g. a decision and action logging capability) create an auditable trail of response considerations, which assists lessons learned efforts.

2.6 Continuous Learning Model

Regulated Entities are required to adopt a continuous learning model to promote improved and future readiness for cyber incidents, including providing targeted training and conducting cyber crisis exercises. This approach enhances responders' capability and confidence with cyber incidents handling.

2.6.1 Training

Regulated Entities are required to provide regular training appropriate to crisis responders' roles in crisis response as well as ad hoc training if there is any change to the Regulated Entity's response process.

2.6.2 Cyber Crisis Exercises

Regulated Entities are required to conduct cyber crisis exercises on an annual basis to ensure that cyber crisis management plans, procedures, and response infrastructure remain relevant and effective. The Regulated Entities are required to increase the complexity and intensity of exercise scenarios as its crisis management maturity advances.

2.7 Third Party Requirements

Regulated Entities are required to include appropriate, crisis-relevant, contractual terms and Service Level Agreements (SLAs) with third party providers to promote the mitigation of the risk introduced to Regulated Entities by third party providers. Regulated Entities are required to obtain sufficient assurance from third party providers to mitigate cybersecurity risks.[5]

2.8 Sector Engagement and Crisis Exercises

Regulated Entities are required to participate in CBK-organized sector-wide crisis exercises (illustrated in Figure 2) focused on cyber and other relevant scenarios. The exercises may be in the form of workshops, tabletop exercises, cyber drills, etc. CBK will use Information

[5] Regulated Entities shall be responsible for mitigating the risk introduced to their operations by those third parties on which the Regulated Entities significantly depend to deliver their services – regardless of whether or not CBK directly regulates the third party. The Regulated Entities shall have sufficient clarity and assurance of such third parties' controls to mitigate cybersecurity incidents and crises.

Security Working Group (ISWG) as a collaboration platform for conducting such exercises to promote the sector's maturity, resilience, and collective response readiness. Figure 2 depicts the planned, gradual increase in complexity of sector wide, crisis exercises as Regulated entities maturity level progresses over time.

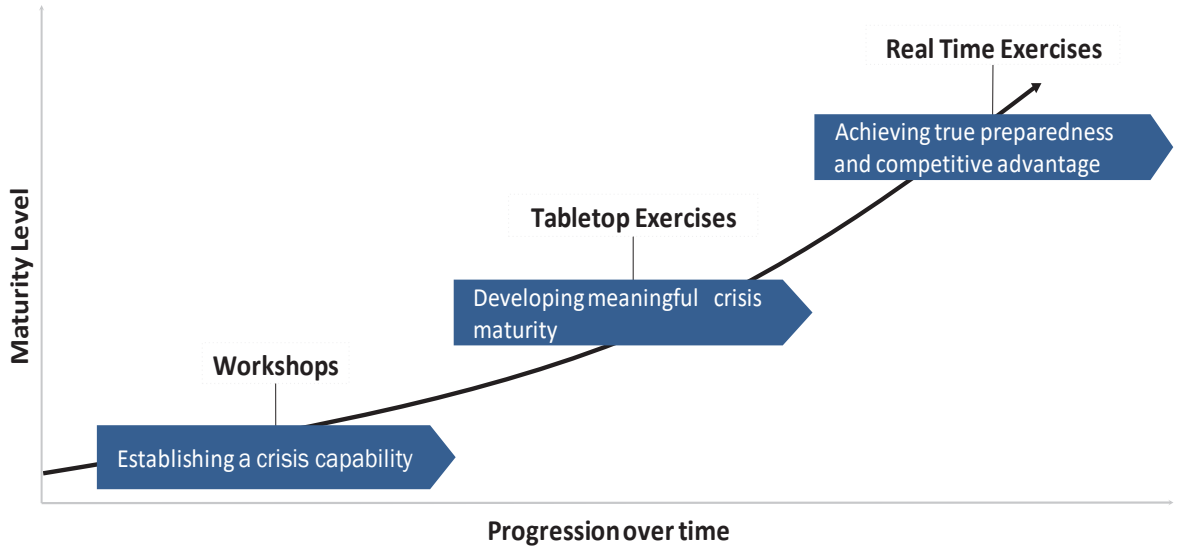


Figure 2: Crisis exercising options

3. Sector Wide Cyber Crisis Management Strategy

The Strategy defines Regulated Entities' cyber crisis management requirements, including processes for crisis responses across the banking sector to promote resilience and the ability to emerge stronger from these incidents. The Strategy includes reporting requirements, a sector severity impact matrix, and a sector wide response process.

3.1 Reporting Requirements of Regulated Entities

Continuous coordination between Regulated Entities and CBK before, during, and after a crisis maximizes the opportunities to deliver effective, efficient, and consistent crisis responses. Regulated Entities are required to execute a formal reporting process to CBK if an incident is detected (specified in Section 4) that has or could have a significant and adverse effect on the Regulated Entity's ability to provide adequate services to its customers, on its reputation, or on its financial condition. To measure the impact, Regulated Entities shall have an internal severity impact matrix to guide appropriate and consistent assessments of the actual and potential impacts of cybersecurity incidents on their organizations (specified in Section 2.3). Regulated Entities are required to notify CBK of cybersecurity incidents, as stated below.

3.1.1 Low Severity Impact

Based on known and forecasted impacts, Regulated Entities are required to report to CBK on a **quarterly** basis for all **low severity impact** rated, cyber incidents for analysis of threat trends to the Kuwaiti banking sector (specified in Section 4.4). CBK may request additional information as deemed necessary to promote its technical assessment of the situation.

Referential examples of relevant impacts for a low severity impact rated incident include but are not limited to:

a. any cybersecurity issue that had minor impact on or the potential to disrupt the Regulated Entity's operations and ability to provide services to its customer population if defensive or responsive actions had not mitigated the threat; or,
b. any cybersecurity issue assessed to have less than 2% of capital **OR** less than 10 million KD of collective financial impact on the Regulated Entity and/or its customers (whichever is lower).

3.1.2 Medium Severity Impact

Based on known and forecasted impacts, Regulated Entities are required to notify CBK (specified in Section 4) regarding **medium severity impact** rated, cyber incidents for response planning coordination within **eight hours (business day hours)** of discovery, having completed initial quantification of potential and/or actual impact to the Regulated Entity and/or its customers. CBK may request additional information as deemed necessary to promote its technical assessment of the situation.

After the initial notification and assuming that the severity impact rating did not increase since the last reporting, Regulated Entities shall provide CBK updates on response efforts using the Situation Report (specified in Section 4.2) every **two business** days from the prior notification (or at a cycle defined by CBK). Regulated Entities shall submit Closure Reports (specified in Section 4.3) as soon as the response and recovery are completed.

Referential examples of relevant impacts for a medium severity impact rated incident include but are not limited to:

a. any cybersecurity issue that partially or fully disrupts the Regulated Entity's operations and ability to provide services to 5-15% of its customer population;
b. any cybersecurity issue assessed to have between 2-5% of capital **OR** between 10-20 million KD of collective financial impact on the Regulated Entity and/or its customers (whichever is lower);
c. any cybersecurity issue assessed to possibly result in a regulatory investigation of and/or sanctions (Kuwaiti or offshore) against the Regulated Entity; or,
d. any cybersecurity issue assessed to possibly have a significantly negative impact on the reputation of the Regulated Entity and/or the Kuwaiti banking sector.

3.1.3 High Severity Impact

Based on known and forecasted impacts, Regulated Entities are required to notify CBK (specified in Section 4) regarding **high severity impact** rated, cyber incidents for response planning coordination within **four hours (business day hours or not)** of discovery, having completed initial quantification of potential and/or actual impact to the Regulated Entity and/or its customers. CBK may request additional information as deemed necessary to promote its technical assessment of the situation.

After the initial notification, the affected Regulated Entity shall provide updates on the response to CBK through the ISWG and/or by using the Situation Report (specified in Section

4.2) **once a day** (or at a cycle defined by CBK following the prior notification). Regulated Entities shall submit Closure Reports (specified in Section 4.3) as soon as the response and recovery are completed.

Referential examples of relevant impacts for a high severity impact rated incident include but are not limited to:

a. any cybersecurity issue completely disrupting the Regulated Entity's operations and ability to provide services to more than 15% of its customer population;
b. any cybersecurity issue assessed to have more than 5% of capital **OR** 20 million KD of collective financial impact on the Regulated Entity and/or its customers (whichever is lower);
c. any cybersecurity issue likely to result in a regulatory investigation of and/or sanctions (Kuwaiti or offshore) against the Regulated Entity; or,
d. any cybersecurity issue assessed to have a significantly negative impact on the reputation of the Regulated Entity and/or the Kuwaiti banking sector.

Notification requirements for Regulated Entity to CBK			
Known and Forecasted Impacts	**Initial Reporting**	**Situation Reporting**	**Closure Reporting**
High	Within 4 hours of discovery (business day or not)	Once a day	Upon closure
Medium	Within 8 hours of discovery (business day only)	Once in 2 business days	Upon closure
Low	Not Applicable	Not Applicable	Quarterly

Table 1: Summary of notification requirements for Regulated Entities to CBK, as applicable to incidents of low, medium, and high impact ratings based on known and forecasted impacts.

3.2 Sector Severity Impact Matrix

Possible crisis triggers and their impacts on the sector are diverse, so the need for clear criteria for invoking sector wide crisis response is imperative to promote predictable actions. As such, CBK will use the Sector Severity Impact Matrix to assess critical categories of impact on the sector as a whole to guide consistent decisions regarding responses' structure and resource allocation.

Timely and consistent notification by the Regulated Entities of both known and forecasted impact details will promote CBK's efficiency in determining whether multiple Regulated Entities

might be the subject of a similar cybersecurity incident and by extension whether a centrally coordinated, sector-wide crisis response might best achieve the strategic drivers. Incident examples by tier include:

a. **Low severity impact rated incident**: Two Regulated Entities report that a cyber actor virtually defaced their websites in such a way that interrupts the ability of many customers – possibly as many as 25,000 – to access online banking services.

b. **Medium severity impact rated incident**: One Regulated Entity reports a cyber breach resulting in the exposure of approximately 10,000 Personally Identifiable Information (PII) records.

c. **High severity impact rated incident:** Three Regulated Entities report their inability to provide services given a ransomware attack encrypting all of their data and their receipt of ransom demands from the attackers to be paid to decrypt the data.

CBK will consolidate all crisis notifications reported by Regulated Entities and will assess them against the Sector Severity Impact Matrix. CBK will respond based on the severity tier identified by analyzing the reported impacts on Regulated Entities for each category, including both known as well as forecasted trends. Meeting only one category's impact description will be sufficient to trigger a response structure for that level. This means that, if CBK combined all Regulated Entities' reported impacts and found that two categories had "low" severity impacts and one category had a "medium" severity impact, then then CBK would intervene and would leverage "medium" severity response protocols.

If available data does not support a clear determination that an impact category's impact description was met fully, CBK will presume a higher level of impact and react accordingly as a default response methodology. CBK may raise or lower response protocols based on new data.

Sector Severity Impact Matrix						
	Impact Category / Severity Tier	Service disruption impact from incident	Reputational impact from incident	Impact of fraud or theft	Impact from data breach incident	Impact from other cyber incidents [6]
CBK intervention	**High**	Complete service disruption to >2 OR partial service disruption to >5 OR minimal impact without service disruption to >10 Regulated Entities	Significant discourse challenging the reputation of the Kuwaiti banking sector	Fraudulent offenses or theft of property impacting >10 entities and/or >50 million KD in value	Significant unauthorized access or release of records impacting >10% of customer base	Other events impacting >10 Regulated Entities
	Medium	Complete service disruption to 1-2 OR partial service disruption to 3-5 OR minimal impact without service disruption to 5-10 Regulated Entities	Discourse challenging the reputation of >5 Regulated Entities	Fraudulent offenses or theft of property impacting 5-10 Regulated Entities and/or 20-50 million KD in value	Unauthorized access or release of records impacting 2-10% of customer base	Other events impacting 5-10 Regulated Entities
	Low	Partial service disruption to 1-2 OR minimal impact without service disruption to 1-4 Regulated Entities	Discourse challenging the reputation of 1-4 Regulated Entities	Fraudulent offenses or theft of property impacting 1-4 Regulated Entities and/or <20 million KD in value	Unauthorized access or release of records impacting up to 2% of customer base	Other events impacting 1-4 Regulated Entities

Table 2: Severity Impact Matrix to assess consistently the sector-wide impacts / response actions.

[6] 'Impact from other cyber incidents' includes impacts from incidents such as port scanning, malware infections, DDoS, unauthorized access, unauthorized privilege escalation, destructive attack, and others. The thresholds that applied to this column were created with the intention of being applicable to and tailored to various potential events.

3.3 Sector Wide Response

There may be a need for a unified, sector wide response to enable the Kuwaiti banking sector to outperform some, high impact cyber threats. Regulated Entities' full participation across the following actions will maximize the skills, knowledge, and understanding that the banking sector has to leverage in its cybersecurity efforts and crisis responses.

3.3.1 Structure of Response

In all low, medium, and high impact rated incidents, impacted Regulated Entities are responsible for appropriately initiating their own incident response plans at the Regulated Entities' discretion to respond and mitigate the impact of the incident. Upon receipt of Regulated Entities' notifications (e.g., for medium and high impact rated crises), CBK will assess the impact category and assist based on the below:

a. **Low severity impact to the sector:** If CBK assesses the reported, known, and forecasted details have a "**low**" severity impact on the sector as a whole, then the reporting Regulated Entities will operate independently to mitigate and to recover from the crisis. While CBK will not plan to take any immediate action, CBK might escalate the responses from the individual Regulated Entities to the ISWG for broader coordination. CBK will coordinate internally to ensure appropriate awareness across CBK's leadership.

b. **Medium severity impact to the sector**: If CBK assesses the reported, known, and forecasted details have a "**medium**" severity impact on the sector as a whole, CBK will direct the reporting Regulated Entities to deliver their responses to mitigate and to recover from the incident. CBK might escalate the responses from the individual Regulated Entities to the ISWG for broader coordination. CBK will coordinate internally and with Regulated Entities to support crisis responses. CBK's coordination may include engaging national coordination bodies and/or the executive leadership of the relevant Regulated Entities.

c. **High severity impact to the sector**: If CBK assesses the reported, known, and forecasted details have a "**high**" severity impact on the sector as a whole, CBK will instruct the reporting Regulated Entities and the sector to deliver the unified response to mitigate and to recover from the incident. CBK will activate the ISWG for sector coordination related to technical, operational, communications, and other

considerations. Regulated Entities' ISWG Representatives as well as their Crisis Response Leads will report to the ISWG upon CBK's direction to support cross-sector collaboration. CBK's representative at the ISWG will coordinate internally to ensure appropriate awareness across CBK's leadership and will be empowered to make decisions on behalf of CBK and the sector, so as to promote an efficient and effective sector response. CBK's coordination will include engaging national coordination bodies and the executive leadership of the relevant Regulated Entities. CBK might request the affected Regulated Entity to suspend services until the crisis is mitigated.

3.3.2 Response Cycle

CBK will instruct the Regulated Entities on the need and frequency for Regulated Entity-specific alignment meetings and/or ISWG-based alignment meetings. For example, "high" impact rated, sector crises are likely to have daily meetings at the ISWG to coordinate the response effort (e.g., a meeting at 1400) to update on actions during the day. The below Figure 3 illustrates the overall cyber crises management response cycle.

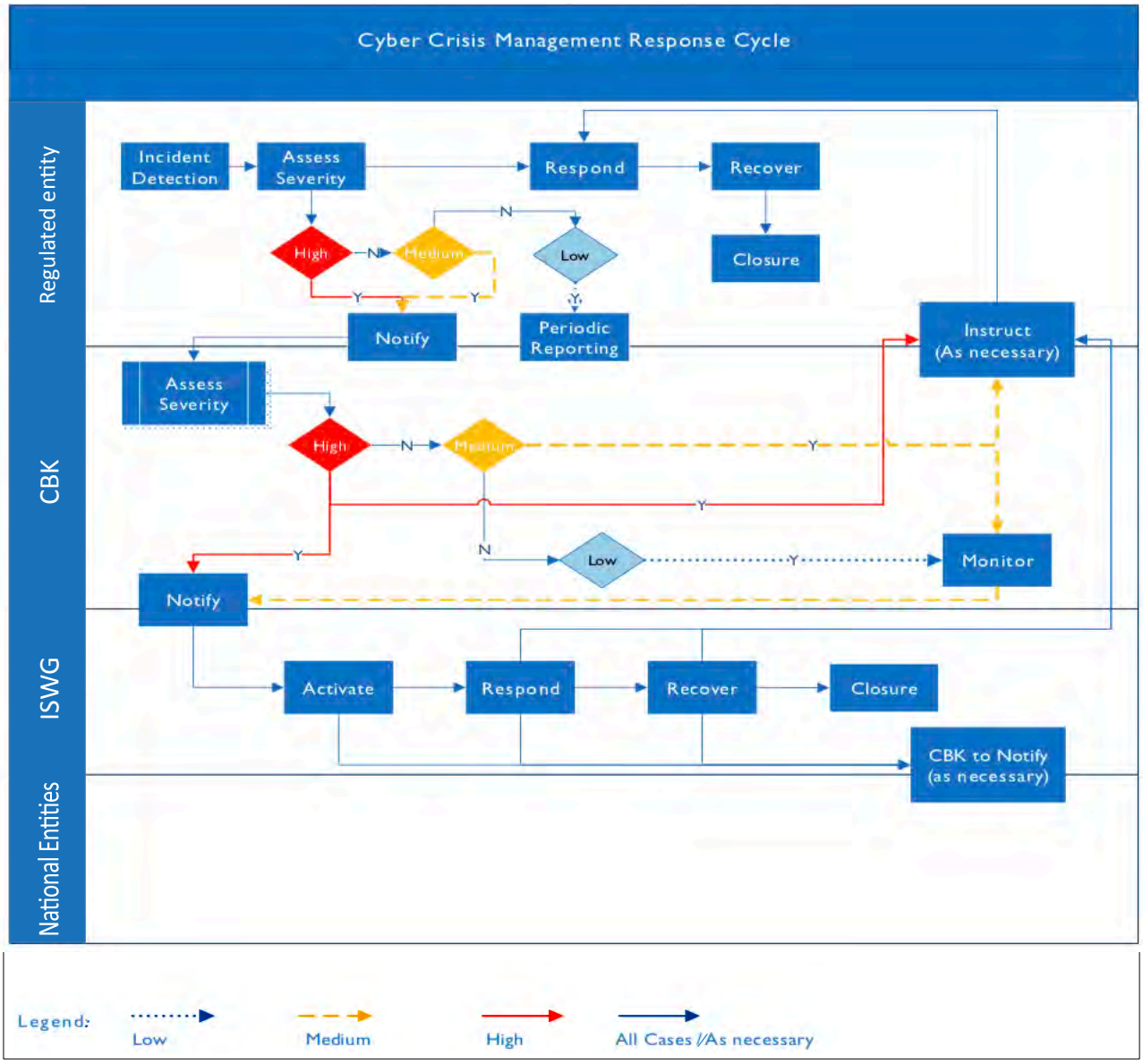


Figure 3: The Strategy's process flow for cyber crisis response from a Regulated Entity and sector-wide perspective, including key responsibilities therein.

3.3.3 Continual Improvement

Regulated Entities are required to work with CBK on a regular basis to foster continual improvement of their cyber crisis management preparedness. This approach will gradually improve the cyber crisis management maturity of the entire banking sector, as well. Regulated Entities are required to implement relevant training and exercising programs and to submit Closure Reports (specified in Section 4.3) to CBK to highlight areas of improvement. As part of the continual improvement process, CBK will review Regulated Entities' areas of improvement and their lessons learned and will undertake changes to the Strategy to improve the banking sector's cyber capabilities, preparedness, and maturity.

4. Appendix - Crisis Notification to CBK

Regulated Entities shall use these templates to consistently structure their notifications to CBK of cybersecurity incidents for low, medium, and high impact rated incidents. Regulated Entities shall email these written notifications (encrypted) to **KB_ISWG@CBK.GOV.KW** and thereafter should call CBK at **+965 1814444** (operational 24/7) to confirm CBK's receipt of the written notification. If all telecommunications are unavailable, Regulated Entities shall make every reasonable effort to make contact with CBK as soon as is possible.

4.1 Initial Notification

In line with Section 3.1 reporting requirements, Regulated Entities shall use this template to structure their initial notifications to CBK of cybersecurity incidents.

Initial Notification			
Regulated Entity Name & Crisis Response Lead Name	Entity Name Lead Name Telephone	Date / Time of report	DD MMM YYYY HHMM
Entity's severity impact rating	ex., high, medium, or low	Entity's incident reference #	Unique identifier, if applicable
Description of issue	Describe the issue, including the incident category (ex., DDoS, defacement, information breach, etc.), the attack vector, the level of service disruption, regulatory investigation / sanction potential, reputational impact, and percentage estimate for number of customers affected		
Timeline of incidents and how discovered	Enter description		
Description of mitigation effort	Enter description		

Estimated time to resolution	Enter description
Risks to resolution	Enter description
Requests for help from CBK	Enter description

4.2 Situation Report

In line with Section 3.1 reporting requirements, Regulated Entities shall use this template to structure their notifications to CBK of their response's progress to mitigate an already declared cybersecurity incident.

Situation Report					
Regulated Entity name	Name				
Entity's severity impact rating	As per Entity's severity impact matrix		Entity's incident reference #		Unique identifier, if applicable
Current Situation as of	Date:	DD MMM YYYY	Time:	HHMM	
1. What has happened since the last notification?	Enter description				
2. When did changes happen?	Enter description				
3. Where did changes happen?	Enter description				
4. How, when, and by whom was anything new discovered?	Enter description				
Cause					

1. What is your understanding now of what caused the incident?	Enter description
2. Was the source internal, external, or unknown?	Enter description
Impact updates	
1. Operations	Enter description
2. Customers	Enter description
3. Staff	Enter description
4. Data/systems	Enter description
5. Notification / communication requirements	Enter description
6. Legal / Regulatory	Enter description
7. Reputation	Enter description
Response updates	
1. What response actions have taken place so far?	Enter description
2. How effective has the attempted mitigation been?	Enter description
3. What challenges remain to resolving the situation?	Enter description

4. What is the current estimated time of resolution of the situation?	Enter description
Severity and Potential for Escalation	
1. How could the situation get worse?	Enter description
2. What other entity and/or systems might become affected?	Enter description
Questions	
1. What other information should CBK know?	Enter description
2. What support do you require from CBK?	Enter description

4.3 Closure Report

In line with Section 3.1 reporting requirements, Regulated Entities shall use this template to structure their response closure reporting to CBK, documenting their efforts, conclusions, and lessons learned from the crisis.

Closure Report					
Regulated Entity name	Name				
Entity's severity impact rating	As per Entity's severity impact matrix		Entity's incident reference #		Unique identifier, if applicable
Current Situation as of	Date:	DD MMM YYYY	Time:	HHMM	
1. Description and date of incident response start and closure	Enter description				
2. Description of response plan and action	Enter description				
3. Parties involved in response action	Enter description				
4. Role played by CBK, if applicable	Enter description				
5. Role played by third parties, if applicable	Enter description				
6. Original estimated time to resolution (as documented in Notification Report)	Enter description				
7. Actual time to resolution	Enter description				
8. Impact on customer base	Enter description				
9. Financial impact	Enter description				

10. Reputational impact	Enter description
11. Notable challenges in recovery process	Enter description
12. Legal/regulatory involvement	Enter description
13. Lessons learned and planned developmental actions	Enter description

4.4 Low Impact Incident Reporting Template

In line with Section 3.1.1 reporting requirements, Regulated Entities shall use this template to report quarterly amalgamated summaries of low impact cyber incidents.

Low Impact Incidents Report		
Regulated Entity name	Name	
Date range included	Date:	DD MMM YYYY - DD MMM YYYY
1. Summary overview of incidents listed below	Enter description	
2. Summary overview of response actions taken to incidents listed below	Enter description	
3. Summary overview of impacts of incidents listed below	Enter description	
4. Summary of lessons learned and further actions needed	Enter description	

resulting from the incidents listed below	
5. Virus discoveries	Enter number total
6. Phishing attempts	Enter number total
7. Port scans	Enter number total
8. DDoS attacks	Enter number total
9. Cryptoware attempts	Enter number total
10. Malware attempts	Enter number total
11. Breach discoveries	Enter number total

5. Appendix – Glossary

Term	Definition
CBK	Refers to the "Central Bank of Kuwait".
CSF	Refers to the "Cybersecurity Framework".
CMSP	Refers to the "Cyber Crisis Management Strategy and Plan"
Local banks	Refers to all Banks including the Kuwaiti Banks and the Foreign Banks authorized by CBK.
Regulated Entities / Banking Sector	Refers the following: ● Kuwaiti Banks ● Foreign Banks ● Finance Companies ● Exchange Companies ● Investment Companies ● Electronic Payment Infrastructure Provider, Electronic Payment Agents, that are subject to Instructions Regulating Electronic Payments of Funds (No. 44/430 of Year 2018)
Responsibility	The responsibility of the individual(s) who actually complete the task(s), action(s), and implementation. Responsibility can be shared.
Accountability	The accountability of the individual(s) who is ultimately answerable for the activity or decision.
Crisis Response Lead	A Regulated Entity employee who is authorized to make crisis response related decisions independently and on behalf of the Regulated Entity and to act as a single point of contact and lead representative of the Regulated Entity in CBK-led, sector-wide responses
ISWG	Refers to the "Information Security Working Group"
Cybersecurity maturity	Refers to the assessment of cybersecurity against levels defined as a part of Cybersecurity assessment process.
Third Party	Refers to any organization providing products or services to the Regulated Entities.

Third Party	Refers to any organization providing products or services to the Regulated Entities.
Incident	An event 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 whether resulting from malicious activity or not.

GUIDE BOOK - CYBERSECURITY READINESS ASSESSMENT TEMPLATE FOR KUWAIT BANKING SECTOR

GUIDE BOOK - CYBERSECURITY READINESS ASSESSMENT TEMPLATE FOR KUWAIT BANKING SECTOR

TABLE OF CONTENTS

1 Introduction

This document outlines the methodology for 'Ongoing Assessment and Maturity Improvement' to the overall Cybersecurity Program of CBK, and provide guidance on how to use the 'Cybersecurity Readiness Assessment Template' by regulated entities.

1.1 Target Audience

This document is expected to be read by individual assessors who will be responsible for updating the information required in the Template. In addition, senior management, information security, information technology, risk & compliance professionals and any other personnel of regulated entities who are responsible for providing inputs for the assessment are expected to be abreast with this document.

1.2 Approach Overview

Regulated Entities shall follow a structured self-assessment approach, which will assist in identifying the current Maturity level of the organization. The steps for performing the self-assessment include:

a) **Inherent Risk Profile**: Regulated Entities shall identify the inherent risk based on set of parameters that have been outlined in the Template. The intent of the inherent risk profile is twofold; one is to provide the Regulated Entity with a consistent method to assess their own inherent risk profile, second is for CBK to consistently measure the inherent risk of all the entities under its supervision.

b) **Baseline Assessment:** Regulated Entities shall complete a baseline self-assessment in order to assess maturity of their cybersecurity program. Appropriate business justifications for exclusion shall be documented as part of the assessment.

c) **Reporting:** Regulated Entities shall provide CBK with their inherent risk profiling and baseline assessment results and the remediation activities and plans as per the periodicity defined by CBK.

d) **Periodic / ad-hoc assessment and reporting:** Regulated Entities shall provide information as per the periodicity that will be defined by CBK. In addition, ad-hoc information as stipulated by CBK from time to time will have to be provided by the Regulated Entities.

2 Ongoing Assessment and Maturity Improvement Program

The below figure depicts the operational view of the ***Cyber Resilience Roadmap*** that has been developed by CBK**.** In this document, we have covered the specific operational aspects of the Assessment and Maturity component from the program.

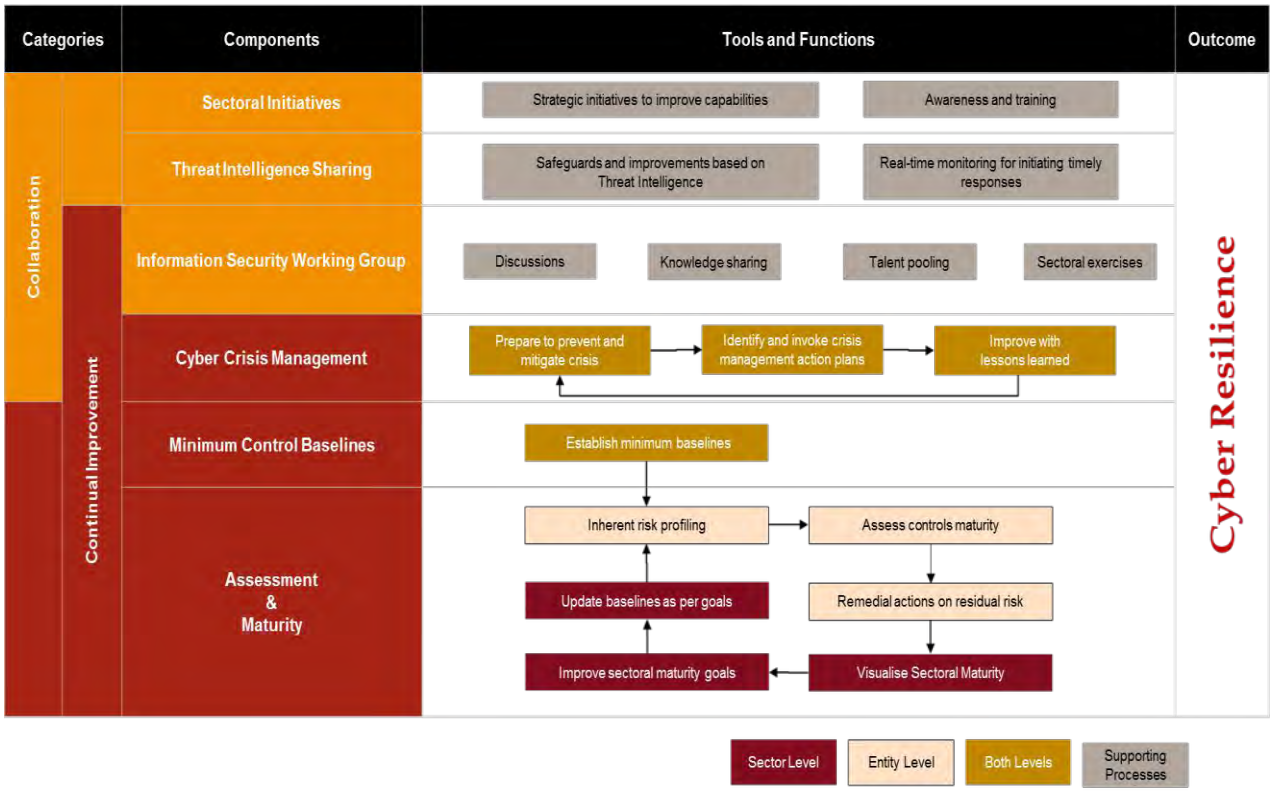
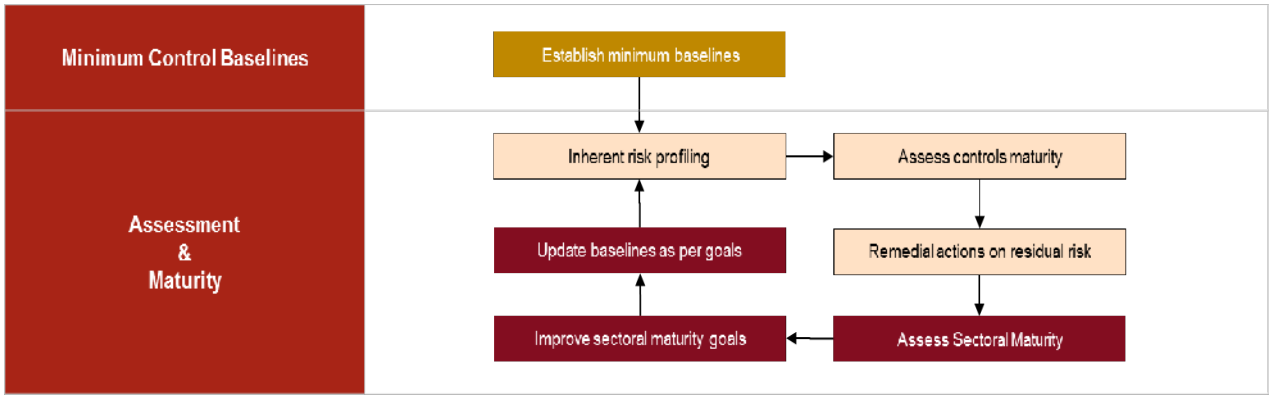


Figure 1: Cyber Resilience Roadmap (as visualized in Cybersecurity Framework (CSF) Document)



*This Illustration depicts the levels for the activities to be performed, and does not depict roles and responsibilities.

- Sector level activities and entity level depict the variation between conducting the process for an entity or for sector as aggregation/representation of multiple entities.
- Both levels is used for collaborative or isolated set of activities to be performed by all entities.

Figure 2: Extract of Cyber Resilience Roadmap for Assessment and Maturity component of CSF

The assessment and maturity improvement program will involve the following steps. The assessments will be conducted using a excel based template which will be published by CBK. The template serves as a method for consistent data sharing by the Regulated Entities.

2.1 Step 1: Inherent risk profiling

The Regulated Entities are expected to conduct a self-assessment of their inherent risk profile using the template before conducting the baseline maturity assessment. The Inherent Risk Profile assists by assessing the risk profile of the entity.

2.2 Step 2: Assess baseline maturity

The Regulated Entities are required to use the Baseline-Self Assessment template and conduct a self-assessment to assess the baseline maturity of implemented controls. This would provide the Regulated Entities with an accurate view of their preparedness and compliance with respect to the cybersecurity risks. The results of the baseline maturity assessment would assist the Regulated Entities to undertake initiatives to fulfill the identified gaps and improve their cyber resilience.

2.3 Step 3: Remedial actions

The completion of baseline assessment provides a set of controls on which the Regulated Entity needs to undertake improvements/ initiatives and ensure compliance. Regulated entities are required to undertake the necessary improvements as such gaps need to be remediated. A plan for remediation is required to track and complete all remedial actions.

The consolidated results obtained after performing step 1 to 3 would need to be submitted to CBK at pre-defined intervals.

2.4 Step 4: Assess sectoral maturity

CBK would collate individual outcomes provided by each Regulated Entity and arrive at the overall sectoral and sub sectoral maturity.

The inherent-risk profiling will assist CBK in stratifying the Entities into groups and prescribe specific reporting, compliance and baseline controls. The baseline maturity assessment results will assist CBK in evaluating compliance, and overall status of sectoral Cybersecurity risks.

2.5 Step 5: Improve maturity goals

CBK shall periodically or at its discretion undertake independent review of the inherent risk profile and baseline maturity assessment data shared by the Regulated Entities. Upon finding any gap as part of this activity, CBK shall instruct the Regulated Entities to further undertake initiatives to improve their security posture.

The above paragraph shall trigger steps 1 to 3 to be followed by the Regulated Entities and the required submissions to be made to CBK.

2.6 Step 6: Improve and update baselines

Based on the overall trends in the sector, CBK will undertake further initiatives with a view to improve the overall maturity and to address changes happening around the world in cybersecurity risks and incorporate necessary changes in the Inherent Risk Profile and Baselines. CBK will perform trend analysis based on the data collated from various regulated entities over a period of time. In addition, cyber fraud related data from the banking sector will also be considered while doing the trend analysis.

Every significant update will trigger an update of the inherent risk profile as well as the minimum baselines prescribed for the Kuwait banking sector.

The steps 1-3, 4, 5 and 6 are non-linear and maybe invoked on an ad-hoc basis due to changes in the business environment or any other factor significantly.

3 About the Template

This section is a user manual to guide the Regulated Entities on how to use the 'Cybersecurity Readiness Assessment Template' (hereafter referred as the Template) and also assists in updating the required information in the Template.

The 'Template' is designed to capture data from the Regulated Entities in a consistent manner so that a baseline maturity score for individual regulated entities can be derived consistently.

The Template has the following tabs / modules (more commonly referred as tab in the document):

- Document Control / Instructions;
- Rating Guide;
- Inherent-Risk Profile;
- Baseline-Self Assessment;
- Baseline Risk Map; and
- Domain and Subdomain wise Maturity View.

This section describes the objective for each tab and also further details out the tables and fields, within each table for complete understanding purpose. In order to minimize data update errors, all fields except user editable fields are locked in the template. In this guide, fields which are user editable have been marked in bold and italics in each table explained below.

4 Usage Manual

Overview: Each tab has a set of data capturing templates/ tables which are explained in detail in this section.

4.1 Document Control and Instructions

Objective: The objective of the tab is to capture static information about the Regulated Entity which is essential to identify the entity, submission period, details of person providing the sign off on the document, etc.,

Document Template Change Control History

Serial Number	Document	Version	Change Description	Approved By
Running Serial Number for Tracking Purpose	Name of the Document along with the version history and applicable period for which this version can be used by the Regulated Entities	Version number of the document	Details of changes done from the previous version and other important notes.	Name of the person authorized by CBK to release this version.

Entity Details

Name of Regulated Entity *(Free Text)*	Name of the Entity as per the Certificate of Incorporation Provided by CBK
Unique Number (Free Text)	Unique Registration / Serial Number provided to the entity by CBK at the time of registration
Contact Person (Free Text)	Person who has been authorized by the entity to submit the information required in the document.

Baseline-Self Assessment Details

Serial Number	Assessment Period	Name of Assessor *(Free Text)*	Date of Submission *(DD-MMM-YY)*	Remarks *(Free Text)*
Serial number	The period for which the information is being submitted.	Name of the assessors who were involved in the baseline-self assessment exercise	Actual date of filing of the information with CBK.	Any other comments that the Regulated Entity wants to submit as part of the submission

4.2 Rating Guide

Objective: The tab provides definition and declarative statements that Regulated Entities shall consider while conducting the maturity assessment.

Baseline-Self Assessment Rating Guide

Exposure Level - Maturity Rating Criteria	
Maturity Level	Definition and Criteria
Relevant Rating Scale	Definition and criteria serve as a measurement scale using which each control needs to be assessed and a maturity level needs to be assigned by the Regulated Entity.

4.3 Inherent-Risk Profile

Objective: The tab provides guidance and rating scale for conducting inherent-risk profile. The assessment criteria's have guidance statements which the Regulated Entities need to evaluate and fill in the appropriate inherent risks information.

Cybersecurity inherent risk profile results provide a mechanism for CBK to stratify the Entities (grouping of entities based on the risk profile) and assists CBK in effective management of risk. In addition, it provides a comparative measurement and the level of risks that each entity poses to the banking ecosystem.

The inherent-risk profile is a dynamic list and would be enhanced and updated on a periodic basis by CBK.

The advantages for inherent risk profile for the Regulated Entity include the following:

- Identifies factors contributing to the Regulated Entity's overall cyber risk; and
- Determines the risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.

The advantages for CBK include the following:

- Visibility of all Regulated Entities inherent risk profile basis a common scale; and
- Quantifies the Inherent risk exposure that the individual Regulated Entities pose to the Banking sector by way of their operations.

Domain	Sub-domain	Sub-domain Number	Assessment Criteria	Information to be Updated by Regulated Entities	Guidance for updating the values in the adjacent column	Comments, if any from Regulated Entities
Name of the Domain	Name of the sub-domain	Unique Sub-domain reference number	User to fill in appropriate inherent risk level based on the guidance provided for each assessment criteria	*Regulated entities can capture the reasons for the risk scores provided for each sub-domain*	Provides additional information to the Regulated entities for filling up the inherent risk profiling sheet.	Regulated entities can add additional comments / information as necessary for better understanding of CBK

4.4 Baseline-Self Assessment

Objective: The tab is to be used for conducting the baseline maturity assessment for each control objective which is then aggregated using simple average at domain and sub domain level. Since baselines are mandatory controls, each control has been given equal weightage for aggregating the overall maturity scale.

The baseline-self assessment is based on the baseline document published by CBK. It provides the mechanism for identifying the Maturity of individual control that an Entities has established for the four (4) specified domains and thirty-six (36) sub domain areas.

The advantages for the Regulated Entity include the following:

- Assesses the Entity's cybersecurity preparedness;
- Assesses the level of compliance against the minimum baseline as mandated by CBK; and
- Determines the risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired minimum baseline standards.

The advantages for CBK include the following:

- Visibility of Maturity levels across all Regulated Entities through common reporting template;
- Quantifies the risk exposure that the individual Entities pose to the Banking sector; and
- Aggregated risk within the sector.

The assessment sheet is split into two parts, static information and information that will have to be updated by the Regulated Entities.

Part A: Static fields from the table

Assessment Period	Domain Code	Domain Name	Subdomain Code	Subdomain Name	Control Code	Control Details	Rated at *(Sub Domain / Control)*
Will be populated from Document Control Sheet Automatically	Unique reference code of each domain	Name of the domain as per the Baseline Document	Unique reference code of each sub-domain	Name of the sub-domain as per the Baseline Document	Unique code number given to each control from the baseline document.	Control requirement as established in the baseline document.	This field helps understanding whether the assessment is to be done at a control or sub domain level. This has been retained for futuristic purpose.

Part B: Editable fields from the table

Current Maturity	Internal Policy and Other References	Current Gaps Applicable where ever the Current Maturity Level is < 3	Remediation Action Plan	Target Date *(DD-MMM-YY)*	Global Framework Reference	CBK Comments *(Reserved For CBK)*
Using the rating guide Regulated Entities need to fill in the maturity level at a control or sub-domain level. This is a drop-down field.	Regulated Entities are expected to fill in the exact policy reference based on which this control has been rated. This will aid the regulator to assess the compliance quickly as part of the annual / ad-hoc or periodic reviews.	The identified gaps that need to be plugged by the Regulated Entity in order to reach a minimum maturity level of 3. This will form the basis for the ongoing corrective action plan tracking	The board approved remediation plan needs to be captured here highlighting the key actionable, control owner, stakeholders involved etc.,	Date by when the control is expected to be implemented by the Regulated Entity.	In case of global entities having presence in Kuwait, Regulated entities may rely on global policies for complying with the baseline requirements. The global policies that may have been referred too while conducting the self-assessment need to be captured in this field	This column is reserved for CBK comments. Basis the periodic assessment that may be conducted any non-compliance or inconsistencies will be captured in this filed for the entity to action upon the same.

4.5 Baseline Risk Map

Objective: The tab provides a side by side view between the inherent-risk profile and Maturity of cybersecurity controls implemented by the Regulated Entity.

The table below present a side by side comparison for the inherent-risk score and the assessed Maturity. Regulated Entities can priorities their actionable based on the comparative chart as presented below.

Cybersecurity Maturity Level

Domain	Sub Domain	Sub Domain Code	Inherent Risk Level	Maturity Score
Name as domain per the baseline document	Name of the sub-domain as per the baseline document	Unique code provided to the sub-domain	Simple average of the inherent-risk score from the inherent-risk profile tab. This is column is auto populated from the Inherent-Risk Profile Sheet	Simple average of the Baseline-Self Assessment at sub-domain level. This column is auto populated from the Baseline-Self Assessment Sheet

4.6 Domain and Subdomain Graph

Objective: The tab provides a bar graph of domain wise Maturity of cybersecurity controls implemented by the Regulated Entity.

4.7 CSVs

Objective: The tab provides an exportable Pipe("|") separated output of the completed template for sharing or for uploading to appropriate analytical tool/s for further analysis and inferences. This output is generated only when the document state in "Document Control & Instruction" sheet is marked as "Closed".